United States
Department of Justice

Privacy Policy Development Guide

and Implementation Templates

Providing justice practitioners with practical guidance for the privacy policy development process

October 2006

Privacy Policy Development Guide

and Implementation Templates

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

BJA

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Contents

Section 1 Acknowledgments 1-1

Section 2 Foreword 2-1

Section 3 Introduction 3-1

Section 4 Privacy Policy Overview 4-1

4.1 What Is a Privacy Policy? 4-1
4.2 When Should an Entity Develop a Privacy Policy? 4-1
4.3 The Intersection Between Privacy, Information Quality, and Security 4-1
4.3.1 Privacy and Information Quality 4-1
4.3.2 Privacy and Security 4-2
4.3.3 Future Guidance Statement 4-2
4.4 Resources 4-2

Section 5 Governance 5-1

5.1 Identifying the Project Champion or Sponsor 5-1
5.2 Resource Justification 5-2
5.3 Identifying the Project Team Leader 5-2
5.4 Building the Project Team and Stakeholder Contacts 5-3
5.4.1 Project Team 5-3
5.4.2 Stakeholder Contacts 5-3
5.5 Team Dynamics 5-4
5.6 Resources 5-4

Section 6 Planning 6-1

6.1 Developing a Vision, Mission, Values Statement, and Goals and Objectives 6-1
6.1.1 Vision Statement 6-1
6.1.2 Mission Statement 6-2
6.1.3 Values Statement 6-2
6.1.4 Goals and Objectives 6-3
6.1.4.1 Goals 6-3
6.1.4.2 Objectives 6-3
6.2 Writing the Charter 6-3
6.3 Resources 6-4

Section 7 Process 7-1

7.1 Understanding Information Exchanges 7-1
7.1.1 Tools to Assist With Understanding the Flow of Information 7-3
7.1.1.1 *Justice Information Privacy Guideline* 7-3
7.1.1.2 Justice Information Exchange Model (JIEM) 7-3
7.1.1.3 Privacy Impact Assessment (PIA) 7-4
7.2 Analyzing the Legal Requirements 7-5
7.2.1 Introduction 7-5
7.2.2 Approach to the Legal Analysis 7-5
7.2.3 Focusing the Legal Analysis 7-6
7.2.3.1 Suggestions for Approaching the Legal Analysis 7-6
7.2.3.2 Potential Sources of Legal Authority and Limitations 7-6
7.2.3.3 Particular Events and Actions 7-7
7.2.3.4 Information Related to a Specific Person 7-8
7.2.4. Performing the Legal Analysis 7-8
7.2.4.1 Principles 7-8
7.2.4.1.1 Collection of Information 7-9
7.2.4.1.2 Information Quality Relative to Collection and Maintenance of Information 7-9
7.2.4.1.3 Sharing and Dissemination of Information—Public Access 7-9
7.2.4.1.4 Provisions Relevant to the Individual About Whom Information Has Been Collected 7-10
7.2.4.1.5 Information and Record Retention and Destruction 7-11
7.2.4.1.6 Agency or Project Transparency 7-12
7.2.4.1.7 Accountability and Enforcement 7-12
7.2.4.2 Specific Laws to Examine 7-12
7.3 Identifying Critical Issues and Policy Gaps 7-14
7.3.1 Identifying Team Members' Privacy Concerns 7-14
7.3.2 Using Legal Research as a Guide 7-15
7.4 Resources 7-15

Section 8 Product 8-1

8.1 Vision and Scope for the Privacy Policy 8-1
8.2 Outline and Organizational Structure 8-1
8.2.1 Introduction or Preamble 8-2
8.2.2 Definitions 8-2
8.2.3 Applicability 8-2
8.2.3.1 Who Is Subject to the Policy? 8-2
8.2.3.2 To What Information Does It Apply? 8-2
8.2.4 Legal Requirements and Policy Guidance 8-3
8.2.5 Accountability 8-3
8.2.6 Process for Revisions and Amendments 8-3
8.3 Writing the Privacy Policy 8-3
8.3.1 Making the Policy Choices—Filling in the Gaps 8-3
8.4 Vetting the Privacy Policy 8-4
8.5 Sample Privacy Policy Outline 8-4
8.6 Templates to Assist With Drafting the Privacy Policy 8-8
8.6.1 *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* 8-8
8.7 Resources 8-8

Section 9 Implementation 9-1

9.1 Formal Adoption of the Policy 9-1
9.2 Publication 9-1

9.3 Outreach 9-1
9.4 Training Recommendations 9-2
9.4.1 Trainees 9-2
9.4.2 Content 9-2
9.4.3 Method 9-2
9.4.4 Frequency 9-3
9.4.5 Additional Resources 9-3
9.4.6 Acknowledgment 9-3
9.4.7 How Will You Measure Your Success? 9-3
9.5 Evaluating and Monitoring 9-3
9.6 Resources 9-3

Section 10 Preface to Information Quality 10-1

10.1 What Is Information Quality? 10-1
10.2 Impact of Data Quality on Privacy and Public Access 10-1
10.3 What Generates Data Quality Issues? 10-1
10.4 In-Depth Information Quality Guidance 10-2

Appendix A *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* A-1

Appendix B *Privacy and Information Quality Policy Development for the Justice Decision Maker* B-1

Appendix C Case Study: Illinois Criminal Justice Information Authority (ICJIA) and Illinois Integrated Justice Information System (IIJIS) C-1

Introduction C-1
Background C-1
Project Team C-2
Planning C-3
Project Process C-3
Products Produced C-5
Lessons Learned C-5
Additional Reading and Resources C-6

Appendix D Glossary of Terms and Definitions D-1

Section 1
Acknowledgments

This ***Privacy Policy Development Guide and Implementation Templates*** was developed through a collaborative effort of the Global Privacy and Information Quality Working Group (GPIQWG) of the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global). Global serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives.

Global supports the initiatives of DOJ and aids Global member organizations and the people they serve through a series of important collaborative efforts. These include the facilitation of Global working groups. GPIQWG is one of four various Global working groups covering critical topics such as intelligence, privacy, and standards.

GPIQWG assists government agencies, institutions, and other justice entities in ensuring that personal information is appropriately collected, used, and disseminated within integrated justice information systems. GPIQWG addresses accuracy and reliability issues involved in updating criminal history records with subsequent events (e.g., prosecution, adjudication) when those events cannot be linked to an arrest notation previously entered into the criminal history repository. This work includes exploring biometrics technologies and addressing the privacy and information quality issues these technologies present.

In order to formulate a unified and comprehensive approach to privacy and information quality issues, GPIQWG actively coordinates with the other Global working groups.

This document is the product of Global and its membership of justice practitioners and industry professionals. By their very nature, to be responsive to current justice information sharing issues, Global working group memberships are dynamic and dependent on the expertise required at any given time. Therefore, a special thank-you is expressed to the GPIQWG and its members for developing and contributing to this document. During the crafting of this guide, GPIQWG membership was as follows:

Jeanette Plante, Chair
Justice Management Division
U.S. Department of Justice
Washington, DC

Robert P. Boehmer, Vice Chair
Illinois Criminal Justice Information Authority
Chicago, Illinois

Francis X. Aumand III
Vermont Department of Public Safety
Waterbury, Vermont

Alan Carlson
The Justice Management Institute
Kensington, California

David Byers
Arizona Supreme Court
Phoenix, Arizona

Steven Correll
Nlets – The International Justice and Public Safety Information Sharing Network
Phoenix, Arizona

Cabell Cropper
National Criminal Justice Association
Washington, DC

Robert Deyling
Administrative Office of the United States Courts
Washington, DC

Owen Greenspan
SEARCH, The National Consortium for Justice Information and Statistics
Sacramento, California

Bob Greeves
Bureau of Justice Assistance
Washington, DC

Barbara Hurst
Rhode Island Office of the Public Defender
Providence, Rhode Island

John Jesernik
Illinois State Police
Joliet, Illinois

Rhonda Jones
National Institute of Justice
Washington, DC

Erin Kenneally
San Diego Supercomputer Center
La Jolla, California

Erin Lee
National Governors Association
Washington, DC

Hayes Lewis
American Indian Development Associates
Albuquerque, New Mexico

Thomas MacLellan
National Governors Association
Washington, DC

Ada Pecos Melton
American Indian Development Associates
Albuquerque, New Mexico

Wil Nagel
Illinois Criminal Justice Information Authority
Chicago, Illinois

Michael Ramage
Florida Department of Law Enforcement
Tallahassee, Florida

Anne Seymour
Justice Solutions, Inc.
Washington, DC

Steve Siegel
Denver District Attorney's Office
Denver, Colorado

Cindy Southworth
National Network to End Domestic Violence Fund
Washington, DC

Martha Steketee
Independent Consultant
Chicago, Illinois

Elizabeth Whitaker
Georgia Tech Research Institute
Atlanta, Georgia

Carl Wicklund
American Probation and Parole Association
Lexington, Kentucky

Included in this guide is an essential tool for justice system practitioners to use when drafting comprehensive privacy policies, entitled *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*, contained in Appendix A. This resource is a product of DOJ's Global initiative and was developed in partnership with Alan Carlson and the Justice Management Institute (JMI). The templates are relevant to the administration of justice, strategic and tactical operations, and national security responsibilities and are intended to address all types of public safety and public protection risks and threats, whether criminal or from natural disasters.

Section 2
Foreword

Ethical and legal obligations compel every professional in the justice system to protect privacy interests when sharing justice information. Today's increased security needs not only dictate enhanced justice information sharing but also highlight the need to balance privacy protection and justice information access. The ease of digital access now makes analysis of privacy obligations a more complex process. Nonetheless, the underlying foundations for privacy policy exist in our current laws and customs. Constitutions, statutes, regulations, policies, procedures, and common-law requirements still control justice entity collection and sharing of information. What is new is the need for professionals in the justice system to articulate clearly the rules that control their information gathering and sharing activities in a manner that translates into system requirements for system developers and information managers.

The U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee (FAC)[1] and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support broadscale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is a "group of groups,'' representing more than 30 independent organizations, spanning the spectrum of law enforcement, judicial, correctional, and related bodies. Member organizations participate in Global with a shared responsibility and shared belief that, together, they can bring about positive change by making recommendations to and supporting the initiatives of DOJ.

The Global Privacy and Information Quality Working Group (GPIQWG) is a cross-functional, multidisciplinary working group of Global and is comprised of private and local, state, tribal, and federal justice agency representatives. The GPIQWG assists governmental and nongovernmental agencies and institutions involved in the justice system in ensuring that personally identifiable information is appropriately collected, maintained, used, and disseminated within evolving integrated justice information systems.

The Global privacy vision calls for individual agencies to identify their privacy policy requirements within the context of the myriad of legal and societal constraints. Global recognizes the indispensable and primary role of local, state, and tribal justice leadership in enhanced information sharing. Each justice entity must actively define privacy protection and information quality requirements for collecting, sharing, and managing the personally identifiable information that it controls in order to enhance sharing while protecting privacy.

1 The Federal Advisory Committee Act, Title 5. Government Organization and Employees, Appendix 2, www.archives.gov/federal-register/laws/fed-advisory-committee/15.html.

Recognizing the need for tiered privacy policy-related material, GPIQWG members produced two related resources that can be used in tandem or separately, depending on the audience:

1) *Privacy and Information Quality Policy Development for the Justice Decision Maker*[2] –

Geared toward the justice executive to engender awareness about the topic, this high-level, easy-to-read booklet makes the case for privacy policy development and **underscores the *imperativeness* of leadership** in promoting privacy issues within justice agencies. An excellent primer and educational tool, this paper applies settled privacy principles to justice information sharing systems, addresses applicable legal mandates, and makes recommendations on best practices to ensure privacy and information quality.

2) *Privacy Policy Development Guide and Implementation Templates* –

Geared toward practitioners charged with developing or revising their agency's privacy policy, the *Privacy Policy Development Guide and Implementation Templates* is a practical, hands-on resource. Using this guide is the next logical step for those justice entities that are ready to move beyond awareness into the actual policy development process. It assists agencies in articulating privacy obligations in a manner that protects the justice agency, the individual, and the public and makes it easier to do what is necessary—share critical justice information.

Included in this guide is an essential tool for justice system practitioners to use when drafting comprehensive privacy policies, entitled *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems,* contained in Appendix A. The templates are relevant to the administration of justice, strategic and tactical operations, and national security responsibilities and are intended to address all types of public safety and public protection risks and threats, whether criminal or from natural disasters.

2 Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG), *Privacy and Information Quality Policy Development for the Justice Decision Maker*, October 2004, Appendix B, within this guide.

Section 3
Introduction

The ***Privacy Policy Development Guide and Implementation Templates*** is a practical, hands-on resource that supports analysis of privacy protection requirements for information sharing environments. Its purpose is to provide guidance for the process of developing agency privacy policy that articulates agency privacy obligations and supports information sharing, as well as protects privacy and information quality interests. Basic guidance and information is provided for each step of the privacy policy development process with resource lists and Web links to more in-depth information on specific subjects.

The guide begins by providing an overview and definition of a privacy policy and then progresses through planning, developing a project team, and drafting the guidance statements (for example, vision, mission, and values statements, as well as goals and objectives). The guide identifies certain common issues to be addressed and suggests approaches for issue resolution. It walks the user through the steps to determine what specific information a justice entity collects, uses, and disseminates during the course of routine justice operations and assists in the identification of what laws control the collection and sharing of that information.

A privacy policy is necessary whenever information sharing takes place, regardless of the size of the system or number of participants. In order to provide the appropriate context for each step of the policy development process, it is best to read this guide in its entirety before beginning the process.

The authors of this guide assume the following:

1) The justice system entity has, at best, a strategic plan but, at a minimum, has a mission statement and guiding principles.

2) The privacy policy development process cannot be successfully completed by one individual but should use others, whether a formal team or borrowed resources, to assist in the policy development.

3) There exists, or can be generated, high-level interest and support among the agency's senior managers in developing a privacy policy.

4) There is, or will be, specifically assigned responsibility for the development of the privacy policy.

5) An information sharing system includes the mechanism for sharing information (whether electronic, paper, or verbal) and the governing policies, procedures, and customs.

6) There are probably few, if any, clearly identified resources allocated specifically for privacy policy development.

Section 4
Privacy Policy Overview

4.1 What Is a Privacy Policy?

A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, access, expungement, and disposition.

The purpose of a privacy policy is to articulate publicly that the agency will adhere to legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

A privacy policy is different from a security policy. A security policy alone may not adequately address the protection of personally identifiable information or the requirements of a privacy policy in their entirety. The Global Security Working Group (GSWG) has developed *Applying Security Practices to Justice Information Sharing*[3] to address security practices.

The inherent value of a well-developed privacy policy for justice entities is that it protects the agency, the individual, and the public and promotes public trust in information sharing.

4.2 When Should an Entity Develop a Privacy Policy?

A privacy policy is an essential ingredient of sound management and can be developed before, during, or after implementation of any information gathering practice. The optimal time to develop a privacy policy is in the design phase of the system.

4.3 The Intersection Between Privacy, Information Quality, and Security

While privacy is related to and overlaps with information quality and security, each also has distinctly different issues that must be addressed and that may require separate and distinct solutions. As such, these topics merit separate attention and are addressed in related Global products.

4.3.1 Privacy and Information Quality

This guide addresses the development of privacy policies to ensure proper gathering and sharing of accurate personally identifiable information. Justice entities must recognize that despite the implementation of an effective privacy policy, damage and harm can still occur if the underlying information is deficient in quality.

3 Global Security Working Group (GSWG), Global Justice Information Sharing Initiative (Global), *Applying Security Practices to Justice Information Sharing*, Version 2.0, March 2004, http://it.ojp.gov/documents/200404_ApplyingSecurityPractices_v_2.0.pdf.

Information quality can be defined as the accuracy and validity of the actual content of the data, data structure, and database/data repository design. The elements of information quality are accuracy, completeness, currency, reliability, and context/meaning. Section 10, Preface to Information Quality, provides an overview of the privacy and information quality interplay.

4.3.2 Privacy and Security

Personally identifiable information needs to be protected with reasonable safeguards against risk of loss or unauthorized access, modification, use, destruction, or disclosure. Information systems should provide the controls to prevent, detect, and respond to threats and vulnerabilities that may compromise the integrity of the information systems.

An effective **privacy** policy should describe how security is implemented within the integrated justice system for the purposes of protecting personally identifiable information. Similarly, a **security** policy should address information classification, protection, and periodic review to ensure that information is being stewarded in accordance with an organization's privacy policy.

4.3.3 Future Guidance Statement

An agency **must** address the intersection of data quality and security with privacy. In-depth guidance of information quality and security issues ***is forthcoming and will be available as a separate and complementary Global resource***.

4.4 Resources

- Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG), *Privacy and Information Quality Policy Development for the Justice Decision Maker*, October 2004, Appendix B, within this guide.

- Smith, Robert Ellis. *Ben Franklin's Web Site Privacy and Curiosity From Plymouth Rock to the Internet*, 2000, ISBN 0-930072.

- Global Justice Information Sharing Initiative (Global) Security Working Group (GSWG), *Applying Security Practices to Justice Information Sharing,* Version 2.0, March 2004, http://it.ojp.gov/documents/200404_ApplyingSecurityPractices_v_2.0.pdf.

- The Data Warehouse Institute (TDWI), *What Works: The Burden of Information Accountability*, Volume 18, November 2004, www.tdwi.org/Publications/WhatWorks/display.aspx?id=7306.

- Massachusetts Institute of Technology (MIT), Total Data Quality Management (TDQM) Program and International Information Quality (IQ) Conference, http://web.mit.edu/tdqm/www/index.shtml.

Section 5
Governance

This section describes the roles and responsibilities of those who initiate policy development and those with the ultimate responsibility to produce the policy. It is important to have the structure and support for the planning effort clearly defined from the outset. Presumptively, a collaborative project team will be appointed to develop the privacy policy. Collaborative teams function best when participant roles and responsibilities are clear.

5.1 Identifying the Project Champion or Sponsor

Once the need for a privacy policy is established, the next step is to designate a high-level project champion or sponsor within the organization to drive the effort. The project champion will be the individual to help steer the development of the privacy policy, to identify and allocate the necessary resources (both human and other support), and to oversee policy implementation. The project champion or sponsor should:

- Advocate for and defend the effort, the project team leader, and the team.
- Empower the team and its leaders with appropriate authority.
- Ensure that adequate and appropriate resources are available to the team.
- Remove obstacles and address political and organizational issues.
- Support the team on policy issues.
- Act as the high-level authority for the effort.
- Articulate and share the common goals of the effort.

The project champion or sponsor can be:

- The person who designated the project team leader, someone higher in the chain of command that is in a position to facilitate decision making and resource allocation.
- The highest-ranking officer in the particular justice entity.
- The governor of a state or tribal leader.

In the case of a collaborative effort where the ultimate policy may be adopted by more than one organization, there may be champions from each organization who will be bound by the completed policy statements.

Selection of the project champion or sponsor for this development effort will depend entirely on factors specifically related to the assignment and the organization. The key to identifying the project champion is not

only to recognize the need for a sponsor but to identify what role the champion will serve. This person should provide a strong voice for the team effort, particularly when there is competition for scarce resources. The champion should also provide the mechanism for efficient decision making when the project team leader or project manager does not have the authority to make decisions in selected areas.

5.2 Resource Justification

Any privacy policy development team must make an estimation of resource needs and make those resource needs known to the project champion. Different resources may be needed at different phases of the effort. At a minimum, however, the team should project a realistic estimate of resource needs, including:

- Number and needed skill sets of team members required to successfully work on the project.
- An approximate number of hours necessary to complete the project.
- A list of any additional support resources that may be necessary (for example, computers, software, and access to legal services).

While this estimate may change, it will be beneficial to provide the project champion and organization with basic information about resource needs in order to assist the organizational assessment of resource allocation. Providing this estimate should result in an articulated response from the organization's management about what resources will or will not be made available for this project.

In determining resource needs, questions need to be asked in order to prepare a resource justification:

- How many team members will be needed or available from the initiating organization and other organizations?
- What types of resources are needed to support a privacy policy development team (for example, skills or interests of team members, meeting facilities, hardware and software, other equipment, and technical support and legal support)?
- Can resources be reallocated within the agency?
- What other support, staff, travel, materials, or contract support will be needed?
- What, if any, training is available or needed?
- Are the identified resources available within the initiating organization or from other organizations, and who has authority over these resources?
- If not, what are other potential sources of the needed resources and what approaches can be used to obtain them? Who has authority over these resources, and will the project champion support these requests?

In the initial stages of development, not all of these questions may be answered, but going through the process of answering such questions will help to define what is or is not available and may be useful, as the project progresses, in supporting future requests for needed resources.

5.3 Identifying the Project Team Leader

The privacy policy development project must have a project team leader—someone who will direct and manage the project on a day-to-day basis. Generally, the individual assigned to read this guide may have been designated as the project team leader. In any event, the project team leader should possess the following essential characteristics:

- **Organizational Credibility**
  The project team leader should be in a position of credibility within the organization and with outside agencies essential to the success of developing and implementing privacy policies. This does not necessarily mean that this individual possesses an in-depth knowledge of every technology and privacy-related issue. These individuals should, however, understand the technological applications for justice information sharing and the limitations of these applications, as well as the organization's work flow, specifically as it involves the control of data.

- **Organization Authority**
  The project team leader should be in a position to access resources (human and financial) necessary to complete the task and to obtain needed approval or direction from the project champion and organization's chief executives.

- **Ability to Build and Manage Coalitions**
  Since success in this endeavor depends on the substantive involvement of a number of individuals within the department and from outside agencies, the project team leader's ability to build and manage coalitions is essential. The foundation of this ability is the art of managing human relationships—making sure that individual needs are met in the process of accomplishing the ultimate goal of developing and implementing privacy policies that affect multiple justice agencies.

- **Ability to Manage Day-to-Day Tasks Over an Extended Period of Time**
  The process of developing privacy policies will take a significant amount of effort over an extended period of time. It is essential for the project team leader to be able to manage the day-to-day privacy policy development activities, under what is probably minimal human and financial resources, as well as set and adhere to timelines and maintain focus on the ultimate goal.

5.4 Building the Project Team and Stakeholder Contacts

5.4.1 Project Team

Appointing a multidisciplinary, multiagency team is necessary to be successful in the process of developing and implementing privacy policies. This type of collaboration lends a wide range of viewpoints, substantive knowledge, and energy to a process that can easily be bogged down in details and differing interpretations and objectives. To succeed, this team needs structure, leadership, and a sense that the goal can be accomplished.

While the project team should represent a broad array of perspectives, it is important that the number of team members be kept to a manageable size to ensure that the team can accomplish its goals and objectives. Team members must represent the core agencies that are entrusted with the protection of private information for justice information sharing.

The project team should have access to subject-matter experts in areas of privacy law and technical systems design and operations, as well as skilled writers, but these individuals do not necessarily have to be team members.

5.4.2 Stakeholder Contacts

Stakeholder contacts are agencies or individuals that are essential to the development and implementation of the privacy policy but who are not on the project team. Stakeholders have interests in the outcome of the privacy policy and are solicited by the project team to provide input.

When determining broader stakeholder participation, the team should consider whether representation or input is desired from a particular entity or from a particular individual. To avoid creating an unwieldy team, carefully consider what agencies and individuals are essential to developing and implementing the privacy policy. Also take into consideration the authority of the individuals comprising the team who may be able to represent a position on behalf of an organization or entity.

Determine some method for obtaining sufficient input from stakeholders. Approaches to obtaining stakeholder input can include focus groups, surveys, documents for public comment, or invitations to speak on varied issues at team meetings.

In determining the composition of the project team, a helpful analysis may be to divide potential stakeholders into three categories:

1) Individuals and agencies that can implement privacy policies.

2) Individuals and agencies that are affected by privacy policies.

3) Individuals and agencies that have an interest in privacy policies.

The project team should include representatives of the stakeholders described in category one. These representatives may be agencies participating in information sharing, local or state lawmakers or tribal leaders, and the legal community (judges, prosecutors, and defense attorneys).

The second category of stakeholders may include community members, offenders and their families, victims of crime, and employees of agencies involved in justice information sharing, as well as nonjustice agencies who require access to justice information. Carefully consider the local justice information sharing environment and determine if it is advantageous to include representatives from some of these groups on the project team.

The third category of stakeholders includes the public at-large, academia, commercial data consolidators, and private security organizations. At a minimum, information should be made available concerning privacy policies to these groups. In addition, victim rights advocates, privacy advocates, and the media can also affect the development and implementation of privacy policies for justice information sharing.

5.5 Team Dynamics

It is important to establish a decision-making process that is clear to all team members and creates a sense of value and participation. This process should allow for diverse input yet move towards achieving the stated goal.

5.6 Resources

- National Criminal Justice Association (NCJA), Survey of State Governance Structure, *States' Governance of Justice Information Systems Integration: Managing Decisionmaking in an Integrated Environment*, June 2001, www.nga.org/cda/files/STATESGOVJUSTICE.pdf.

- U.S. Department of Homeland Security (DHS), SAFECOM Governance, www.safecomprogram.gov/SAFECOM/about/default.htm.

  This is a model for a governance structure that creates an executive committee and advisory committee with the mission to enable public safety nationwide (across local, state, tribal, and federal organizations) by improving public safety response through more effective and efficient interoperable communications. Specifically, SAFECOM functions as an umbrella program within the federal government, managed by the DHS's Science and Technology Directorate.

- Beyerlein, Michael M., and Cheryl Harris. *Guiding the Journey to Collaborative Work Systems: A Strategic Design Workbook*, San Francisco: Pfeiffer Press, 2003.

  This is a hands-on, practical guide for dealing with the challenges of designing and implementing collaboration in the workplace. The workbook covers a broad range of topics necessary for successful change, including generating and maintaining support for the initiative, launching a thoroughly planned

change program, and effectively communicating the plan to the rest of the organization. Filled with assessments, tools, and activities and based on interviews conducted with twenty-one experts and hundreds of team members, *Guiding the Journey to Collaborative Work Systems* offers the support needed to design in-depth plans for changing work systems to facilitate collaborative excellence.

- Francis, David, and Don Young. *Improving Work Groups: A Practical Manual for Team Building*, Revised Edition, San Francisco: Jossey-Bass/Pfeiffer Publishers, 1992.

  Improving Work Groups: A Practical Manual for Team Building contains guidelines and 25 activities designed to build and maintain effective teams. Aimed at any manager, consultant, or employee responsible for developing effective teams, this publication offers a step-by-step system for initiating and evaluating team performance.

- Graham, Robert J., and Randall L. Englund. *Creating an Environment for Successful Projects*, 2nd Edition, San Francisco: Jossey-Bass Publishers, 2003.

  Since it was first published in 1997, this book has become a landmark work that shows how to develop project management as an organizational practice. This second edition offers solid, results-oriented advice on how upper management can create an environment that supports the success of special projects and the development of new products. The book also includes a wealth of examples from the author's workshop participants and readers of the first edition who have successfully implemented these concepts within their organizations. The following are new in the second edition:

  - Case-study drawn practices about how to achieve greater overall success.
  - Advice for helping project teams come together to become more effective.
  - Information for developing the chief project officer position.
  - Suggestions for implementing project management information systems.
  - More descriptions about organizations and people who have used these principles to develop vastly improved environments.

- Varney, G. H. *Building Productive Teams: An Action Guide and Resource Book*, San Francisco: Jossey-Bass Publishers, 1989.

  This book offers information that shows how to systematically build a productive team by identifying, understanding, and overcoming the inherent problems that occur in a team's day-to-day work.

- The following documents can be obtained from American Indian Development Associates, 2401 12th Street, NW, Suite 212, Albuquerque, New Mexico, 87120, (505) 842-1122, e-mail: Info@aidainc.net.

  2004 Charter for the New Mexico Crime Data Project.

  Melton, A. P., and S. Wall. Integrated Justice Systems in American Indian Communities Planning Series: *Intergovernmental Agreements Supporting Crime Information and Exchange Among Tribes and State*s, 2004, www.aidainc.net/Publications/index.htm.

  Melton, A. P., S. Wall, and H. Lewis. Integrated Justice Systems in American Indian Communities Planning Series: *Understanding the Tribal Justice and Law Enforcement Environment*, 2004, www.aidainc.net/CRD%20Envir.pdf.

- The following resources can be obtained from Chief Mike Lasnier, Post Office Box 1021, Suquamish, Washington, 98392, (360) 598-4334.

Tribal Law Enforcement Information Sharing Initiative: *Concept of Operations*, 2005.

Northwest Association of Tribal Enforcement Officers, *Governance Board Charter*, 2005.

- Team Building Associates, *The Strategic Approach: Six Stages to Higher Performance,* http://teambuilder.server101.com/strategicteambuilding.htm.

  This report is a brief review of the required elements for an effective team.

- Tuckman, Bruce, Ph.D. *Forming Storming Norming Performing [Team Development] Model*, 1965, www.businessballs.com/tuckmanformingstormingnormingperforming.htm.

- Clark, Donald. *Teamwork Survey*, 2004, www.nwlink.com/~donclark/leader/teamsuv.html.

  This is a questionnaire used to evaluate the effectiveness of how a team operates.

- Cook, Ian. The Center for Association Leadership, Whitepaper: *Kickstarting a Brand New Team*, January 2002, http://www.asaecenter.org/PublicationsResources/whitepaperdetail.cfm?ItemNumber=12185.

  This is an article on what to do and what to avoid when creating, managing, and leading a new project team.

Section 6
Planning

Through the planning process, the privacy policy development team can ensure production of a concrete, articulated privacy policy within a reasonable time frame. The systematic process of building commitment among team members and key stakeholders to meet a common mission and goal is essential to ensure acceptance of the policy by those most affected by its implementation. Good planning can focus attention on common goals, articulate individual responsibilities, identify individual issues and challenges, and provide a timetable for completing tangible products.

6.1 Developing a Vision, Mission, Values Statement, and Goals and Objectives

The first step in the planning process should be a team effort to produce a set of written guidance statements (a charter) that serve as an overall guide to both the project and to the team. The process of developing these statements is as important as the statements themselves. The process will help to build team trust and serve as a reference for all team members throughout the effort.

The team charter should include guidance statements comparable to a vision statement, mission statement, values statement, and goals and objectives as hierarchical declarations that logically flow from one to the other. Conceptual definitions are as follows:

- **Vision:** A compelling, conceptual image of the desired, successful outcome.
- **Mission:** A succinct, comprehensive statement of purpose of an agency, program, subprogram, or project that is consistent with the stated vision.
- **Values:** The core principles and philosophies that describe how an agency conducts itself in carrying out its mission.
- **Goals:** The desired long-term end results that, if accomplished, would mean the team has achieved its mission.
- **Objectives:** Specific and measurable targets for accomplishing goals that are usually short term with a targeted time frame.

6.1.1 Vision Statement

Ideally, most justice entities have an articulated vision statement and/or mission statement. This can serve as the starting point for the project team in developing a vision statement. The vision statement describes a compelling, conceptual image of the desired, successful outcome.

For example, the Global Privacy and Information Quality Working Group (GPIQWG), who developed this guide, drafted the following guiding vision statement for the working group.

To accomplish justice information sharing that promotes the administration of justice and public protection by:

- *Preserving the integrity and quality of information.*
- *Facilitating the sharing of appropriate and relevant information.*
- *Protecting individuals from consequences of inappropriate gathering, use, and release of information.*
- *Permitting appropriate oversight.*

6.1.2 Mission Statement

If the agency does not have a vision statement but has a mission statement, use the mission statement as the basis for creating the project team's mission, more narrowly focusing on the specifically assigned responsibility. Mission statements are generally short, preferably no more than a paragraph. The mission statement provides the common statement of purpose among the team members and identifies the function that the project team is supposed to serve.

The mission statement should not describe strategies or detail how to accomplish the mission, rather it is a statement of the long view of the project team's resulting effort. It serves as an important internal document and functions as a public statement to stakeholders and interested persons about the team's focused efforts to address privacy issues and promote information sharing. The mission statement should:

- Educate.
- Establish expectations and limitations.
- Clarify organizational purposes and foster cooperation.

The following is an example of a mission statement:

The mission of [name] is the development and implementation of a privacy policy that promotes justice information sharing while protecting individuals, public safety, and privacy.

Throughout the course of the project team's development of the privacy policy, frequent reference to the mission statement as a resource can help the team focus on activities that contribute directly to policy development and implementation.

6.1.3 Values Statement

A values statement is the guiding or defining principle or principles by which the team will operate. It describes the core principles by which the team will be bound as it goes about developing the privacy policy.

While a values statement is not always necessary, it is recommended that a privacy policy development team engage in some discussion of values statements because of the very nature of the issues. As a result of inherent and recognized conflicts between justice system information sharing and privacy protection, a privacy policy team of stakeholders is likely to bring many varied perspectives to the team effort. Development of common values statements helps establish the rules by which the team will work and will build trust among team members that all perspectives will be considered when formulating policy statements.

The following are examples of values statements:

- We believe victims have a special interest in their privacy.
- We demand integrity and ethical behavior by entity employees and users at all times.

- We accept our responsibility to protect personal privacy.
- We recognize crime control and prevention as fundamental law enforcement responsibilities.

Note, however, that the above are only examples. The process of team determination of common values that results in a culture of trust is as important an outcome as the values statements themselves.

6.1.4 Goals and Objectives

After developing mission and values statements, the next planning tool for the team effort is the identification of clear goals and objectives. Goals and objectives are more specific statements of sought-after outcomes that, when met, help the team achieve its mission. **Goals** are broad, intentional targets that may be intangible and abstract but are more specific than the mission statement. **Objectives** are more tangible, narrow, and concrete statements of outcomes that typically will be completed within a limited time period.

6.1.4.1 Goals[4]

Goals provide a framework for more detailed levels of planning. Goals are more specific than the mission statement but remain general enough to stimulate creativity and innovation.

6.1.4.2 Objectives[5]

Objectives are specific and measurable targets for accomplishing goals. In contrast to goals, objectives are specific, quantifiable, and time-bound statements of desired accomplishments or results. As such, objectives represent intermediate achievements necessary to achieve goals.

The following are examples of goals with associated objectives:

Goal: Increased justice information sharing among identified entities.
Objective: Clearly stated rules for information sharing between entity A and entity B by [date].

Goal: A written privacy policy that is current.
Objective: A stated privacy policy provision that describes the timing and process for review and revision of the privacy policy.

Goal: Executive support for the implementation of the privacy policy.
Objective: An education/marketing plan for agency executives.

While development of these various planning tools will take time, in the end, they contribute to more efficient and effective project team operations. Because all team members participate and present their perspectives and because all team members agree to the final statements, the team charter functions as a valuable resource that keeps the team on target throughout the process.

6.2 Writing the Charter

After completing the vision, mission, values statements, and the goals and objectives, the team should collect these organizing tools into one document, known as the project charter. The charter will serve as a reference and resource throughout the course of the privacy policy development effort. It should memorialize the current status of the effort and can be amended when things change. There is no hard-and-fast rule

4 Adapted from Office for Victims of Crime, *Strategic Planning Toolkit*, Anne Seymour, 2004.
5 Ibid.

that dictates the charter contents or length. The most critical feature of the charter is that it memorializes the planning efforts and agreements of the team members to achieve specific goals and, thus, serves as an historical record of team plans and efforts.

At a minimum, the charter should include an introduction that describes what the charter is about, a section with background information that includes a statement about the authorization or mandate to develop the privacy policy, and a section on membership that includes team member names, as well as a description of member skill sets or special interests. Finally, the charter should reiterate the vision, mission, values statements, and goals and objectives that the team has adopted.

The following is an example of the table of contents of a project charter:

I. Introduction

II. Background

III. Membership

IV. Mission

V. Values Statements

VI. Goals and Associated Objectives

Depending on the nature of the project team and the formality of the assignment to develop a privacy policy, consider presenting the charter for approval to the project champion or sponsor once all project team members have adopted it.

6.3 Resources

- Illinois Integrated Justice Information System (IIJIS), *Privacy Schmrivacy? Drafting Privacy Policy in an Integrated Justice Environment*, June 2004, www.icjia.state.il.us/iijis/public/pdf/PRV/PrivacySchmrivacy_FINAL.pdf.
- Global Privacy and Information Quality Working Group (GPIQWG), Vision Statement, http://it.ojp.gov/topic.jsp?topic_id=55#Vision.
- Global Privacy and Information Quality Working Group (GPIQWG), Mission Statement, http://it.ojp.gov/topic.jsp?topic_id=55#Mission.
- Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), *Charter*, 2002, http://it.ojp.gov/documents/GAC_Charter_2002.pdf.
- Global Justice Information Sharing Initiative (Global), *Guiding Principles and Strategic Vision of the Global Justice Information Sharing Initiative*, Vision Statement, page 3, September 2004, http://it.ojp.gov/documents/200409_GAC_Strategic_Plan.pdf.
- Global Justice Information Sharing Initiative (Global), *Guiding Principles and Strategic Vision of the Global Justice Information Sharing Initiative*, Mission Statement, page 4, September 2004, http://it.ojp.gov/documents/200409_GAC_Strategic_Plan.pdf.
- Melton, A. P., and S. Wall. Integrated Justice Systems in American Indian Communities Planning Series: *Preliminary Planning for Justice Integration in Tribal Communities*, 2004, www.aidainc.net/Publications/index.htm.

Section 7
Process

At this stage, the project champion has been identified; a project team leader and project team members have been appointed; some sense of resource needs (or resource limitations) have been estimated; and a charter has been drafted that lays out the project team's vision, mission, values statements, and goals and objectives. Now the work of the team begins on the substantive activities that will provide the basis for the privacy policy. Although the task may appear daunting, some preliminary analysis of the scope of the project will help to assure the team that development of a privacy policy is not impossible.

The first step is to fully understand the information exchanges to which the privacy policy will apply. The next step will be a legal and policy analysis of existing authority and constraints regarding the collection and use of the set of information exchanges identified in the first step. The last step is to identify the unresolved critical issues and gaps that will require agency policymaking, agency rule making, or legislation.

7.1 Understanding Information Exchanges

Understanding the information exchanges—that is, determining what personally identifiable information[6] the agency collects, manages, and protects—will define the scope of the privacy project and bring success within reach. The project team will limit its development of privacy policy to information that it collects, exchanges, or controls. Thus, the simple step of identifying the information that is exchanged or accessed, as well as identifying communication partners, will help to focus the team on issues that directly support policy development specific to the team's needs.

It is important for the project team to understand the information that is controlled by the agency in order to identify the personally identifiable information that may require privacy protection. Understanding information exchanges or flows not only distinguishes information that should be the subject of the privacy policy development efforts but also pinpoints where that information is along the continuum of a justice process. Highlighting the decision points at which privacy becomes an issue for information collection, use, and dissemination automatically places reasonable limits on the process of developing a privacy policy.

Begin the process with the project team by asking questions about the information the agency gathers from within and outside the agency that it needs to conduct usual business activities. Specific inquiry falls into approximately four categories:

1) Information collection.
2) Information dissemination and access.
3) Information use.
4) Information maintenance and retention.

6 Personally identifiable information is defined and explained in Appendix D, Glossary of Terms and Definitions.

The questions to be answered are:

Information Collection

1) What personally identifiable information does my agency collect?
2) Why is the information collected?
3) What is the source of the information? Where do we get the information?
4) Who within the agency collects the information?
5) How is the information gathered? What methods are used?
6) How is the information kept?
7) Who is responsible for the collection of new data sets?
8) Who is responsible for ensuring the accuracy of the information received?
9) Who is responsible for updating and aging out the information?
10) Who is responsible for expunging the information?
11) Who is responsible for record retention?

Information Dissemination and Access

1) Who within the agency uses the information?
2) With whom does the agency share the information? Who has access to the information?
3) Why is it shared?
4) How is it shared?
5) Who authorizes the sharing or dissemination of the information?
6) How do we authenticate users?

Information Use

1) Who within the agency controls the information?
2) How is it controlled? What systems are used to capture and manage the information?
3) For what purpose does the agency use the information?
4) Who, if anyone, has responsibility for determining when the information should be destroyed or aged out?

Information Maintenance and Retention

1) What personally identifiable information is kept by the agency?
2) How is the information stored—in paper form or searchable electronic form?
3) What are the records retention policies for the agency? How long can the agency keep information? When must the agency purge information?
4) Are there policies requiring the agency to review information for possible purging when other or new information becomes known?
5) Is the agency required to notify those who have accessed information when it is subsequently purged?
6) Does the agency have to keep a record of what information has been destroyed or purged?

These are some of the preliminary questions that must be answered. There are a variety of tools available to assist with understanding information exchanges. The team, together, must decide on what methods to use to obtain basic knowledge about the information exchanges. The team may choose focus groups, interviews, or technical tools that will assist with mapping the information flow. Certainly, the team should investigate whether any mapping tools have been used for other purposes that could be amended to meet the needs of the team.

An information flow map, for example, will reveal those decision points where different privacy protections attach because the information is at a different stage of the justice process and different laws apply. For example, a law enforcement officer may receive a tip that a crime has been committed. He may investigate the tip and make an arrest that ultimately leads to a conviction. In other cases, the charges may be dismissed. At each stage of the process, there will be some collection and communication of personally identifiable information about the alleged offender, victims, and witnesses. In turn, at each stage of the process, the privacy restrictions and protections may differ.

Once an information flow model is created for an agency system or an interagency information exchange, the model can then be reused. Thus, an information flow model for the criminal justice system may need only a few additions and revisions to apply to the juvenile justice system. Adding social services interactions with the court, attorneys, or other advocates, along with the particulars of the postdisposition organizations, may be the only needed additions to capture and understand the entire flow of information.

Frequently, systems developers of case management or records management systems map the flow of information during the design stage, albeit not from a privacy perspective. Check within the agency to determine whether information flow maps already exist with respect to the system in question. With an existing information flow map, the only additional step for assessing privacy implications may be the analysis of changes to information privacy at each information exchange point.

Ask these critical questions: What is the personally identifiable information? What is its source? Who has or wants access to it? To whom is it communicated? How is it communicated, and for what purpose is it communicated? Finally, and most importantly, what privacy laws, policies, or restrictions apply at this stage of the proceedings?

7.1.1 Tools to Assist With Understanding the Flow of Information

7.1.1.1 *Justice Information Privacy Guideline*[7]

This comprehensive guide provides detailed information on the development and history of privacy policies, analysis of current widely accepted privacy guidelines, and specific tools for Mapping Information Flows (Chapter 6) and conducting Privacy Impact Assessments (Chapter 7).

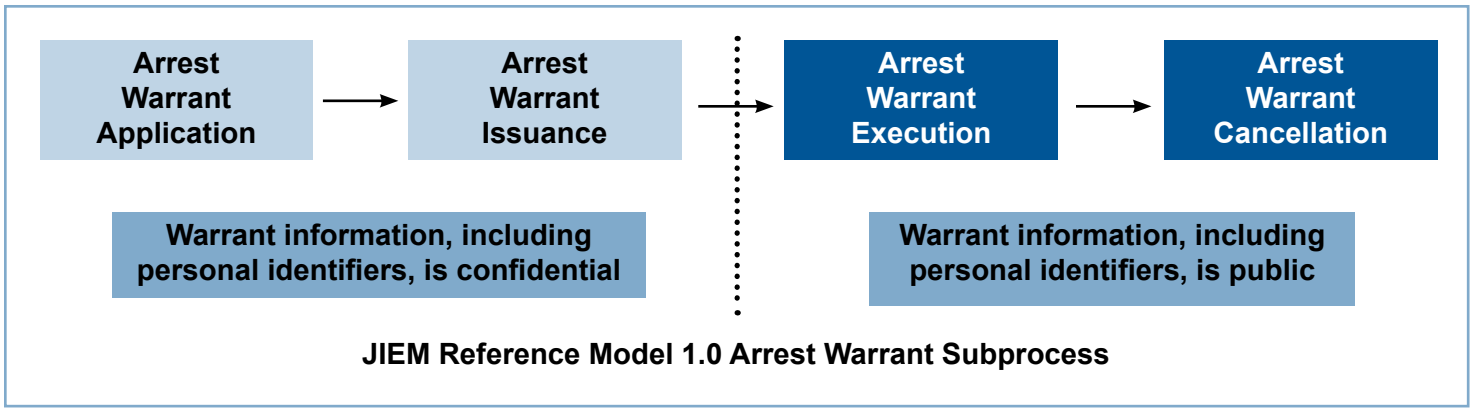
7.1.1.2 Justice Information Exchange Model (JIEM)

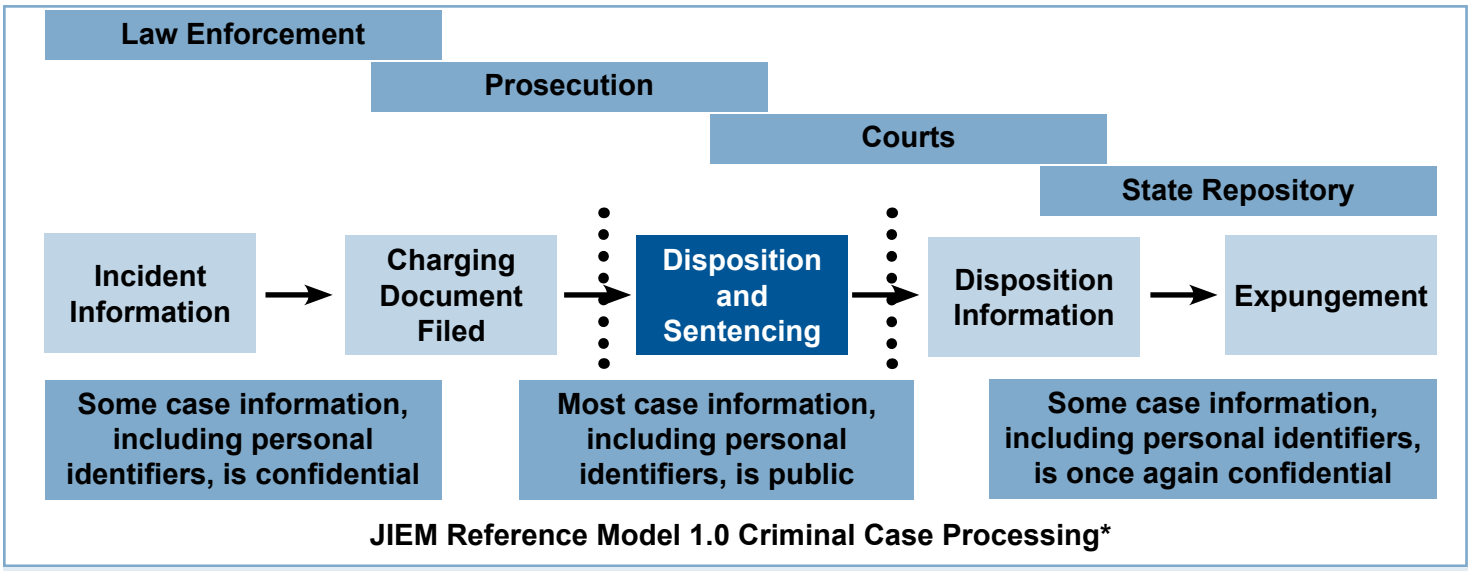
Developed by SEARCH, The National Consortium for Justice Information and Statistics, the Justice Information Exchange Model (JIEM)[8] is a useful tool in planning and implementing justice integration projects. The JIEM is a conceptual framework that defines the dimensions of information exchange; a research and planning methodology for modeling the operational dynamics of this information exchange; and a Web-based software application—the JIEM Modeling Tool—that enables data collection, analysis, and reporting by users and researchers. Although originally designed to aid the systems development process, the JIEM tool is also valuable for breaking down criminal justice processes into key decision points and identifying critical points where the justice community shares and accesses information electronically.

7 National Criminal Justice Association (NCJA), *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*, September 2002, www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/default.htm.

8 SEARCH, The National Consortium for Justice Information and Statistics, Justice Information Exchange Model (JIEM), www.search.org/programs/info/jiem.asp.

The following diagrams are examples of a high-level depiction of a JIEM functional flow, illustrating how privacy concerns may change around a set of information as the information moves through various processes.





*This illustration depicts a partial model. It does not, for example, include as part of the information sharing community the defense, corrections, prerelease, and postdisposition treatment agencies or other private government participants in the justice arena.

The Justice Information Exchange Model has proven to be valuable in analyzing the flow of criminal justice information and in modeling complex business processes. For more information on the JIEM, refer to www.search.org/programs/technology/jiem.asp.

7.1.1.3 Privacy Impact Assessment (PIA)[9]

The availability of information, from personal information to public information, is made all the easier today due to technological changes in computers, digitized networks, Internet access, and the creation of new information products. The E-Government Act of 2002[10]

9 U.S. Department of Justice, Privacy and Civil Liberties Office, *Privacy Impact Assessments*, www.usdoj.gov/pclo/pia.htm.

10 E-Government Act of 2002, PL 107-347, December 17, 2002. This act requires covered agencies to conduct a privacy impact assessment (PIA) before developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form, from or about members of the public. *In general, PIAs are required to be performed and updated, as necessary, where a system change creates new privacy risks.* See *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, www.whitehouse.gov/omb/memoranda/m03-22.html.

recognized that these advances also have important ramifications for the protection of personal information contained in government records and systems.

Privacy impact assessment (PIA) is a comprehensive process designed to assist organizations in determining the effects of information services and sharing initiatives on individual privacy. Similar to a risk management approach, the fundamental components include project analysis, data analysis, privacy analysis, and privacy impact assessment report. PIAs analyze and describe:

- The information that is to be collected.
- Why the information is being collected.
- Intended use of the information.
- With whom the information will be shared.
- What opportunities individuals will have to provide information or to consent to particular uses of the information.
- How information will be secured.
- Whether a system of records is being created under the privacy policy.

7.2 Analyzing the Legal Requirements

7.2.1 Introduction

In order to achieve the goals of effectiveness, comprehensiveness, and legitimacy, a privacy policy must comply with the law. The project team must conduct an analysis of the applicable laws to provide guidance to the agency about what information may be collected, what information may not be collected, how the information can or cannot be collected, and with whom it may be shared. The analysis will also identify gaps where there is no law to guide the policy or where there are conflicts in laws and practices that need to be reconciled before drafting a policy. The objective of the legal analysis is to produce a policy that complies with both the letter and the intent of all applicable local, state, tribal, and federal laws.

Legal compliance should be included in the policy development process from the beginning, not treated as an add-on. Development of a privacy policy, including the legal analysis, should occur during the planning stage and not be postponed until project operations are under way. It is much easier to integrate access, privacy, and disclosure capabilities into a project during the design phase than it is to retrofit.

7.2.2 Approach to the Legal Analysis

One of the keys to conducting an efficient legal analysis is to define the scope of the privacy policy. Specifying what the privacy policy covers will focus the legal analysis and make it more manageable.

For tribal groups, it is important to remember that the policy analysis conducted by state and federal agencies is often not applicable to Indian Country jurisdictions. Therefore, it is essential for tribal groups to identify the people that can provide both culturally relevant and appropriate analysis, as well as legally sound analysis, based on tribal and/or indigenous law.

The approach and suggestions provided in Section 7.2.3.1, Suggestions for Approaching the Legal Analysis, cover a wide range of topics, though not all privacy policies will need to address all of the legal issues identified. By first defining the scope of the privacy policy, the project team can determine which of the sources listed in Sections 7.2.3.2, Potential Sources of Legal Authority and Limitations, are relevant to the privacy policy and which need not be examined.

Decide which entity will perform the legal analysis. The project team, on its own, may not necessarily be responsible for the full legal analysis. Look for assistance from the legal departments of the various entities represented on the team. The scope of the legal analysis will depend upon the scope

of the project. Help may also be available from other agencies that have previously confronted these issues and from tribal, state, and national groups that have already conducted a similar legal analysis. For example, legal analysis help may be available through the tribe's legal counsel or tribal attorney's office.

The legal analysis is particularly important when the project involves Indian tribes. A growing number of tribes are participating in multitribal justice information sharing initiatives. Additionally, most tribes have a legal department, office, or legal counsel that should be enlisted to provide an overview of applicable tribal laws.

Note, however, that there is no universal privacy and information policy that an agency can simply adopt as is. For each project, the agency must examine applicable laws to develop a policy that is compliant and consistent with those laws, including local or tribal laws, and the expectations of funders, users, and the public.

7.2.3 Focusing the Legal Analysis

7.2.3.1 Suggestions for Approaching the Legal Analysis

The initial objective of the legal analysis is to narrow what needs to be analyzed to identify the key legal issues facing the project, given its scope and the nature of the information exchanges involved. This will be much easier if the project team has done the information flow analysis and defined the scope of the project, as discussed previously in this guide.

Some of this work has already been done. The project team is not the first to do this, and it is unlikely the project is so unique that a team has to start from scratch. To begin with, the agency probably already has existing policies and common practices, which may or may not be written down. If they are documented, they may be scattered in policy manuals, bulletins, directives, and memorandums. Gather, review, and organize these documents in a way that exposes the gaps or inconsistencies, if any, with applicable law.

Next, find and leverage the work of others who have already done some of the legal analysis, within the state, for the local tribe, or nationally.

For tribes in particular, legal analysis may be done by such organizations as the National Congress of American Indians (NCAI).[11] The NCAI often conducts policy analysis on overarching issues impacting tribes, such as those dealing with privacy and security, related to information sharing.

Look for other state agencies or local jurisdictions that have similar projects that may have policies the project team can build from or who may have done some of the legal analysis regarding such policies. Tribal groups should look for similar intertribal projects and tribal associations such as the Northwest Association of Tribal Law Enforcement Officers and others.

Finally, the next section of the guide identifies and provides references to a number of existing resources of relevant legal analysis.

7.2.3.2 Potential Sources of Legal Authority and Limitations

Identify all the possible local, state, tribal, and federal laws and policies that apply to the personally identifiable information the agency shares and to the project in the local jurisdiction. These laws may have provisions governing the collection, use, sharing, or retention of certain types of information or information about certain classes of individuals. Examples of the type of laws the project team may need to examine include:

11 National Congress of American Indians (NCAI), www.ncai.org.

- Constitutions—state, tribal, and federal.
- Federal statutes and regulations.
- State statutes and regulations.
- Executive orders.
- Treaties.
- Tribal ordinances.
- Tribal resolutions.
- Descriptions of tribal customary laws.
- Tribal court rules.
- Court procedural and practice rules.
- Case law—federal and state.
- State Attorneys General opinions.
- Professional codes of ethics.
- Local ordinances.
- Laws regarding a criminal history repository.
- Laws regarding an integrated justice information system.
- Laws regarding a criminal intelligence system.
- Laws regarding juveniles, in particular regarding confidentiality of proceedings.
- Family relations laws, in particular child custody and domestic violence.
- Laws regarding medical records and information.
- Laws regarding civil harassment, restraining, and stay-away orders.
- Laws regarding civil commitments of individuals who pose a threat to themselves or others because of mental illness.
- Public records acts, in particular, regarding justice system records and information.
- Open-meeting laws as they affect the agency or the governing body of a justice information system.

Refer to the list of more specific legal topics in Section 7.2.4.2, Specific Laws to Examine. The following discussion will help the project team simplify the legal analysis process and reduce the number of legal sources that need to be examined.

7.2.3.3 Particular Events and Actions

The process of identifying laws that are applicable to the privacy policy development project can be more efficient if there is a context for identifying the laws. One approach is to think in terms of the events, transactions, and information exchanges about which information will be captured by the agency and which are affected by the privacy policy. The legal analysis can proceed by identifying those laws that govern these events, transactions, or exchanges. The laws should be examined to determine if there is specific legal authority, restrictions, prohibitions, or standards of behavior for collecting, storing, using, sharing, or disclosing information of the type identified by the project. The following list describes typical events, transactions, and information exchanges that might be involved in this project:

- Law enforcement contacts—in particular, traffic stops.
- Informants.
- Surveillance, including pen registers and packet sniffers.
- Search warrants.
- Arrest warrants.
- Arrests.
- Interrogation.
- Lineups.
- Officer logs.
- Officer reports—field reports, formal reports, supplemental reports.
- Laboratory or forensic testing or analysis.
- Investigation—existence, work products.

- Trial activities.
- Expungement.
- Retention.
- Disposition.
- Information generated during a trial.
- Victim advocate logs.
- Convictions—any distinctions based on seriousness of crime.
- Sentencing information, including programs providing alternatives to incarceration.
- Treatment programs, including those imposed by problem-solving courts such as drug courts.
- Probation—in particular, terms and conditions.
- Parole—in particular, terms and conditions.
- Domestic violence, civil harassment, and stay-away orders.
- Enforcement of planning, zoning, environmental, and similar laws.
- Other events, transactions, or activities revealed in the project team's information exchange analysis.

7.2.3.4 Information Related to a Specific Person

Many of the laws relevant to the development of a privacy policy are only triggered if the policy covers information that relates to a specific, identifiable person. Expectations about privacy and the laws that have been passed to respond to these expectations often only address the collection and, more importantly, sharing of personally identifiable information (refer to Appendix D, Glossary of Terms and Definitions, for a definition of personally identifiable information). Therefore, the examination of laws that might apply to a privacy policy depends on what types of personally identifiable information are to be gathered, what personally identifiable information will be shared by the agency, and with whom the information will be shared. Information that does not constitute personally identifiable information will generally have far fewer limitations, both in terms of gathering and sharing, than will personally identifiable information.

7.2.4. Performing the Legal Analysis

7.2.4.1 Principles

The following outlined approach tracks the typical steps in the collection and use of information by the justice system. It begins with the collection of the information, addressing what can be collected, how it can be collected, and information quality. The approach then addresses the use, sharing, and dissemination of the information. Included is a separate Subsection, 7.2.4.1.4, Provisions Relevant to the Individual About Whom Information Has Been Collected, on access by an individual to information about that person. Next, are the issues relating to retention and purging of information. Finally, there are subsections on agency transparency and accountability regarding the privacy policy and agency operations.

For each of the stages of the information gathering and use process, there is a listing of the potential subjects to be researched. The research should focus on what authority, limitations, or prohibitions are contained in laws governing the gathering, maintenance, use, and sharing of information. To provide a general background, the discussion of each stage begins with a summary of the related Organisation for Economic Co-operation and Development (OECD) Fair Information Principles (FIPs) – Basic Principles.[12] Although the FIPs were developed around commercial transactions and the transborder exchange of information, they do provide a straightforward description of the underlying principles and a simple framework for the legal analysis that needs to be done with regard to

12 Organisation for Economic Co-operation and Development (OECD), Fair Information Principles (FIPs) – Basic Principles include Purpose Specification Principle, Collection Limitation Principle, Data Quality Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle.

privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

7.2.4.1.1 Collection of Information

The information collection stage concerns not only the act of collecting information but also the means of collection. The FIPs Collection Limitation Principle[13] requires agencies to review both what information they collect and how they collect it. The intent is to avoid unnecessary collection of information and to ensure that only lawful and fair means are used to collect information. In the justice context, the legal analysis should answer the following questions:

1) Are there legal provisions specifying what information can or cannot be collected by the agency/project based on its role and scope?

2) Are there laws that prohibit the gathering of certain types of information—for example, information that relates to the exercise of free speech, free association, or religious freedom—or prohibit gathering of information that involves racial or a similar basis of discrimination?

3) Are there laws specifying a standard for the gathering of information, such as the requirements for obtaining a warrant for search and seizure?

4) Are there laws specifying limits on what methods can lawfully be used to collect information?

5) Are there laws controlling what information can be obtained from third-party, nonpublic information sources? What about concerning the means the third party used to gather the information?

6) What are the requirements, if any, for uniquely identifying an individual who seeks to add information to the agency/project's database, that is, what are the means of authenticating users?

7.2.4.1.2 Information Quality Relative to Collection and Maintenance of Information

In order to be relevant and useful, the information collected must be of high quality. The FIPs Data Quality Principle[14] states that the personally identifiable information gathered should be relevant to the purpose for which it was gathered, and it should be accurate, complete, meaningful, and current. This not only protects individuals, it is necessary for the proper and effective operation of the agency and minimizes waste and misuse of agency resources. Refer to Section 10, Preface to Information Quality, for more information.

7.2.4.1.3 Sharing and Dissemination of Information—Public Access

One of the main purposes of gathering information is to share it with others in the justice system so that the system better accomplishes its mission. However, there must be limits on the sharing of information, both as to with whom and under what circumstances it may be shared. The FIPs Use

13 FIPs 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.

14 FIPs 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.

Limitation Principle[15] asserts that the information gathered should only be shared or used for the purpose for which it was gathered. This is the key to protecting individual privacy. Relevant sharing and dissemination questions for the legal analysis include:

1) Are there legal provisions regarding sharing of information? With whom can information be shared or not shared?

2) What does the state constitution, statutes, and case law, interpreting the provisions, say about openness of agency records and the extent of public access to the information?

3) Is there a law enforcement exception to this public access? If so, how broad is it? To what classes of information does the exception apply?

4) What exceptions exist for specific types of information (for example, arrests or convictions)?

5) What legal exceptions are there regarding specific uses of information? Are there legal provisions with regard to providing information for background checks, preemployment checks, or other noncriminal justice uses? Has certain information been received that is subject to restrictions concerning further dissemination?

6) Are the public access rules for court records more open than for other agencies? When do these rules begin to apply? When is information from other justice system entities introduced into the court record in a case?

7) Are there provisions allowing selling of information to information brokers or third parties? Are there specific categories or types of information for which such bulk transfer of information is permitted or prohibited? Can downstream or third-party use of the information given to information brokers be controlled?

8) What are the requirements for uniquely identifying an individual who seeks access to the information maintained by the agency, that is, what are the means of authenticating users? What are the means of keeping an historical record of the persons or entities with which information has been shared?

7.2.4.1.4 Provisions Relevant to the Individual About Whom Information Has Been Collected

The FIPs Individual Participation Principle[16] focuses on individuals and their access to information about themselves. It requires that individuals

15 FIPs Use Limitation Principle: Personal data should not be disclosed, made available, or otherwise be 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.

16 As stated in the FIPs Individual Participation Principle, an individual should have the right:

a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) To have communicated to him, data relating to him:

- Within a reasonable time;
- At a charge, if any, that is not excessive;
- In a reasonable manner; and
- In a form that is readily intelligible to him;

c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended.

be able to determine if there is information about them, to find out what that information is, and to be able to challenge its quality. Relevant sharing and dissemination questions regarding information about an individual for the legal analysis include:

1) Are there applicable legal requirements regarding notice to individuals of the existence of information about them in agency records? If individuals make inquiries, must they be told about information gathered about them?

2) Are there applicable legal requirements regarding individuals' access to information about them in the agency records? If confirmation or access is denied, must the individual be informed as to the basis for the denial?

3) Are there applicable legal requirements regarding individuals' right to challenge information about them as to its accuracy, completeness, or context?

4) Is there a right of privacy in the state or tribal constitution? How have the courts interpreted this in the justice context?

5) Is there a law establishing a cause of action for invasion of privacy or is there a constitutional provision that is self-executing? Under what circumstances might it apply in the justice context? Does the agency or project have immunity as a governmental agency?

6) Relative to tribal agencies, is there a right to privacy in the tribal constitution, organic documents, tribal customary law, or tribal ordinances? If yes, what are the possible privacy conflicts? What are the remedies for violating tribal privacy laws and/or regulations? Has the tribal court interpreted the Indian Civil Rights Act to include or respect a right to privacy defined by tribal custom or law? Has the tribe established a process to implement any rights to privacy?

7.2.4.1.5 Information and Record Retention and Destruction

One aspect of information quality is currency—a continuing business need for the information. The agency should have a business records retention policy based on need. There may be state or federal records acts that dictate management of records and their disposition. Records retention and disposition policies support efficient use of public resources by avoiding costs of maintaining and sorting through stale or irrelevant information. Relevant records retention and disposition questions for the legal analysis include:

1) Are there applicable legal provisions regarding records retention and disposition? Must information be kept for a certain period of time or destroyed or transferred after a certain period?

2) What are disposition requirements? Disposition? Destruction? Transfer? Expungement?

3) Should anyone's permission be obtained prior to disposition of the records?

4) Should anyone be notified before disposition occurs?

7.2.4.1.6 Agency or Project Transparency

Part of the integrity and legitimacy of the agency and the project is derived from the openness about the existence and nature of the project. The FIPs Openness Principle[17] requires that agencies provide notice about how they collect, maintain, and disseminate information. Relevant questions for the legal analysis regarding agency or project transparency include:

1) Are there legal requirements that policies or other documentation of the agency's project be made available to the public?

2) Are the provisions of open-meeting laws applicable to the agency or the governing board of the project? Are there exceptions in the law for specific meetings or types of deliberative processes?

7.2.4.1.7 Accountability and Enforcement

A good privacy policy is only as good as its implementation. The FIPs Accountability Principle[18] requires an agency to have the means to oversee and enforce its policies regarding the collection, use, and sharing of information. Relevant questions for the legal analysis regarding accountability include:

1) Are there legal requirements regarding audits of the information collected and maintained by the agency?

2) What governmental liability or immunity might the agency or project have regarding:

   - Improper collection of information.
   - Improper disclosure of information.
   - Maintaining information the agency knew or should have known to be incorrect.
   - Not disposing of records, as and when required.

3) Are there legal provisions for sanctions, penalties, or other remedies for unauthorized release or use of information?

4) What sanctions, penalties, or remedies, if any, are specified for failure of the agency to comply with open-meeting laws?

5) Are there legal requirements that agency personnel or users receive minimal training? Do the requirements identify training subjects, such as records management, privacy, and information quality?

7.2.4.2 Specific Laws to Examine

The following is a list of specific laws that may apply to the local jurisdiction and will serve as a checklist for the privacy policy development effort. Not all of these laws may apply to this project, whereas others not listed may significantly affect the project. The intent of providing the list is to help the project team avoid missing any important laws. Review

17 FIPs 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 for 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. Refer to Appendix D, Glossary of Terms and Definitions, for information on the term "data controller."

18 FIPs Accountability Principle: A data controller should be accountable for complying with measures that give effect to the principles stated above.

this list with the project team and legal advisors to determine which laws need to be examined more closely, given the project.

1) **Federal laws and regulations:**
(Refer to Section 7.4, Resources, for cited references.)
   - National Association of State Chief Information Officers' (NASCIO) Compendium of Federal Laws, pp. 84-86.
   - Federal Trade Commission Act of 1914.
   - Title III of the Omnibus Crime Control and Safe Streets Act of 1968.
   - Fair Credit Reporting Act of 1970.
   - Code of Federal Regulations (CFR) Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Parts 20, 22, 23, and 46.
   - Health Insurance Portability and Accountability Act (HIPAA) of 1996.
   - Privacy Act of 1974.
   - Right to Financial Privacy Act of 1978.
   - Privacy Protection Act of 1980.
   - Electronic Communications Privacy Act of 1986.
   - Computer Matching and Privacy Protection Act of 1988.
   - Driver's Privacy Protection Act of 1994.
   - USA PATRIOT Act of 2001.
   - Freedom of Information Act of 1974.
   - Telecommunications Act of 1996.

2) **State statutes and regulations:**
   - SEARCH, The National Consortium for Justice Information and Statistics, Compendium of State Laws: *Compendium of State Privacy and Security Legislation: Overview 2002*, Criminal History Record Information (i.e., criminal history repository laws). Refer to Section 7.4, Resources, for cited references.
   - Criminal justice information system laws.
   - Criminal intelligence system laws.
   - Sex offender registries.
   - Rape shield laws.
   - Victims of crime; crime victims' bill of rights.
   - Problem-solving court provisions.
   - Gang-related laws.
   - Witnesses.
   - Children.
     - Generally.
     - Victims.
     - Juvenile dependency.
     - Juvenile delinquency.
     - Children in custody or visitation cases.
   - Jurors—prospective jurors, trial jurors, or grand jurors.
   - Domestic violence—spousal or partner abuse and elder abuse. This includes the Address Confidentiality Program and its requirements.
   - Harassment, civil protective orders, stay-away orders.
   - Privacy laws. (Refer to Section 7.4, Resources, for the Robert Ellis Smith Compilation, Compilation of State and Federal Privacy Laws.)
   - Drivers—Department of Motor Vehicles (DMV) information.
   - Racial and ethnic profiling.
   - Mental health—evaluations, diagnosis, and treatment.
   - Substance abuse—diagnosis, evaluations, and treatment.
   - Medical—diagnosis and treatment.
   - Financial information.
   - Employee/personnel information.
   - Denial of licensing or benefits.

- Background, preemployment, or other noncriminal justice record checks.
- Voters.
- Public housing.
- Education.
- Communication intercepts (telephone, e-mail, etc.).
- False reports to law enforcement.
- Identity theft.
- Commercial disclosure of personally identifiable information, especially unintentionally or stolen.
- Law enforcement civilian review boards.
- Mandatory reporting laws—doctors, teachers, counselors, etc.
- Gun control laws—checking before purchase.
- Credit reporting.
- Confidentiality of information about individuals involved in specific programs or research projects.
- PIA requirements.
- Expungement or sealing of arrests and convictions.
- Categories of case dispositions with special interpretations or purging requirements (for example, diversion, adjournment in lieu of disposition, convictions converted to dismissals if a program is successfully completed).
- Rehabilitation of individuals with convictions, including restoration of civil rights.

3) **Local and tribal laws, resolutions, and ordinances involving:**
   - Law enforcement review boards.
   - Criminal history repositories.
   - Criminal justice information systems.
   - Criminal intelligence systems.
   - Public records or freedom of information laws.
   - Open meeting laws.
   - PIA requirements.
   - Tribal codes.
   - Contracts regulations and provisions (for example, P.L. 93-638).
   - Federal statutes applicable to Indian Country.
   - Code of Federal Regulations (CFR) that apply to Indian Country.
   - Tribes may have code provisions or may be subject to federal statutes or regulations that address all of the topics listed above in Category 2.
   - State statutes and regulations.

7.3 Identifying Critical Issues and Policy Gaps

Once most of the legal research has been completed, the project team will understand the policy choices that have already been made for the jurisdiction and the body responsible for making those policy choices. For example, the legal research should identify the jurisdiction's laws or policies that are enacting requirements mandated by federal law. It should also identify those laws and policies that reflect choices made by the jurisdiction that were not mandated by federal law. Finally, the legal research should identify those gaps in the jurisdiction's laws or policies that still need to be addressed. Once the team understands the policy choices and determines if an existing policy choice should be revisited, it will know whether to address its findings to the state legislature (if the decision is embodied in state statute) or to the specific administrative agency. Where the current laws and regulations do not address an issue, the team should deliberate based upon the issue's similarity to other resolved issues.

7.3.1 Identifying Team Members' Privacy Concerns

While the legal analysis and FIPs will provide a framework for the development of the privacy policy, the project team should also determine the team's view of privacy issues. The team members will likely deal with information-access issues on a regular basis. They should be aware of the privacy

issues that have caused them concern or caused concern from members of the public with whom they interact. Identify issues to be dealt with when completing the legal analysis and drafting the policy. The team's discussion of identified concerns should provide some clarification as to the policy issues that need to be addressed and help to identify the vision and scope of the privacy policy.

7.3.2 Using Legal Research as a Guide

In drafting the actual privacy policy itself, it is important to keep some things in mind. The local jurisdiction probably has already enacted a significant amount of privacy law that, while scattered throughout the statutes, nevertheless reflects the jurisdiction's privacy policy choices. In developing the policy, it is important to build from existing laws and policies by compiling them into one comprehensive policy and restating them in a brief and clear statement of policy.

7.4 Resources

- National Criminal Justice Association (NCJA), *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*, Chapter 3, September 2002, www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/default.htm.

- U.S. Department of Justice, Privacy and Civil Liberties Office, *Privacy Impact Assessments*, www.usdoj.gov/pclo/pia.htm.

- Office of Management and Budget, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* PL 107-347, December 17, 2002, www.whitehouse.gov/omb/memoranda/m03-22.html.

- Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Fair Information Principles (FIPs), October 26, 2004, http://it.ojp.gov/documents/OECD_FIPs.pdf.

- National Association of State Chief Information Officers (NASCIO), *Information Privacy: A Spotlight on Key Issues*, Compendium of Federal Laws, Version 1.0, February 2004, http://www.nascio.org/publications/InformationPrivacy2004.pdf.

- NASCIO, Federal Privacy Law Compendium, Version 1.0, April 2003, http://www.nascio.org/publications/documents/PrivacyLawCompendium.pdf.

- SEARCH, The National Consortium for Justice Information and Statistics, Compendium of State Laws: *Compendium of State Security and Privacy Legislation: Overview 2002*, Criminal History Record Information, Bureau of Justice Statistics (BJS), November 2003, NCJ 200030, www.ojp.usdoj.gov/bjs/abstract/cspsl02.htm.

- National Conference of State Legislatures (NCSL), listing of Privacy Protections in State Constitutions, www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm.

- Electronic Privacy Information Center (EPIC), listing of privacy laws by state, www.epic.org/privacy/consumer/states.html.

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968, PL 90-351; 18 USC Chapter 119—Wire and Electronic Communications Interception and Interception of Oral Communications, http://straylight.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html.

- Fair Credit Reporting Act of 1970, PL 91-508; 15 USC §1681. Congressional Findings and Statement of Purpose, http://straylight.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00001681----000-.html.

- Health Insurance Portability and Accountability Act (HIPAA) of 1996, PL 104-191, http://aspe.hhs.gov/admnsimp/pl104191.htm.
- Privacy Act of 1974, PL 93-579; 5 USC §552a. Records Maintained on Individuals, http://straylight.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html.
- Right to Financial Privacy Act of 1978, PL 95-630; 12 USC Chapter 35—Right to Financial Privacy, http://straylight.law.cornell.edu/uscode/html/uscode12/usc_sup_01_12_10_35.html.
- Privacy Protection Act of 1980, PL 96-440; 42 USC §2000aa. Searches and Seizures by Government Officers and Employees in Connection With Investigation or Prosecution of Criminal Offenses, http://straylight.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00002000--aa000-.html.
- Electronic Communications Privacy Act of 1986, PL 99-508; 18 USC Chapter 121—Stored Wire and Electronic Communications and Transactional Records Access, http://straylight.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_121.html.
- Computer Matching and Privacy Protection Act of 1988, PL 100-503; 5 USC §552a. Records Maintained on Individuals, http://straylight.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html.
- Driver's Privacy Protection Act of 1994, PL 103-322; 18 USC §2721. Prohibition on Release and Use of Certain Personal Information From State Motor Vehicle Records, www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002721----000-.html.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act of 2001), H. R. 3162, www.epic.org/privacy/terrorism/hr3162.pdf.
- Freedom of Information Act (FOIA) of 1974, PL 104-231; 5 USC §552. Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings, Amended fall 1996, www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm.
- Telecommunications Act of 1996, S. 652, Federal Communications Commission (FCC), www.fcc.gov/Reports/tcom1996.pdf.
- Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*, ISBN 0-930072-11-1, 2003.
- University of Miami, Florida, Ethics Program, Privacy/Data Protection Project, Selected Federal Privacy Statutes, http://privacy.med.miami.edu/web_laws_regs.htm.
- University of Miami, Florida, Ethics Program, Privacy/Data Protection Project, U.S. Federal Privacy Laws, http://privacy.med.miami.edu/glossary/xd_us_privacy_law.htm.
- Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 20—*Criminal Justice Information Systems,* www.it.ojp.gov/documents/28CFR_Part_20.PDF.
- 28 CFR—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 22—*Confidentiality of Identifiable Research and Statistical Information,* www.it.ojp.gov/documents/28CFR_Part_22.PDF.
- 28 CFR—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23—*Criminal Intelligence Systems Operating Policies,* www.it.ojp.gov/documents/28CFR_Part_23.PDF.
- 28 CFR—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 46—*Protection of Human Subjects,* www.it.ojp.gov/documents/28CFR_Part_46.PDF.

Section 8
Product

8.1 Vision and Scope for the Privacy Policy

Having identified issues and completed the analysis, the project team is now ready to draft the privacy policy. Defining the vision and scope of the policy is an essential beginning point for the development of the elements of the privacy policy. The team must make a determination as to whom the policy applies and the scope of its authority. It should also define what the policy will cover.

There will be more than one audience for the policy. The audience will include members of the public, as well as actual practitioners who will use the policy to make day-to-day decisions on how to handle a particular piece of information. The team should aim to draft a privacy policy that is clear in its vision and scope and is readable and understandable by all audiences, in order to ensure its use and instill confidence and public trust.

8.2 Outline and Organizational Structure

The next step is to develop an outline of the policy. The outline does not have to be final at this point, but it can provide guidance on additional research and decision making. A sample outline of a draft policy follows in Section 8.5, Sample Privacy Policy Outline, but the project team should develop an outline and approach that works best for them.

While many entities will be addressing similar issues, each will also likely have some unique issues. Begin by identifying what the privacy policy will accomplish. For example, the user of this guide could be from a single agency that wishes to develop its own privacy policy or from a participant in a multiagency information sharing system. While many of the principles remain the same, there may be particular needs of the local or tribal agency or jurisdiction that do not need to be dealt with by any other agency. For example, tribal groups often have to deal with the overlapping or shared criminal jurisdictions among tribal, state, and federal agencies. As a result, tribal policies may have unique features that are not applicable to other groups.

So far, the project team has identified applicable laws and policies that may apply to information sharing, as well as a process for making determinations about which laws and regulations apply and which laws and regulations may need to be changed. Finally, the team has noted where integration creates new issues that have not yet been addressed or that changes the nature of the sharing such that a particular policy should be revisited. The team should articulate policy recommendations on what laws may need to be updated and areas that remain unaddressed.

While there is no single outline that works best for everyone, there are some elements that should be included in every privacy policy outline. The policy should have an introduction that discusses the importance of privacy in the integrated justice environment and explains what the document is trying to accomplish. The policy should provide general principles that outline the philosophical underpinnings of the privacy policy and provide a statement of the general policy requirements to aid in the resolution of issues not specifically

addressed in the guidance section. The policy should also include a statement that defines its applicability. It should address the collection, access, use, disclosure, expungement, disposition, retention, and quality of justice information. An accountability section should be included to make clear who has the responsibility for implementing and monitoring compliance and should include a discussion of possible sanctions for violation of the policy. Finally, the policy should include an explanation of the process for reviewing and amending the policy on a regular basis.

Significant sections of the document should provide the actual legal requirements and policy decisions concerning the handling of particular types of justice information. Section 7, Process, identifies federal laws that apply to information sharing and outlines a process for analyzing local, tribal, and federal laws and regulations.

8.2.1 Introduction or Preamble

To the extent that the project team identified areas of needed change, they have also identified continued work for the team to effect change.

8.2.2 Definitions

In this section, the team should identify key words or phrases that are regularly used in the privacy policy for which the team wants to specify a particular meaning. This may include terms that are not commonly known or have multiple meanings that may need to be clarified as to which one applies to the privacy policy. Examples might include:

- Personally identifiable information.
- Access.
- Accurate information.
- Criminal history record information.
- Conviction information.

8.2.3 Applicability

8.2.3.1 Who Is Subject to the Policy?

Identify what the privacy policy is about and to whom it will apply; for example, a single agency that wishes to develop its own privacy policy for its employees and information system users, or a participant in a multiagency information sharing system for the employees and users of all the participating agencies. There may also be different provisions applicable to employees, nonemployee users, contractors, third parties (i.e., the media or information brokers), and the public. When developing a statewide policy, it is important to recognize that the stakeholders represent a wide range of political and administrative entities that may have different priorities and vastly different mission statements. Much of a privacy policy can be embraced regardless of the missions of different branches of government, but the scope of a statewide policy is likely to mean that the first step—identifying common principles and goals—will be more time-consuming. Note: *Unless there is agreement and a common purpose at the outset, it is unlikely there will be agreement on specifics.* Developing policy across a statewide structure also means that no stakeholder has a controlling voice.

8.2.3.2 To What Information Does It Apply?

Indicate to what types of information the policy applies in the agency. There may be different policy provisions for different types of information. For example, criminal intelligence information may have different provisions than those of criminal history information or investigatory information. There may also be distinctions based on the type of information, for example, informant information, police reports, or evidence.

8.2.4 Legal Requirements and Policy Guidance

The legal requirements and policy guidance section will be the main section of the document and will spell out the actual provisions regarding the collection, use, and disclosure of personally identifiable information. Legal requirements and policy guidance are discussed in Section 7.2, Analyzing the Legal Requirements.

8.2.5 Accountability

There are several progressing elements of accountability. At the lowest level, the employees and users must be accountable for compliance. This is primarily an internal focus. At the next level, the agency is accountable to its governing body and funders. Finally, the agency is accountable to the public. Provisions for audits, periodic reviews, and responses to allegations of errors or misuse that allow the governing body and the public to monitor agency compliance with the privacy policy and applicable laws address the latter layers of accountability.

8.2.6 Process for Revisions and Amendments

Provisions should be included for regular and systematic review of the privacy policy to keep it current and relevant. The policy provisions should be reviewed in light of new laws (statutory or court decisions), changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

8.3 Writing the Privacy Policy

Once the outline has been drafted, the necessary policy decisions have been identified and discussed, and recommendations have been made regarding the resolution of privacy issues, the project team can begin drafting the policy. As mentioned earlier, the policy writer should keep in mind the audiences for which it is drafting. Since persons of varying backgrounds, including justice practitioners and members of the general public, may read the policy, it is important for it to be written succinctly and clearly. In addition, the rationale for the policy choices should be clearly documented. For example, use commentary to support the formal policy language. Including the rationale will provide additional authority for the policy and will provide some guidance for analogous new issues that arise after the policy is adopted.

A concise executive summary of three pages or less is a valuable tool for the vetting process (refer to Section 8.4, Vetting the Privacy Policy), for review by citizens and executives, and for use at the time of publication (refer to Section 9.2, Publication).

Even though the project team has already done most of its work in discussing and making recommendations regarding particular policy issues, their work is not yet done. The team needs to be involved in the final drafting process. The choice of the language to use in the final document must clearly convey the intent of the privacy policy. Team members will be a valuable resource in ensuring that the language accurately conveys the message intended.

8.3.1 Making the Policy Choices—Filling in the Gaps

In drafting the actual policy, it is important to consider the following: The local jurisdiction probably has already enacted a significant amount of privacy law that, while scattered throughout the statutes, nevertheless reflects the jurisdiction's privacy policy choices. In developing the policy, it is important to build from existing laws and policies, compile them into one comprehensive policy, and restate or reference them in a brief and clear statement of policy. Where gaps in the existing laws are identified or where integration reveals new issues that are not addressed in existing law, the team should explore those issues and recommend a policy decision that will enhance the goals and purposes of the existing policy choices.

8.4 Vetting the Privacy Policy

The draft privacy policy should be broadly disseminated for comment before it is finalized. During the team's deliberations, the project team leader should encourage the team members to consult with and keep their constituencies apprised of the progress of the privacy policy development. The team members should also be encouraged to share the draft privacy policy with their constituents. While significant input should come from the team members who represent large groups, such as police chiefs or sheriffs, additional input should be sought from others who were not involved on the team before the policy is finalized. With this input, additional persons will have been given an opportunity to comment or express concerns about the policy.

How and when others are consulted should be agreed upon by the project team. During the drafting process, it may be appropriate to bring specific issues that need to be resolved to the attention of constituencies for their input. As an initial draft is prepared, it may be appropriate to allow small groups or selected individuals to review portions of the draft. However, the team must be careful not to circulate drafts too early or circulate too many versions of the draft in order to avoid confusion or distribution of incomplete information.

8.5 Sample Privacy Policy Outline

Title I. Preamble

This section will briefly discuss the importance of privacy in the integrated justice environment and explain what this document is trying to accomplish.

Title II. General Principles

This section will outline the philosophical underpinnings of the privacy policy; it will provide a statement of the general policy requirements to aid in the resolution of issues not specifically addressed in the guidance section. The purpose for which personally identifiable information is collected should be specified.

Title III. Policy

This section will provide specific policy concerning the handling of personally identifiable information. Issues to be addressed include the collection, access, use, disclosure, and quality of personally identifiable information.

Article 100. Definitions

(101) Personally identifiable information

(102) Accurate information

(103) Criminal history record information

(104) Conviction information

(105) Other disposition information

(106) Access—by individuals and case by case, as well as bulk or compiled access

(107) Public—includes media

(108) Other definitions

Article 200. Information About Individuals

(201) Information concerning suspects

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing

3. Public access
4. Retention of suspect information

(202) Information concerning arrestees

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of arrestee information

(203) Information concerning defendants

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of defendant information

(204) Information concerning convicted persons

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of offender information

(205) Information concerning probationers

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of probation information

(206) Information concerning incarcerated sentenced persons

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of prisoner information

(207) Information concerning parolees

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of parolee information

(208) Information concerning victims of crime

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Victim protection—specialized confidential data
6. Retention of victim information

(209) Information concerning witnesses

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Witness protection—specialized confidential data
6. Retention of witness information

(210) Information concerning defendant/offender families

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of family information

(211) Information concerning jurors

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of juror information

(212) Information concerning justice officials

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of justice officials' information

(213) Members of the general public

1. Purposes for collection
2. Justice system access
   a. Collection
   b. Sharing
3. Public access
4. Others' access
5. Retention of general public members' information

Article 300. Information About Incidents

(301) Information about noncriminal incidents

1. Purposes for collection
2. Justice system access
3. Public access
4. Others' access
5. Retention of noncriminal incident information

(302) Information about criminal incidents

1. Purposes for collection

(303) Information about arrest incidents

1. Purposes for collection

(304) Contact card information

1. Purposes for collection

Article 400. Special Circumstances

(401) Officer safety information

1. Purposes for collection
2. Justice system access
3. Public access
4. Others' access
5. Retention of officer safety information

(402) Warrant information

1. Purposes for collection

(403) Biometrics (fingerprints, DNA, etc.)

1. Purposes for collection

(404) Intelligence information

1. Purposes for collection

(405) Special considerations

There may be additional categories of information that require specific treatment, such as social security numbers, tribal census numbers, juvenile justice information, financial account numbers, health information, sealed or expunged records, or other information that is specific to the agency's information exchanges.

1. Purposes for collection

(406) Publicly available information

1. Purposes for collection

(407) Tribal enrollment status

1. Purposes for collection
2. How membership was or was not determined
3. Justice system access
4. Public access

Title IV. Accountability and Transparency

(500) Openness of information management practices

(600) Remedies available under law

(700) Compliance audits

(800) Process for correction of information

Title V. Quality of Justice Information

(800) Data quality provisions

(900) Individuals' rights to access and review justice information

Title VI. Review and Amendments

(1000) Continuing review

(1100) Amendments

8.6 Templates to Assist With Drafting the Privacy Policy

The following resource is provided to assist the project team with drafting the privacy policy.

8.6.1 *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*

Developed by the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) in partnership with the Justice Management Institute (JMI), *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*, contained in Appendix A, is a practical tool for justice system practitioners that provides templates for drafting comprehensive policies to protect privacy, civil rights, and civil liberties principles. The policy templates were developed for use by law enforcement agencies, prosecutors, courts, or other justice system agencies or jurisdictions at the local, state, regional, tribal, territorial, or federal level. They were designed to cover a range of computer-based justice information systems that seek or receive, store, and make available information in support of activities associated with the justice system, public safety, and health. The templates are relevant to the administration of justice, strategic and tactical operations, and national security responsibilities and are intended to address all types of public safety and public protection risks and threats, whether criminal or from natural disasters.

8.7 Resources

- Illinois Criminal Justice Information Authority (ICJIA) and Illinois Integrated Justice Information System (IIJIS), Appendix C, Case Study, within this guide.

- American Bar Association (ABA), American Jury Project, *Principles for Juries and Jury Trials*, *Principle 7—Courts Should Protect Juror Privacy Insofar as Consistent With the Requirements of Justice and the Public Interest*, 2005, www.abanet.org/juryprojectstandards/principles.pdf.

- Steketee, M. W., and A. Carlson. *Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts*. Williamsburg, VA: National Center for State Courts. Final report to the State Justice Institute (SJI-01-N-054 and SJI-02-N-007), October 18, 2002, www.ncsconline.org/WC/Publications/Res_PriPub_GuidelinesPublicAccessPub.pdf also www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf.

- National Center for State Courts (NCSC), Public Access to Court Records, www.courtaccess.org.

  State policies are constantly evolving. This is one resource for the latest developments in state-level policies and practices related to court records and associated issues.

- U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global), *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*, September 2006, Appendix A, within this guide.

Section 9
Implementation

9.1 Formal Adoption of the Policy

At some point, the appropriate governing body should formally adopt the privacy policy. The first step for adoption should be approval by the privacy project team itself. Further, if the project team is working under the auspices of some other governing board, approval should be sought from the governing board as well. The governing body may have existing protocols for considering and adopting policies. It may require that the draft be published for comment for a certain period or require public hearings before the governing body. As was discussed earlier, the privacy policy will not necessarily contain any new concepts. For the most part, a privacy policy will include a compilation of various laws and rules that regulate information sharing in the justice system. Simply stated, the privacy policy puts those laws and regulations into context. However, there may be some things that are recommended for the privacy policy that may not be currently addressed under those laws and rules. Depending on the nature of those parts of the policy, the project team may need to seek approval from the legislature.

9.2 Publication

The adopted privacy policy should be readily available to justice decision makers,[19] practitioners, and the general public. The privacy policy should be available to all executives of agencies involved in the development and implementation processes, to local, tribal, and state elected or appointed officials, and the media. The electronic version should be available in a format suitable for downloading from Web sites, internal and public, of all agencies participating in the justice information sharing system. The policy should also be incorporated into training for agency staff and users.

The process by which individuals can ascertain and correct the personally identifiable information maintained about them in participating justice agencies' databases should also be included on all copies of the privacy policy.

9.3 Outreach

If the team has done a thorough job of involving stakeholders and conducting a transparent development and implementation process, outreach to the larger community should be relatively easy. Since all individuals and agencies, including potential opponents, were involved in the process, these representatives can act as emissaries to their colleagues and constituencies. The people who have been involved in developing the policy will no doubt have an established rapport and credibility with their peers and can relate the rationale behind the policy.

19 Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG), *Privacy and Information Quality Policy Development for the Justice Decision Maker*, October 2004, Appendix B, within this guide.

Even with an extensive network of involved individuals, the project team leader, as a representative of the project champion or sponsor, should conduct more formal outreach. This type of outreach can include:

- Press releases and briefings.
- Briefings for elected or appointed local, state, and tribal officials, especially members of the governing body, whether it is a county commission or the state legislature.
- Community hearings.
- Establishment of a volunteer speakers' bureau to provide presentations on request to civic organizations or other groups.

For Indian tribes and communities, outreach and community education are essential because tribal assumptions about privacy are different from state or federal assumptions. Outreach should begin with presentations to the tribal governing body (i.e., tribal councils and judges) and justice system staffs. Outreach should include articles in tribal newspapers to inform tribal citizens.

The purpose of the outreach strategy is to inform the public about the thoughtful, intentional process used to develop the policy and to promote public confidence in the safety and integrity of the personally identifiable information contained in justice systems.

9.4 Training Recommendations

Training is essential to effective implementation of any privacy policy. Each team should determine and recommend an approach to training based on the particular organizational structures, existing training programs, and available resources. At a minimum, a subgroup of the team should be assigned to begin development of training recommendations at the inception of the project team.

Before completion of the privacy policy, the initial training recommendations may exist more as an outline than as substantive content for training. As appropriate, the training team may begin to work on content for the planned methods for training during policy development. For example, the legal analysis may be completed before the formal privacy policy is written, but work on training materials for understanding the law can begin when the legal analysis is complete and does not have to wait for the entire policy to be completed.

Taking into consideration the size of the justice entity, available resources, existing training programs, and the nature of the training to be undertaken, the following areas should be addressed in the team's training recommendations:

9.4.1 Trainees

At a minimum, consider trainees from the following groups: senior management, information technology staff, and those individuals that use the information in their day-to-day jobs.

9.4.2 Content

Training should at least address two broad areas:

- The substance of the policy and its importance to the entity's mission and responsibility, including potential consequences of violating the policy.
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user.

9.4.3 Method

Different approaches to training include lecture courses, distance learning, computer-based training, train-the-trainer courses, and course modules added to existing training programs.

9.4.4 Frequency

There is no question that along with the initial training plan, there should be periodic training updates, refresher materials, and training provided. The critical element is that the project team recommendation contemplates periodic retraining and updates for all users that are affected by the privacy policy.

9.4.5 Additional Resources

Consider whether additional resources might assist the users as they begin to implement the privacy policy. For example, should the project team develop a checklist of steps to follow for certain job functions that could be at the desktop? Would a Web site with frequently asked questions (FAQs) or a Help Desk assist the users?

9.4.6 Acknowledgment

Consider whether there should be some active acknowledgment that privacy policy training was received or reviewed within the agency, such as a signed statement of policy review.

9.4.7 How Will You Measure Your Success?

When developing the training plan, include performance measurement as the final piece of the plan. Consider that the measurement of training success may be rolled into the overall method of measuring the success of the privacy policy. As long as the project team considers what the training is supposed to accomplish, articulates such, and follows a chosen approach to ensure that it has succeeded, the team's training goal will be met.

9.5 Evaluating and Monitoring

A scheme or plan for evaluation and continued monitoring of the implementation of a privacy policy should be in place before the policy is implemented. It is far easier to gain a commitment to ongoing evaluation and monitoring when the investment of the team is high, at the inception of the project, than as an afterthought after the policy is fully developed and on the verge of implementation.

The evaluation should ask such questions as:

- Does the privacy policy, as implemented, respond to the purposes and goals defined in the beginning?
- Is the privacy policy responsive to the legal demands identified at the outset?
- Does the policy have to be updated in response to events occurring since the inception of the project?
- Is any of the justice data that is shared inaccurate and what can be done to minimize that occurrence?

9.6 Resources

- American Society for Training & Development (ASTD), formed in 1944, www.astd.org/ASTD.

  ASTD is the world's largest association dedicated to workplace learning and performance professionals.

- *Training* magazine, www.trainingmag.com.

  Training magazine is a 41-year-old professional development magazine that advocates training and workforce development as a business tool. The magazine delves into management issues, such as leadership and succession planning; human resources (HR) issues, such as recruitment and retention; and training issues, such as learning theory, on-the-job skills assessments, and alignment of core workforce competencies to enhance the bottom-line impact of training and development programs. Written for training, human resources, and business management professionals in all industries, *Training*

combines a primarily paid circulation with a small percentage of qualified, controlled recipients to deliver the strongest circulation in the market.

- McNamara, Carter. Authenticity Consulting, LLC, *Employee Training and Development: Reasons and Benefits*, Free Management Library, The Management Assistance Program for Nonprofits, 1999, www.managementhelp.org/trng_dev/basics/reasons.htm.

Section 10
Preface to Information Quality

10.1 What Is Information Quality?

Information quality is the accuracy and validity of the actual content of the data, data structure, and database/data repository design. The elements of information quality are accuracy, completeness, currency, reliability, and context/meaning.

10.2 Impact of Data Quality on Privacy and Public Access

Gathering and providing access to inaccurate information is not a public service; in fact, it can be a public and personal injustice. In developing the privacy policy, it is important that justice organizations address information quality in concert with privacy issues. Data quality is specifically enumerated as an issue to be considered in the privacy design principles (refer to Section 7.2.4.1.2, Information Quality Relative to Collection and Maintenance of Information). In practice, the accuracy, completeness, currency, and reliability of information connected to an individual may raise as many concerns as the release of the information or its public availability.

Justice agencies should seek to implement privacy-enabling information technologies—technologies that facilitate electronic records storage, internal use, and filtering in accordance with the public right to access relevant data efficiently and in context. Publicly accessible information that may be source accurate can nonetheless be perceived as inaccurate if access to it is prohibitive or if it is presented out of context so as to confuse its meaning or interpretation.

10.3 What Generates Data Quality Issues?

Some of the causes of problems with data quality include:

- Subjective judgment and techniques in data production/collection.
- Poor integration of data from multiple data sources and erroneous linking of information.
- Bypassing data input rules and too restrictive data input rules.
- Large volumes of data.
- Distributed heterogeneous systems.
- Complex data representations, such as text and image.
- Coded data from different functional areas.

- Changing data needs from information consumers.
- Security-accessibility trade-off.
- Limited computing resources.
- Human error (e.g., data entry, transposition, translation, carelessness).
- Data cleansing, normalization, standardization, and processing.

10.4 In-Depth Information Quality Guidance

As highlighted in Section 4.3, The Intersection Between Privacy, Information Quality, and Security, agencies **must** address the issue of data quality. In-depth guidance of information quality issues ***is forthcoming and will be available as a separate and complementary Global resource***.

Appendix A
Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems

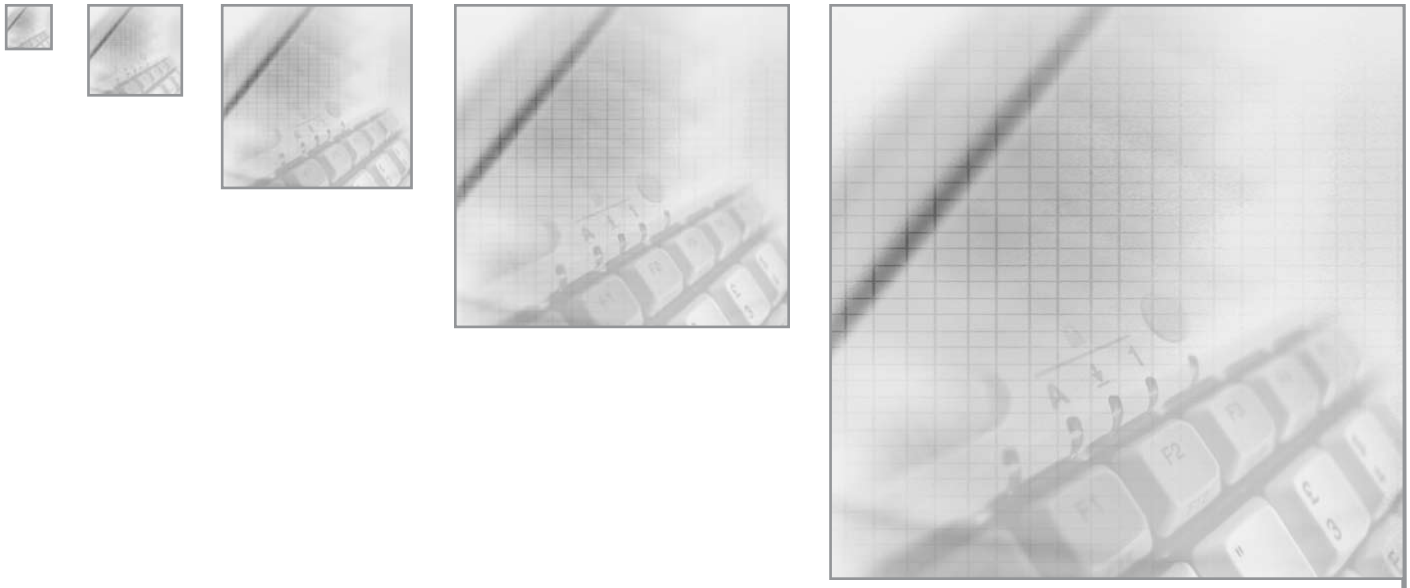
Developed by the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) in partnership with the Justice Management Institute (JMI), *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* is a practical tool for justice system practitioners that provides templates for drafting comprehensive policies to protect privacy, civil rights, and civil liberties principles. The policy templates were developed for use by law enforcement agencies, prosecutors, courts, or other justice system agencies or jurisdictions at the local, state, regional, tribal, territorial, or federal level. They were designed to cover a range of computer-based justice information systems that seek or receive, store, and make available information in support of activities associated with the justice system, public safety, and health. The templates are relevant to the administration of justice, strategic and tactical operations, and national security responsibilities and are intended to address all types of public safety and public protection risks and threats, whether criminal or from natural disasters.

Global Justice Information Sharing Initiative

United States Department of Justice

Privacy, Civil Rights, and Civil Liberties

Policy Templates for Justice Information Systems



Privacy, Civil Rights, and Civil Liberties

Policy Templates for Justice Information Systems

September 2006

To request a Word version of this document, please submit your request to GLOBAL@iir.com.

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

This project was supported by Award No. 2003-DD-BX-K011, awarded by the Bureau of Justice Assistance, U.S. Department of Justice, to the Justice Management Institute.

BJA

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the Justice Management Institute and the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

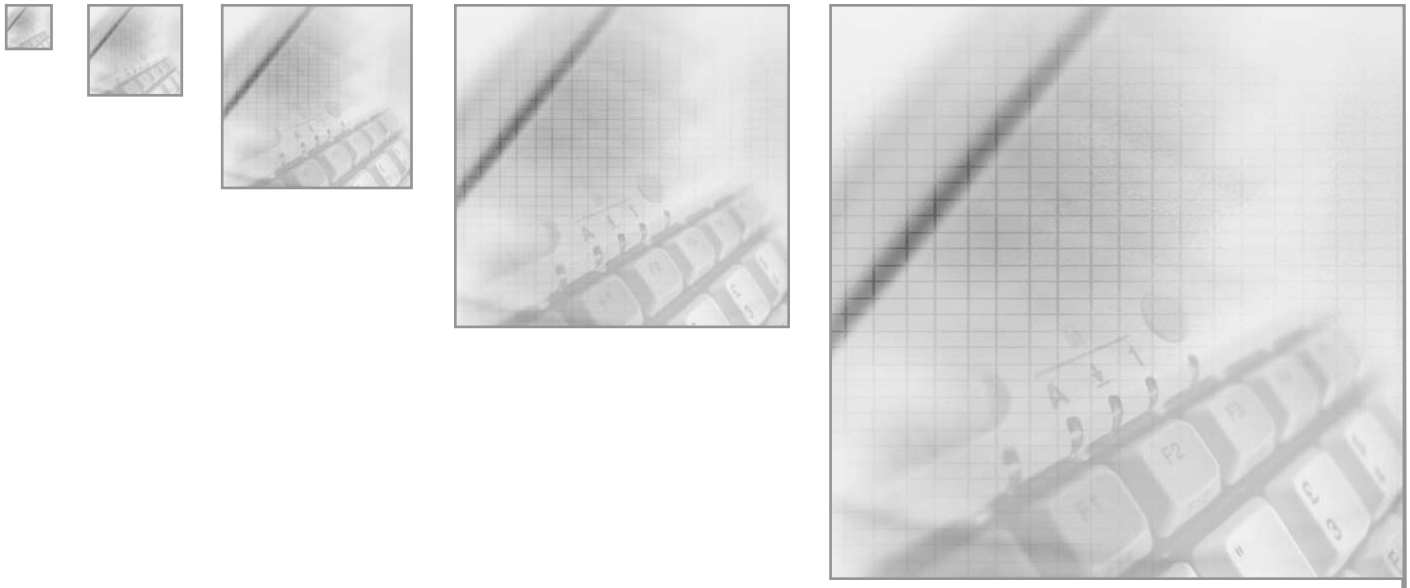


Table of Contents

Acknowledgements ..... **v**

Preface ..... **ix**

Introduction **1**
- Answering a Critical Need, Responding to the Field 1
- Audience 2
- Scope of Policy Templates 2
- Purpose of the Templates 3
- Concepts Underlying Templates 3
- Organization of Policy Templates 4
- Format of Policy Templates 4
- How to Use the Templates 5

A. Elements of Enabling Legislation or Authorization **7**

A.1.00 Statement of Purpose 7

A.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties 9

A.3.00 Agency Transparency and Accountability 10

B. Elements of a Basic Internal Operations Policy **11**

B.1.00 Statement of Purpose 11

B.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties 12

B.3.00 Definitions 12
- B.3.10 Definition of Agency 12
- B.3.20 Definition of Information 12
- B.3.30 Definition of Law 12
- B.3.40 Definition of Public 13

B.4.00 Seeking and Retaining Information ... 13
B.4.10 What Information May Be Sought or Retained? ... 13
B.4.20 Methods of Seeking or Receiving Information ... 15
B.4.30 Classification of Information Regarding Validity and Reliability ... 17
B.4.40 Classification of Information Regarding Limitations on Access and Disclosure ... 17

B.5.00 Information Quality ... 18

B.6.00 Collation and Analysis of Information ... 20
B.6.10 Collation and Analysis ... 20
B.6.20 Merging of Information From Different Sources ... 20

B.7.00 Sharing and Disclosure of Information ... 21
B.7.10 Sharing Information Within the Agency and With Other Justice System Partners ... 22
B.7.20 Sharing Information With Those Responsible for Public Protection, Safety, or Public Health ... 22
B.7.30 Sharing Information for Specific Purposes ... 23
B.7.40 Disclosing Information to the Public ... 24
B.7.50 Disclosing Information to the Individual About Whom Information Has Been Gathered ... 25

B.8.00 Information Retention and Destruction ... 26
B.8.10 Review of Information Regarding Retention ... 26
B.8.20 Destruction of Information ... 26

B.9.00 Accountability and Enforcement ... 27
B.9.10 Information System Transparency ... 27
B.9.20 Accountability for Activities ... 27
B.9.30 Enforcement ... 29

B.10.00 Training ... 29

C. Provisions for a Multiagency Agreement for an Information Sharing System ... 31

C.1.00 Statement of Purpose ... 31

C.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties ... 32

C.3.00 Sharing of Information Among Participants ... 32
C.3.10 Expectations Regarding Information Gathered and Shared ... 32
C.3.20 Sharing Information With Other Justice System Partners ... 33

C.4.00 Use and Disclosure of Information Originating From Another Participating Agency ... 33
C.4.10 Disclosure of Information According to the Originating Agency's Access Rules ... 33
C.4.20 Reporting Possible Information Errors to the Originating Agency ... 33

C.5.00 Participating Agency Accountability and Enforcement ... 34
C.5.10 Expectations Regarding Accountability and Enforcement ... 34
C.5.20 Enforcement of Provisions of Information Sharing Agreement ... 34

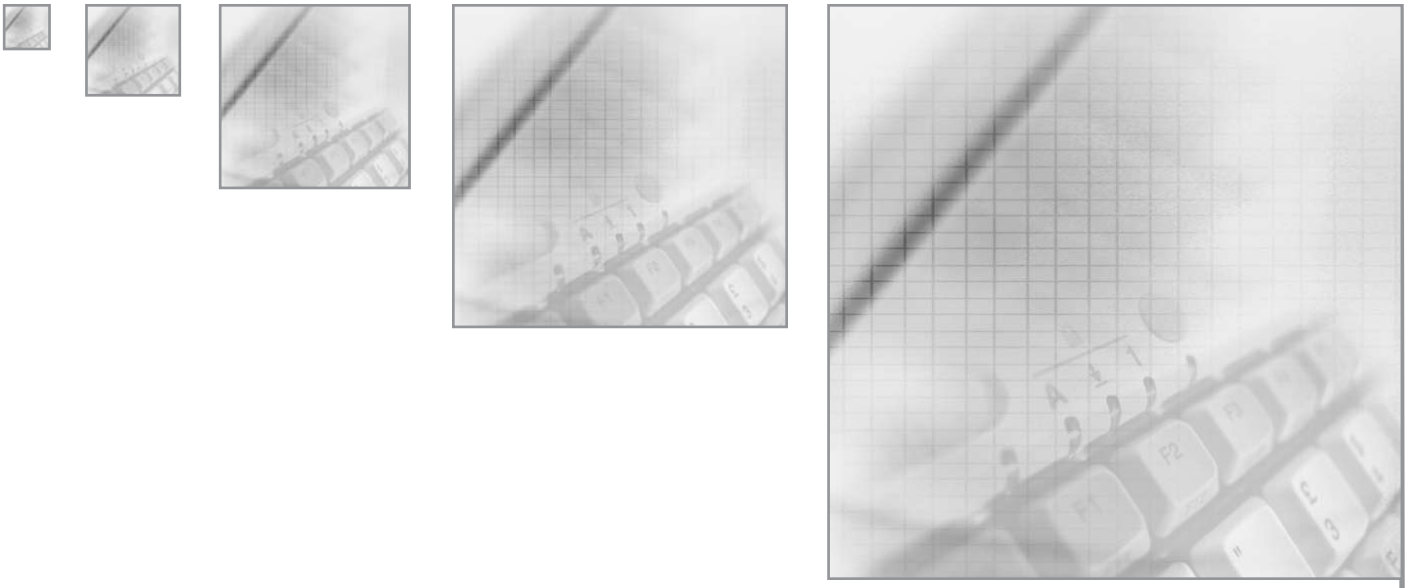
Appendix One—Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information ... 35

Appendix Two—Local, State, Tribal, and Territorial Laws Possibly Relevant to Seeking, Retaining, and Disseminating Justice Information ... 37

Appendix Three—Bibliography for Sources and References ... 39

Appendix Four—Index of Subjects ... 41

Appendix Five—Cross-reference To Privacy-related Laws And Other Policies ... 43



Acknowledgements

Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems is a product of the U.S. Department of Justice's (DOJ) Gloval Justice Information Sharing Initiative (Global) and was developed with the assistance of two of Global's working groups and individuals from several organizations and in partnership with the Justice Management Institute (JMI).

The policy templates presented here were drafted based on the shared wisdom, experiences, and comments of the justice practitioners and industry professionals who were members of the Global Intelligence Working Group and the Global Privacy and Information Quality Working Group. A special thank-you is expressed to the members of these two working groups and to Alan Carlson for contributing to and supporting this document.

Members of the Global Intelligence Working Group

Jack Anderson
Orange County Sheriff's Department
Norwalk, California

Maureen Baginski
Federal Bureau of Investigation
Washington, DC (retired)

William Berger
North Miami Beach, Florida, Police Department
Miami, Florida

Kenneth Bouche
Illinois State Police
Chicago, Illinois

Donald Brackman
National White Collar Crime Center
Richmond, Virginia

Ledra Brady
U.S. Drug Enforcement Administration
Quantico, Virginia (retired)

Ron Brooks
Northern California HIDTA
San Francisco, California

Melvin Carraway
Indiana State Police
Indianapolis, Indiana
(No longer a member)

Steve Casteel
U.S. Drug Enforcement Administration
Arlington, Virginia

Henry Coffman
INTERPOL-USNCB
Washington, DC

Carlo Cudio
Monterey Police Department
Monterey, California

Michael Duffy
U.S. Department of Justice
Washington, DC

Edward Flynn
Massachusetts Executive Office of Public Safety
Boston, Massachusetts

Max Fratoddi
Federal Bureau of Investigation
Washington, DC (retired)

Thomas Frazier
Major Cities Chiefs Association
Baltimore, Maryland

Dennis Garrett
Arizona Department of Public Safety
Phoenix, Arizona (retired)

Bart R. Johnson
New York State Police
Albany, New York

Vernon Keenan
Georgia Bureau of Investigation
Decatur, Georgia

Phil Keith
Knoxville Police Department
Knoxville, Tennessee (retired)

Gerard P. Lynch
Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network
Newtown, Pennsylvania
(Now Chief Executive Officer of Regional Information Sharing Systems® (RISS))

George P. March
Office of Information Technology
RISS
Thorndale, Pennsylvania

Ritchie Martinez
Arizona Department of Public Safety
HIDTA
Tucson, Arizona

Jerry Marynik
California Department of Justice
Sacramento, California

Miles Matthews
Counterdrug Intelligence Executive Secretariat
U.S. Department of Justice
Washington, DC
(No longer a member)

Kent Mawyer
Texas Department of Public Safety
Austin, Texas

Patrick McCreary
Bureau of Justice Assistance
Washington, DC

Peter Modafferi
Rockland County District Attorney's Office
New City, New York

Dennis Morton
National Drug Intelligence Center
Johnstown, Pennsylvania (retired)

Daniel Oates
Aurora Police Department
Aurora, Colorado

Thomas O'Connor
Maryland Heights Police Department
Maryland Heights, Missouri

Marilyn Peterson
New Jersey Division of Criminal Justice
Trenton, New Jersey (retired)

Joseph Polisar
Garden Grove Police Department
Garden Grove, California

Russ Porter
Iowa Department of Public Safety
Des Moines, Iowa

Louis Quijas
Federal Bureau of Investigation
Washington, DC

Richard Randall
Kendall County Sheriff's Office
Yorkville, Illinois

Steven Raubenolt
Office of the Attorney General
Columbus, Ohio

Edward Reina
Yavapai-Prescott Tribal Police Department
Prescott, Arizona

Richard Russell
U.S. Department of Homeland Security
Washington, DC
(Now with the ODNI)

Kurt Schmidt
Office of National Drug Control Policy
Washington, DC

Michael Schrunk
Multnomah County District Attorney's Office
Portland, Oregon

Richard Stanek
Minneapolis Police Department
Minneapolis, Minnesota

Gregory Stieber
U.S. Secret Service
U.S. Department of Homeland Security
Washington, DC
(No longer a member)

Mark Zadra
Florida Department of Law Enforcement
Tallahassee, Florida

Members of the Global Privacy and Information Quality Working Group

Francis X. Aumand III
Vermont Department of Public Safety
Waterbury, Vermont

Robert P. Boehmer
Institute for Public Safety Partnerships
University of Illinois at Chicago
Chicago, Illinois

David Byers
Arizona Supreme Court
Phoenix, Arizona

Alan Carlson
The Justice Management Institute
Kensington, California

Steven Correll
Nlets—The International Justice and Public Safety Information Sharing Network
Phoenix, Arizona

Cabell Cropper
National Criminal Justice Association
Washington, DC

Robert Deyling
Administrative Office of the United States Courts
Washington, DC

Owen Greenspan
SEARCH, The National Consortium for Justice Information and Statistics
Sacramento, California

Bob Greeves
Bureau of Justice Assistance
Washington, DC

Barbara Hurst
Rhode Island Office of the Public Defender
Providence, Rhode Island

John Jesernik
Illinois State Police
Joliet, Illinois

Rhonda Jones
National Institute of Justice
Washington, DC

Erin Kenneally
San Diego Supercomputer Center
La Jolla, California

Erin Lee
National Governors Association
Washington, DC

Hayes Lewis
American Indian Development Associates
Albuquerque, New Mexico

Thomas MacLellan
National Governors Association
Washington, DC

Ada Pecos Melton
American Indian Development Associates
Albuquerque, New Mexico

Wil Nagel
Illinois Criminal Justice Information Authority
Chicago, Illinois

Jeanette Plante
Office of Records Management Policy
Justice Management Division
U.S. Department of Justice
Washington, DC

Michael Ramage
Florida Department of Law Enforcement
Tallahassee, Florida

Anne Seymour
Justice Solutions, Inc.
Washington, DC

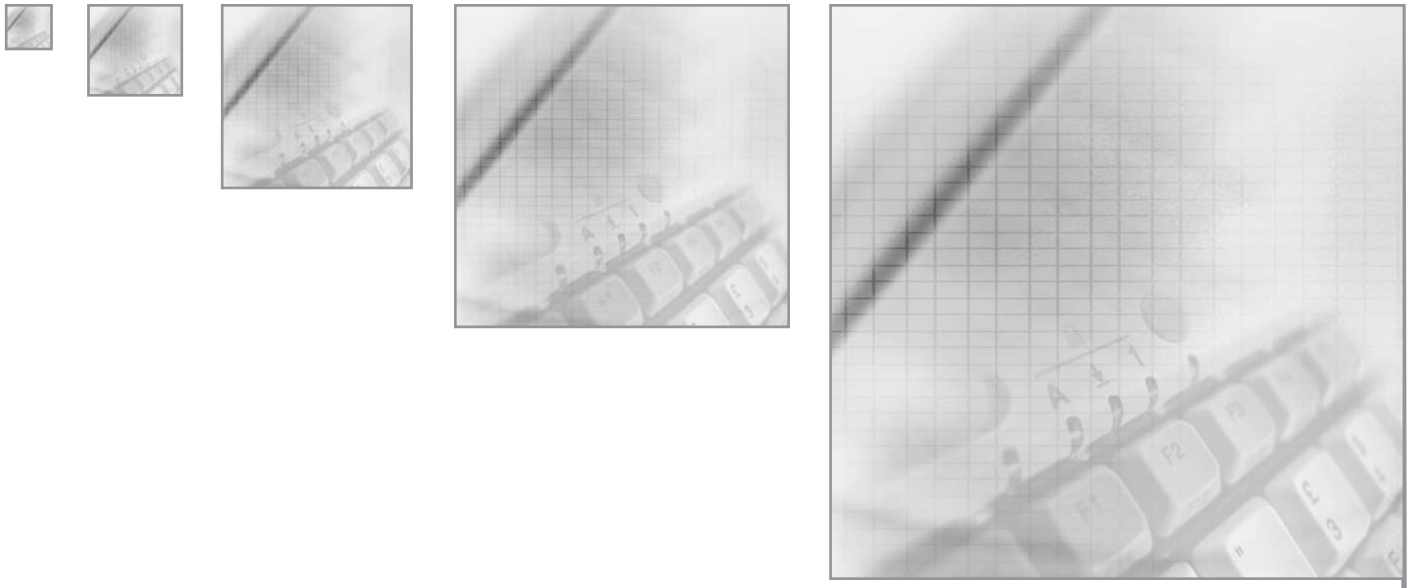
Steve Siegel
Denver District Attorney's Office
Denver, Colorado

Cindy Southworth
National Network to End Domestic Violence Fund
Washington, DC

Martha Steketee
Independent Consultant
Chicago, Illinois

Elizabeth Whitaker
Georgia Tech Research Institute
Atlanta, Georgia

Carl Wicklund
American Probation and Parole Association
Lexington, Kentucky



Preface

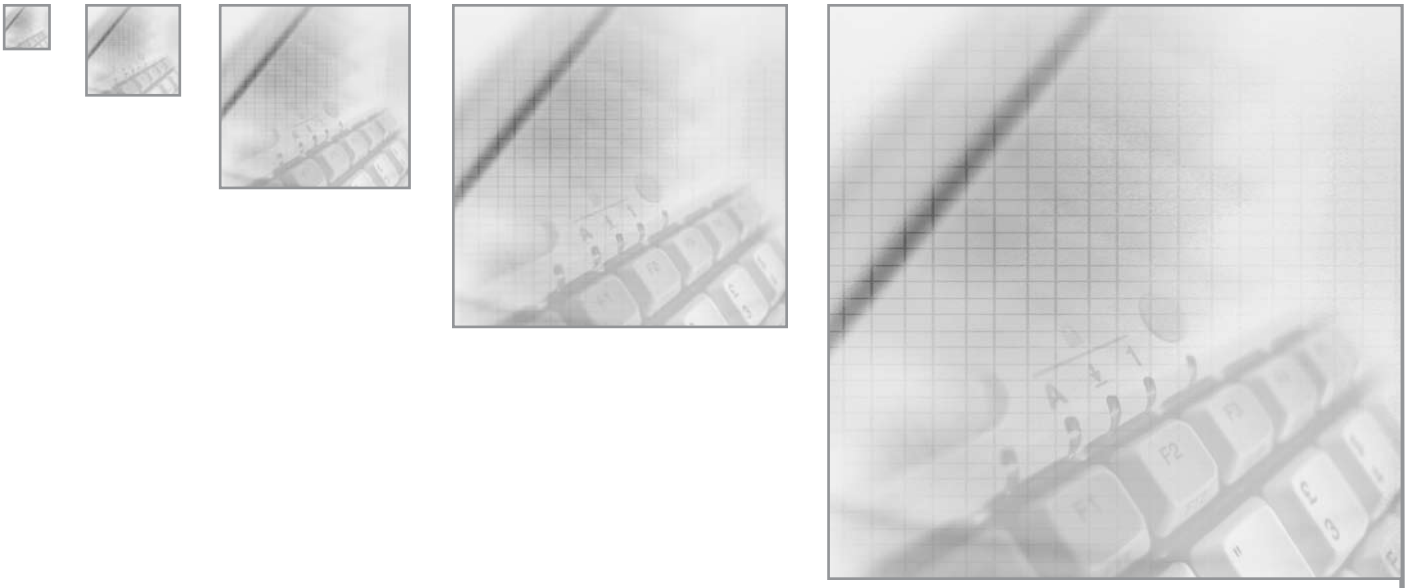
Quite simply, privacy may be one of the most important issues affecting the use of technology in the twenty-first century.

Responsively, the U.S. Department of Justice (DOJ), Office of Justice Programs, Bureau of Justice Assistance (BJA), is pursuing the best resources and recommendations from the field to further efficient, comprehensive, and appropriate sharing of information. These goals will be achieved by ensuring privacy and security protections are in place throughout the information exchange process, safeguarding the safety, health, and personal data of our nation's residents in the face of ever-advancing technologies.

A primary approach that BJA uses to explore key information sharing issues such as privacy (and arrives at associated recommendations) is through efforts of DOJ's Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC or "Committee"). The GAC is a volunteer group of high-level justice executives and practitioners representing over 30 key agencies across the justice and public safety landscape (and, by extension, 1.2 million justice practitioners). This group serves as the Federal Advisory Committee to the highest-ranking law enforcement official in the land, the U.S. Attorney General, on standards-based justice-related information sharing.

GAC-supported recommendations and resources are informed through a number of avenues: mainly via the work of the Global working groups but sometimes (as in this case) as a result of subject-matter experts' activities. Recognizing the need for a hands-on privacy policy tool, the Justice Management Institute (JMI) diligently pursued the crafting of *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* ("templates"). When the JMI templates were presented to the GAC for review and discussion, Global members enthusiastically recognized their value to the field. Subsequently, the templates were included in the Committee's catalogue of "recognized resources."

BJA and the GAC strive to coordinate product development complementarily, with individual products proving useful both on their own as well as when viewed as a suite of tools. Considering that approach, please see Appendix Three: Bibliography for Sources and References for additional information sharing-related resource suggestions (most are also referenced in the body of this document). The enumerated Global items as well as other valuable DOJ-supported tools are available on the OJP Information Technology Web site, located at http://it.ojp.gov. This appendix contains more information on the site and Global offerings.



Introduction

The atrocities of September 11, 2001, brought into focus the need to greatly improve our methods of gathering and sharing information on terrorists, criminal activities, and the individuals and organizations likely involved. It also highlighted the need to do so in an efficient manner, one that did not waste time and resources gathering irrelevant information, duplicating information already collected, or gathering information about people unlikely to be involved in illegal activities. Improving these capabilities would also enhance public confidence in the ability of the justice and public safety systems to protect people, property and, ultimately, our way of life. There are a number of aspects to improving our capacity to prevent harm, including taking advantage of new technology, making better use of existing technologies and systems, linking information systems, and improving our justice system policies and business practices.

One element of a more robust information gathering and sharing system is an up-to-date and comprehensive policy protecting individuals' privacy, civil rights, and civil liberties. Improved public safety does not have to come at the expense of these rights. Rather, public safety is further enhanced when individuals are sufficiently comfortable with the integrity of justice information system operations and therefore are willing to cooperate with and support them. Precisely drawn privacy, civil rights, and civil liberties protection policies thus contribute to a number of goals. First, such policies are legally required by the U.S. Constitution and state constitutions and other laws adopted over time that regulate life in our society and the operation of our public agencies. Second, a strong privacy policy is good public policy, because it is responsive to widely held public expectations about the collection and use of information about individuals and the fair and open operation of a democratic government. Third, it is the right thing to do.

Answering a Critical Need, Responding to the Field

The need for effective privacy policies has been consistently recognized in recent U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) efforts (detailed in the Preface) directed at the improvement of justice information gathering and sharing systems:

- It is succinctly summarized in *Privacy and Information Quality Policy Development for the Justice Decision Maker*;[1]
- It is supported by several recommendations of the *National Criminal Intelligence Sharing Plan* (NCISP);[2] and

1 Located at http://it.ojp.gov/documents/200411_global_privacy_document.pdf.
2 Located at http://it.ojp.gov/documents/ncisp/. Note: high bandwidth required.

- In response to a tremendous amount of requests from the field for assistance with the underlying process, the *Privacy Policy Development Guide and Implementation Templates*[3] ("Policy Guide") was assembled.

Building on these previous works and offering excellent supplementation to the Global Policy Guide, the objective of *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* ("policy templates" or "templates") is to provide policy templates that justice system practitioners can use to draft comprehensive policies to protect privacy, civil rights, and civil liberties principles applicable to their operations.

Audience

The policy templates were developed for use by law enforcement agencies, prosecutors, courts, or other justice system agencies or jurisdictions at the local, state, regional, tribal, territorial, or federal level. The templates were designed to cover a range of computer-based justice information systems, including:

- An incident- or event-based records management system (RMS);
- An offender-based information system (OBIS) or offender-based tracking system (OBTS);
- A case management system (CMS) used by an agency or court;
- An integrated criminal justice information system (often referred to as IJIS or CJIS) supporting the activities of several agencies and related courts;
- A criminal history record information (CHRI) system;
- A criminal intelligence gathering system (CIS);
- A corrections or jail management system (JMS); or
- A justice information sharing network through which information in one or more of the above systems is shared with users of all systems involved.

The policy templates are intended for systems that seek or receive, store, and make available information in support of activities associated with the justice system, public safety, and health communities. These include criminal investigations, crime analysis, law enforcement, prosecution, defense, courts, corrections, pretrial services, probation, parole, or other activities in support of the protection of public safety, health, or other matters handled through the justice system. Also included are prosecution of activities or circumstances involving violations of public health and safety laws, including zoning and environmental protection. The templates are relevant to the administration of justice, strategic and tactical operations, and national security responsibilities. Finally, the templates are intended to address all types of public safety and public protection risks and threats, whether criminal or from natural disasters.

Scope of Policy Templates

The policy templates proposed here are intended to protect more than just individual privacy. The templates are more comprehensive, addressing:

- Protection of ***privacy***;
- Protection of ***civil rights***;
- Protection of ***civil liberties***; and
- ***Information quality***, which enhances the above protections.

As used in these policy templates, key terms are defined as follows:

> "The term ***privacy*** refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. The U.S. Constitution does not explicitly use the word *privacy*, but several of its provisions protect different aspects of this fundamental right. Although there does not exist an explicit federal constitutional right to an individual's privacy, privacy rights have been articulated in limited contexts by the U.S. Supreme Court. [*Note: several state constitutions do contain explicit language regarding a right to privacy.*] Privacy protections are numerous and include protection from unnecessary or unauthorized collection of personal information (e.g., eavesdropping), public disclosure of private facts, and shame or humiliation caused by release of personal information." (*National Criminal Intelligence Sharing Plan* (NCISP), p. 6, emphasis added, footnotes omitted, and note addressing state constitutions added.)

> "The term ***civil rights*** is used to imply that the state has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and

3 Located at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

Fourteenth Amendments and by acts of Congress. Generally, the term *civil rights* involves positive (or affirmative) government action, while the term *civil liberties* involves restrictions on government." (NCISP, pp. 5–6, emphasis added.)

"The term ***civil liberties*** refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference . . . ." (NCISP, p. 5, emphasis added.)

Most state constitutions contain a statement of rights very similar to and sometimes broader than the Bill of Rights in the U.S. Constitution. It should also be noted that the Bill of Rights enumerated in the U.S. Constitution does not apply to American Indians when they are within Indian Country, although they are afforded the same protections under the Indian Civil Rights Act of 1968.

Information quality refers to various aspects of the information itself. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security,[4] and privacy. The issue of information quality is addressed more specifically in Section B.5.00 of this document. Readers wishing to further pursue the multidimensional aspect of the topic are encouraged to review Global's *Information Quality: The Foundation of Justice Decision Making*.[5]

While these templates address privacy, civil rights, and civil liberties, a review of the Table of Contents reveals sections addressing disclosure, public access, records retention, security, and data management issues.

- *Disclosure* is a subset of privacy, focusing on information that may be available only to certain people for certain purposes but which is not available to everyone.
- *Public access* relates to what information can be seen by the public, that is, information whose public availability is not subject to privacy interests or rights.
- Controlling who has access to information, whether public or internal, is one goal of *security provisions*.
- If information is not retained any longer than necessary under applicable *records retention* schedules, then there is no risk of improper disclosure after the records have been destroyed.

References to these topics are included in order to highlight the intersection of privacy, civil rights, and civil liberties interests with these operational aspects of justice system information sharing and management and because all the topics have implications for the protection of privacy, civil rights, and civil liberties.

Purpose of the Templates

It is important to understand what the policy templates are intended to do.

Existing federal and state constitutional provisions, statutes, rules, and regulations forbid certain conduct and prescribe what and how information can be collected. However, there are often gaps in these provisions—areas where agencies and individuals can exercise discretion about what to do or how to proceed. Agencies should consider adopting policies or practices regarding this discretion to provide more comprehensive protection of personal privacy, civil rights, and civil liberties. One objective of these templates, therefore, is to both identify and organize applicable laws and to indicate where an agency might need to consider adopting new or additional policies or practices.

Concepts Underlying Templates

These proposed policy templates are based on several fundamental concepts intended to improve the effectiveness and success of the justice information systems being developed. These basic concepts include:

- Supporting a proactive approach to managing the collection, use, analysis, retention, destruction, sharing, and disclosure of information.
- Making decisions that are deliberate and considered when collecting or receiving, using, analyzing, retaining, destroying, sharing, and disclosing information.
- Reinforcing appropriate conduct of individuals in the collection, use, analysis, retention, destruction, sharing, and disclosure of information that complies with applicable local, state, regional, tribal, territorial, and federal laws.

4 Please see Global's *Applying Security Practices to Justice Information Sharing* for more information on this topic. The resource is located at http://it.ojp.gov/documents/asp/. Note: High bandwidth required.

5 Scheduled for imminent release, to be posted at http://it.ojp.gov/global.

- Proposing policy language that is relevant to all levels of government—local, state, regional, tribal, territorial, and federal.

Organization of Policy Templates

The policy templates proposed here are designed for use by any one of several types of information gathering or sharing systems described in the Audience section. In order to accommodate all of the common approaches, three sets of policy template provisions are provided in this document:

1. Privacy and civil rights protection provisions for inclusion in enabling legislation or authorization for the justice information system (Part A);

2. A basic privacy and civil rights protection policy template covering the day-to-day operation of the justice information system (Part B); and

3. Privacy and civil rights protection provisions for an interagency agreement[6] between agencies participating in a justice information sharing network or system through which each participating agency will share information (Part C). One provision of the agreement would be that each of the participating agencies will have a basic privacy policy that contains provisions addressing the policies identified in Part B.

Each of the several common approaches of justice information systems[7] would require use of a different combination of the three policy parts contained in this template:

- **Local systems** that serve one agency or the agencies and courts of a city, county, or tribe should include policy elements in their enabling legislation (Part A) and adopt the basic policy (Part B). If the local system joined an information sharing system, an interagency agreement would be needed regarding the participation in the sharing system (Part C).

- **Statewide systems** that provide one of the several types of justice information systems for any agency in the state choosing to use it would need all three policy elements: enabling authority (Part A), a basic policy for the operation of the system (Part B), and an interagency agreement (Part C) signed by each participating agency.

- **A statewide network that integrates local systems** would need enabling legislation for the state-level system (Part A) and an interagency agreement with the participating agency systems (Part C).

- **Multijurisdictional information sharing systems** would need enabling authorization to establish the system (Part A) and an interagency agreement with the participating agencies (Part C). Regional systems could involve multiple jurisdictions across state lines, multiple jurisdictions within a state, or a combination of local, state, regional, tribal, territorial, and federal justice system agencies.

- **Ad hoc systems** that are created in response to an incident or event and will rely on existing information systems in the participating agencies would need an interagency agreement (Part C) tailored to the incident or event.

Format of Policy Templates

The policy templates proposed here contain two types of provisions.

1. There is language reflecting common practices. These are provisions that are straightforward and less controversial in nature, common across many states or across jurisdictions within a state or that incorporate federal provisions applicable to everyone.

2. There are provisions that typically are different in each local or state jurisdiction or where a local or state jurisdiction has unique or special requirements or limitations. These provisions must be tailored or augmented to reflect the specific local or state laws or practices. For these types of provisions, the templates include either alternate versions of common local or state policies or a statement in brackets indicating where local or state laws must be reviewed and reflected in the policy language. Examples include state constitutional or statutory provisions on what records are open to the public, limitations on what information can be sought or received, what methods can or cannot be used to seek or receive information, and records retention schedules.

Definitions of terms with a specific meaning in the policy templates are provided. These may need to be revised to reflect local definitions or terminology. Additional definitions may also need to be added for terms or phrases commonly used in a jurisdiction. Additionally,

6 Such agreements are referred to by a range of acronyms, depending on the state or type of agreement. Examples include IAA (Inter-Agency Agreement), JPA (Joint Powers Agreement), MOA (Memorandum of Agreement), or MOU (Memorandum of Understanding). In this document, "interagency agreement" is used as representative of all these terms.

7 For descriptions of four frequently used justice information systems models, see Chapter 3 of Global's *Applying Security Practices to Justice Information Sharing*, located at http://it.ojp.gov/documents/asp/. Note: High bandwidth required.

Appendix D of the Global Policy Guide[8] contains a glossary of terms and definitions readers may find helpful.

The proposed policy provisions are composed of three segments.

1. Each section begins with the actual policy language, the so-called "black-letter" language. This language is in bold type. It may include language that must be tailored to a jurisdiction's laws, noted in bold and italics within [brackets]. There may also be suggested additional provisions, also in bold and italics within [brackets].

2. Following the specific policy language is a Commentary segment that explains the meaning and intent of the black-letter language. The Commentary is in italics. The Commentary language would generally not be included in a policy but might be relevant to interpretations of the policy language once it is adopted and in use.

3. Finally, Appendix Five contains source and reference information for the language or concepts in each of the proposed sections. These include references to local, state, or federal statutes, regulations, or existing policies protecting privacy, civil rights, and civil liberties. There are also references to the relevant provisions from the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* promulgated by the European Organisation for Economic Co-operation and Development (OECD) and the Safe Harbor Privacy Principles developed by the U.S. Department of Commerce for compliance by U.S. companies with the OECD provisions. These are included because of the frequent reference to them in the field, although it must be noted that these provisions reflect European views of privacy, which are narrower than American views, and that the OECD Guidelines include a very broad law enforcement exception.

How to Use the Templates

The policy templates provided here are designed to provide both a framework for and the language of provisions to be included in enabling legislation, an operations policy, or an agreement between two or more governmental agencies (hereafter referred to as an interagency agreement). They cover the privacy, civil rights, and civil liberties sections that would be incorporated into a larger document containing other provisions regarding the establishment and operation of a justice information system. The intention is for the templates to be used as follows:

- The sections in Part A regarding the enabling authority would be included in the statute, ordinance, resolution, executive order, or other document that authorizes or creates the entity that will oversee the information system.

- The sections in Part B regarding basic system operation would be part of a general policy applicable to the system or become the central provisions of a stand-alone policy that covers protection of privacy, civil rights, and civil liberties.

- The sections in Part C could be included in an interagency agreement among all the participating agencies that form or join an information sharing network or would be an addendum or separate agreement signed by the participating agencies.

It is important to note that the policy template sections proposed are NOT intended to be used "as is" without modification. The objective of the templates is to provide suggested language for use in drafting a policy or an interagency agreement. In some sections, alternative language may be provided or alternatives or additions may be suggested in the commentary. One purpose of suggested alternative language is to raise issues that may be relevant in one jurisdiction but not another or that may be relevant for one type of justice information system but not another.

Steps for Editing the Template Language

One stage of the process[9] of drafting a policy or agreement involves an agency using the templates contained in this document to build a policy. An agency should take the following steps to adapt the language provided in the templates to its justice information system:

1. Clarify the type of justice information system that will be covered by the policy—is it for an RMS, CMS, CJIS, IJIS, JMS, criminal intelligence system, or a combination? The nature of the system will determine the applicable language in key elements (for example, the data collection threshold or the access and disclosure rules).

2. Determine what policy parts are needed based on existing laws and organizational structures. Is the enabling authority of Part A needed? Will the operating policy covered in Part B be a stand-alone

8 Located at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

9 For a more complete review of the privacy policy development process, see Global's *Privacy Policy Development Guide and Implementation Templates*, located at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

policy or be included in an existing policy? Are multiple agencies involved, suggesting the need for the interagency agreement proposed in Part C?

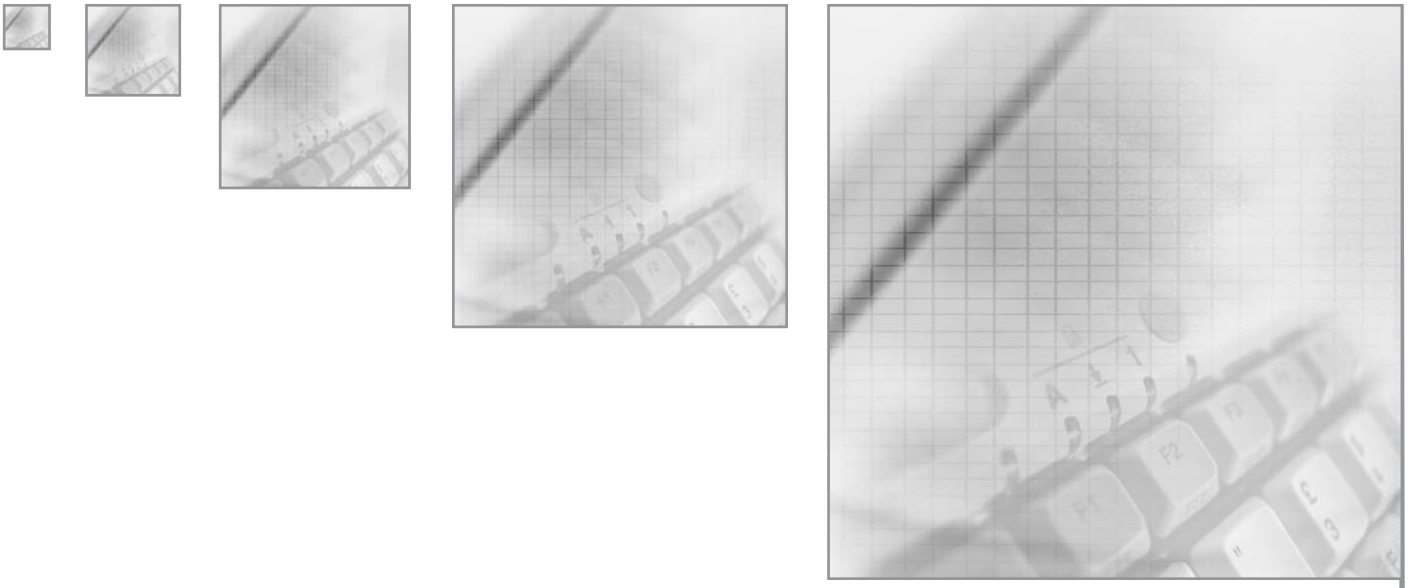
3. Based on these decisions, the agency(ies) should review and edit each section proposed for the Part(s) identified as needed in the previous step and:

   a. Modify the language of relevant sections to include the language of or reference to statutes, rules, standards, or policies applicable to the agency on the subject of each section. Usually, the places where editing is needed are indicated [in italics in brackets]. However, sometimes the general rule stated in the proposed section will also need to be edited to comport with the law in the jurisdiction. A decision must also be made about including suggestions for additional language that are in italics and [brackets] or in the Commentary. In some cases, there may be gaps where no applicable law exists and the agency will have to determine what policy it will follow. Note that it would be helpful to address these policy gaps at a state level in a way that assists local jurisdictions (particularly smaller jurisdictions) in developing more complete policies.
   b. Delete sections i) that are not relevant, based on the information collection and sharing laws applicable in the agency's jurisdiction, ii) that are not relevant to the type of information sharing system for which the policy is being drafted, or iii) that the agency chooses not to include.
   c. Add sections for provisions that are not addressed in the templates but are required by the jurisdiction's information collection and sharing laws.
   d. Change key terms to those applicable to the agency's jurisdiction, especially those that have specific legal meanings. For example, the official title of the agency should be inserted in the definition of "agency" in Section B.3.10, and the name of the information system substituted where indicated. Other examples would be terms defined under Section B.3.00 or legal standards such as those in Subsection B.4.20 (b).
   e. Add details to lists identified in [brackets] in the sections, for example, a list of types of stored information about an individual that are not to be disclosed to that individual pursuant to Subsection B.7.50 (b) (4).
   f. Where indicated, include contact data for the office or person able to answer questions or provide additional information.

During the development process, it is very useful for the drafting committee to keep a record (for example, in minutes) of discussions and options considered. This record can serve as valuable "legislative history" during subsequent interpretation of the policy. It also demonstrates the thoroughness of the drafting committee's considerations and documents any policy gaps addressed.

Once the editing has occurred and necessary additions and changes are made, the draft policy should be submitted to the oversight body. That body should tentatively adopt the draft and circulate it among stakeholders for comment. After comments are received, the draft should be modified based on the comments received and then adopted by the oversight body. For further discussion of the overall policy development process, see Global's *Privacy Policy Development Guide and Implementation Templates*.[10]

10 Located at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf.



A. Elements of Enabling Legislation or Authorization

The following provisions should be included in the instrument or document that authorizes the creation of and designates the oversight body for the justice information system. The instrument could be an enabling statute, resolution, ordinance, or executive order at the local, state, tribal, territorial, or federal level. Not all justice information systems have an explicit enabling document. However, the authority to create the system may be found, at least in part, in budget authorizations or laws describing the conduct of the system that imply its existence. It is generally more effective to have an explicit enabling statement for transparency and accountability purposes, as well as to clarify the goals and limitations of the system. The statement should contain broad, general principles, not details. The details should be in the operational policy that includes the provisions suggested in Part B.

A.1.00 Statement of Purpose

The goal of establishing and maintaining the [*add the name of the justice information system and specify what type of system is involved, for example, a records management system, case management system, integrated justice information system, or criminal intelligence system*] is to further the following purposes:

(a) Increase public safety and improve national security;

(b) Minimize the threat and risk of injury to specific individuals;

(c) Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;

(d) Minimize the threat and risk of damage to real or personal property;

(e) Protect individual privacy, civil rights, civil liberties, and other protected interests;

(f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

(g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;

(h) Support the role of the justice system in society;

(i) Promote governmental legitimacy and accountability;

(j) Not unduly burden the ongoing business of the justice system; and

(k) Make the most effective use of public resources allocated to justice agencies.

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

Commentary

This section identifies 11 interrelated purposes underlying the development and operation of any type of justice information system. Although some do not appear to directly relate to the protection of privacy, civil rights, and civil liberties, each contributes to the legitimacy of the system, thereby increasing a public sense of protection of these basic rights and interests.

These purposes will be achieved by a justice information system that provides complete, accurate, current, and timely information to justice system decision makers; improves the quality of justice system decisions; and increases the rate of apprehension and incarceration of offenders. Proper conduct on the part of individuals collecting information and who have access to information in the system furthers these purposes.

The purposes are not mutually exclusive, although some may be competing in some circumstances. They are not listed in priority order, although considerations of efficiency (Subsection (j)) and effective use of public resources (Subsection (k)) would not trump the interests in security, public and individual safety, and compliance with the law.

Subsection (a): Increase Public Safety and Improve National Security. The ultimate objective of a justice information system is to enhance public safety and improve the nation's security. This objective is accomplished by gathering and sharing information so as to increase the government's ability to detect, deter, defeat, and prosecute criminal, including terrorist, activities. This includes both reactive and proactive activities. Reactive activities include detecting, responding to, and investigating suspected criminal, including terrorist, activities and apprehending suspected criminals, prosecuting cases, and otherwise solving crimes. The expectation is that the prosecution of criminal acts will suppress future crimes, thereby improving public safety. Proactive activities include anticipating, identifying, deterring, preventing, and defeating potential criminal, including terrorist, activities. The expectation is that effective, integrated justice information systems will protect public safety and national security by preventing brutalities like the September 11, 2001, attacks or the Oklahoma City bombing.

Subsection (b): Minimize the Threat and Risk of Injury to Specific Individuals. Sometimes the gathering and sharing of information through a justice information system will identify a risk specific to an individual or group of people, as opposed to the public at large. Protecting individuals is a subset of public protection. Note that there are two aspects to this type of protection. One involves gathering and acting on information about a threat to a specific person, and the other involves protecting information in the justice information system about a specific person from disclosure that would endanger the person's safety. Personal safety can be enhanced by restricting access to information that could be used to injure someone physically, psychologically, or economically. Examples of potential injury to individuals based on information that could be in a justice information system include intimidation of or physical violence towards victims, witnesses, jurors, law enforcement, justice system personnel, or defendants, as well as repeated domestic violence or sexual assault, stalking, and identity theft.

Subsection (c): Minimize The Threat And Risk of Injury to Law Enforcement and Others Responsible for Public Protection, Safety, or Health. Another subset of public safety relates to the risk to law enforcement personnel and other public safety and protection personnel. Information gathered and kept in a justice information system can be used to identify threats and prevent injury to those responding to criminal incidents, natural disasters, or health emergencies of any type.

Subsection (d): Minimize the Threat and Risk of Damage to Real or Personal Property. Criminal, including terrorist, activities can also threaten or damage property. Gathering, analyzing, and sharing information can therefore also protect property or minimize loss to property resulting from criminal, including terrorist, activity. There is an additional aspect to this—protection of critical infrastructure. Justice system information can detect and reduce threats to public safety, public health, and our way of life resulting from the crippling or destruction of infrastructure such as power and water systems and transportation corridors or from the use of chemical and biological weapons.

Subsection (e): Protect Individual Privacy, Civil Rights, Civil Liberties, and Other Protected Interests. There are two aspects to this purpose. One relates to the role of government and the other to how government agencies conduct themselves. One role of the government is to protect individuals' privacy, civil rights, and civil liberties; this is one aspect of public safety. The interest in privacy is protected by preventing inappropriate disclosure of certain kinds of information. Civil rights are obligations imposed upon government to promote equality. The state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other irrelevant characteristics. Justice information systems can assist

agencies in this affirmative duty to protect individuals. The second aspect requires agencies to go about their work in a lawful manner. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference in the conduct of their lives.

Protecting and respecting privacy, civil rights and civil liberties also contributes to public trust and confidence that the justice system understands its role and promotes the rule of law.

Finally, it is important to remember that not everyone cataloged in a justice information system is a criminal. As part of protecting public safety, the justice system will collect and maintain information about victims, witnesses, and those who provide information to or come to the attention of the justice system. Erroneous information may have also been collected about someone, as when the wrong identity is given or assumed about someone being investigated, arrested, or otherwise associated with suspected criminal activity. Care should be taken that the privacy rights and interests of such third persons are not compromised by inappropriate collecting, storage, and disclosure of information in the justice information system.

Subsection (f): Protect the Integrity of the Criminal Investigatory, Criminal Intelligence, and Justice System Processes and Information. Creating and maintaining a justice information system should support justice processes, not undermine them. The activities associated with a justice information system and the collection, storage, analysis, and sharing of information should contribute to the integrity of the result. This will occur if the operations are conducted in a lawful manner and the outcomes are—and appear to be—just. The integrity of the system is enhanced when the information collected is relevant to the role of the system and is of high quality and when disclosure is properly managed so as not to compromise ongoing investigations or monitoring of activities.

Subsection (g): Minimize Reluctance of Individuals or Groups to Use or Cooperate With the Justice System. Individuals and groups will use and cooperate with justice system agencies if they perceive them to be lawful and effective. People will be reluctant to use or support the justice system if they perceive that the information gathered is irrelevant, that public officials are operating "outside the law," or that the information is gathered in a manner that puts people at risk of harm or disrespects their rights or privacy interests. There may also be an unintended effect of encouraging use of alternative solutions, whether in the form of self-help or extra-judicial actions. Conversely, people will have confidence in and will support a justice system that protects them and does so in a manner that respects the law.

Subsection (h): Support the Role of the Justice System in Society. The role of the justice system is to protect the public and prevent crimes, including terrorism. A justice information system should support this role by increasing the effectiveness and efficiency of the justice system in achieving a just result.

Subsection (i): Promote Governmental Legitimacy and Accountability. The operation of the justice information system must enhance accountability and promote legitimacy. In order for people to assess accountability, they must be aware of the existence of the justice information system and be able to evaluate the efficacy of its operations. This requires both openness and accountability regarding the operation of the justice information system. Violations of the operating policies of the system must be identified and appropriate sanctions enforced. Having operational policies available to the public, monitoring performance and compliance, and enforcing the policies promote accountability. A justice information system that integrates privacy and security protections and can document activity can be held accountable. These capabilities also promote greater public trust and confidence in the justice system, giving it greater legitimacy.

Subsection (j): Not Unduly Burden the Ongoing Business of the Justice System. The policies and operation of a justice information system should not unduly burden the justice system in fulfilling its fundamental role of protecting the public and individuals. Keeping too much or irrelevant information will not only be unhelpful, it may even impede work. Unnecessary or improper disclosure of information may also impede operations or diminish the integrity of investigations.

Subsection (k): Make the Most Effective Use of Public Resources Allocated to Justice Agencies. Sharing information leverages those public resources allocated to law enforcement and national security in several ways. Maintaining accurate, complete, and timely information in a justice information system reduces the waste of public resources from chasing false leads, duplicate information collection and entry, and erroneous linking of information from several sources. A robust information sharing system will also allow the larger justice system to "connect the dots" in ways that have not previously been possible.

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

A.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

(a) The [*add the name of the justice information system governing body*] and all participating agencies, employees, and users will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

(b) The [*add the name of the justice information system governing body*] will adopt internal operating policies requiring compliance with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information in the system.

Commentary

These provisions provide an explicit commitment by the agency and key participants to comply with all laws protecting privacy rights, civil rights, and civil liberties of individuals and organizations about whom the agency or users may collect and share information. The term "applicable" is included to confirm that the laws to be followed are those that apply to the agency and its personnel; there is no intent to subject the agency and its personnel to laws that would not otherwise cover the agency.

Subsection (b) requires the agency to adopt operational policies governing the information sharing system and its operations protecting privacy, civil rights, and civil liberties. Since this provision is intended to be in the enabling legislation, it is stated broadly. There may be a large body of law, whether legislative or judicial in origin, that specifies in detail what this provision means. These should not be listed here; rather, the requirements should be incorporated into the provisions in Part B.

A.3.00 Agency Transparency and Accountability

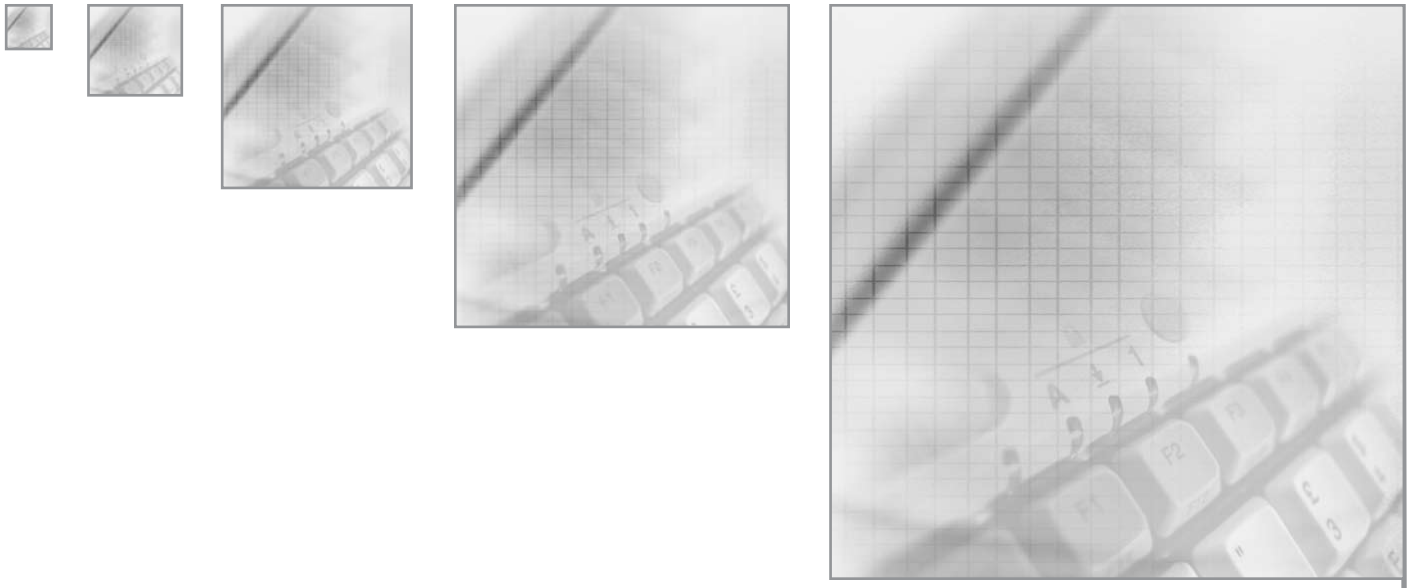
(a) The existence of the [*add the name of the justice information system*] will be made public and the systems policies on protection of privacy, civil rights, and civil liberties will be made available to the public on request and through any public Web site providing information about the system.

(b) The [*add the name of the justice information system governing body*] will adopt provisions to ensure accountability for compliance with all applicable laws and policies in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

Commentary

Making the existence of the justice information system public contributes to the credibility and legitimacy of the agency and information system by demonstrating that the agency has nothing to hide and is amenable to appropriate public oversight. It thus promotes purposes (g), (h), and (i) of Section A.1.00. Operators of criminal intelligence systems may want to consider the extent to which the existence of the system is made known publicly, recognizing that public disclosure that occurs only when a problem is publicized often exacerbates public concerns.

Subsection (b) states that the agency will be accountable for the use of the system and in its operation. Applicable laws and policies include local, state, tribal, territorial, or federal statutes, regulations, rules, court decisions, and policies.



B. Elements of a Basic Internal Operations Policy

The objective of an operations policy protecting privacy, civil rights, and civil liberties is to provide justice agency personnel, contractors, and users with guidelines and principles regarding the collection, analysis, use, retention, destruction, sharing, and disclosure of information kept in any type of justice information system. The provisions suggested in this part are intended to be incorporated into the general operating policies applicable to the justice information system or can form the substantive core of a stand-alone policy covering privacy, civil rights, and civil liberties. These provisions are intended to provide explicit and detailed guidance to agency personnel and other users about what the applicable laws offer or require for each of the topics covered.

Following the statement of purpose and definition sections, the policy elements are arranged in the order in which information is generally handled in a system. The template begins with the collection of information and then addresses analysis, use, dissemination and access, and retention. In addition, there are provisions related to the administration of the system, including agency accountability, policy enforcement, and the training of personnel.

B.1.00 Statement of Purpose

The goal of establishing and maintaining the [*add the name of the justice information system and specify what type of system is involved, for example, a records management system, case management system, integrated justice information system, or criminal intelligence system*] is to further the following purposes:

(a) Increase public safety and improve national security;

(b) Minimize the threat and risk of injury to specific individuals;

(c) Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;

(d) Minimize the threat and risk of damage to real or personal property;

(e) Protect individual privacy, civil rights, civil liberties, and other protected interests;

(f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

(g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;

(h) Support the role of the justice system in society;

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

(i) Promote governmental legitimacy and accountability;

(j) Not unduly burden the ongoing business of the justice system; and

(k) Make the most effective use of public resources allocated to justice agencies.

Commentary

See Commentary under Section A.1.00 in Part A.

B.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

All participating agency personnel, personnel providing information technology services to the agency, private contractors, and users will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

Commentary

See Commentary under Section A.2.00 in Part A.

B.3.00 Definitions

The sections in this subpart provide definitions for words or phrases regularly used in this policy to explain their meaning in the context of this policy. An agency may want to (or need to) define other terms. References to definitions of other terms used in local, state, or federal laws or policies are provided in Appendix Five. While these definitions are stated only in Part B, it may be appropriate to include these definitions in documents containing language from Part A and Part C.

B.3.10 Definition of Agency

***Agency* refers to [*state the official title of the agency or agencies to which this policy applies*].**

B.3.20 Definition of Information

***Information* includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.**

Commentary

Information is defined because the handling of information is the essence of the policy. The definition is very inclusive, because the policy is intended to apply to all types and manner of information sought and retained by an agency, not just information specific to an individual, often referred to as personally identifiable information. Civil rights laws and the integrity of the justice information system implicate the processes and practices of seeking and retaining information as much as the retaining and disclosure of information about a specific individual.

Information can exist in many different mediums and may simultaneously exist in more than one medium. The medium can be physical, hard-copy, or an electronic form. It includes documents, writings, electronic representations of text or graphic documents, and electronic images (including a video image) of a document, evidence, an object, or an event. It also includes information in the fields or files of an electronic database, an audio or video recording (analog or digital) of an event, or notes in an electronic file from which a transcript of an event can be prepared.

B.3.30 Definition of Law

As used in this policy, *law* includes any local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order, as construed by appropriate local, state, tribal, territorial, or federal officials or agencies.

Commentary

In the interest of generating a comprehensive privacy and civil rights policy, the definition is very broad, including items that may not be considered laws in a particular jurisdiction. It includes not only statutes or laws adopted by legislative bodies but also regulations and orders issued by an executive branch agency and decisions, rules, and orders of the judicial branch. The definition could also refer to policies adopted by any of the three branches, if any such policies exist and are relevant to the justice information system. Finally, it includes judicial interpretations, through case decisions, of the meaning or application of statutes and regulations.

B.3.40 Definition of Public

Public **includes:**

(a) Any person and any for-profit or nonprofit entity, organization, or association;

(b) Any governmental entity for which there is no existing specific law authorizing access to the agency's information;

(c) Media organizations; and

(d) Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public **does not include:**

(e) Employees of the agency;

(f) People or entities, private or governmental, who assist the agency in the operation of the justice information system; and

(g) Public agencies whose authority to access information gathered and retained by the agency is specified in law.

(h) [*Consider adding, if bulk release of information is permitted (see Subsection B.7.40 (e)): Public or private entities of any type, whether for-profit or nonprofit, that are authorized by law and obtain requisite permission to receive information in bulk from the agency.*]

Commentary

This definition is included for use in applying the sections providing for access to information by the public (see Section B.7.40).

Subsection (b) states that if there are no explicit provisions applicable to a governmental entity authorizing access and use of the information in the system, the employees of the agency will be treated as members of the general public for purposes of this policy.

Subsection (d) refers to entities that acquire information from many sources and compile them into a database to which their clients direct queries. Examples include credit bureaus, background screening entities, and other commercial database services.

Subsections (e) to (g) describe entities or individuals not defined as public.

Subsection (e) distinguishes agency employees from the public, as employees' access would be covered by Section B.7.10.

Subsection (f) includes other governmental entities, as well as private contractors, who provide services to the agency for the operation of the information system.

Subsection (g) addresses those situations where there is existing law or another policy that governs access to information by the employees of a particular public agency.

Subsection (h) is proposed for those jurisdictions that are authorized by law to release in bulk, to public or private entities, information in the system, including personally identifiable information for matching purposes. See proposed Subsection B.7.40 (e) regarding authority to release information in bulk.

B.4.00 Seeking and Retaining Information

The sections suggested in this subpart relate to the gathering of information and its retention by the agency. The provisions address 1) what information the agency is authorized to seek and retain, 2) what it is prohibited from seeking or retaining, and 3) what methods are permitted for seeking information. Issues associated with receiving information from third parties, including unsolicited information such as tips, is also addressed. Finally, there are provisions about categorizing information with respect to its validity, reliability, and access or disclosure.

B.4.10 What Information May Be Sought or Retained?

(a) This agency will seek or retain only information:

(1) [*for a records management system, case management system, jail management system, or other type of justice information systems, state the standard governing what information may be sought or received and retained in the system, for example:*] Relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; the prevention of crime; or that is useful in crime analysis or in the administration of criminal justice.

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

(2) [*for a criminal history record system*] Collected by criminal justice agencies on specific individuals, consisting of official identifiable descriptions and notations of arrests, detentions,warrants, complaints, indictments, information, or other formal criminal charges and any disposition relating to these charges, including acquittal, sentencing, pre- or postconviction supervision, correctional supervision, and release, but not [*include any exceptions describing information that will not be kept in the system, for example, fingerprint records where such information does not indicate the individual's involvement with the criminal justice system*].

(3) [*for a criminal intelligence system*] Where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity.

(b) This agency will not seek or retain information about an individual or organization solely on the basis of their religious, political, or social views or activities; their participation in a particular organization or event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

(c) This agency will not seek or retain information about the political, religious, or social views; participation in a particular organization or event; or activities of any individual or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation unless such information is:

(1) Relevant to whether an individual or organization has engaged in, is engaging in, or is planning a criminal (including terrorist) activity; or

(2) Needed by the agency:

i) To identify an individual,

ii) In order for the agency to operate effectively, or

iii) To provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.

(d) The agency shall keep a record of the source of all information retained by the agency.

Commentary

This section addresses the content of information as opposed to the means by which the information is acquired (see Section B.4.20). The intent of this section is to explicitly state the rules the agency will follow regarding what information it may or may not seek or retain. It addresses:

- *What information the agency is authorized to seek and retain;*
- *Limitations on what information can be sought and retained; and*
- *What information the agency is prohibited from seeking and retaining.*

Note that the section refers to information sought or retained by the agency. The template language here applies to information contained in a justice information system, that is, information in electronic form. However, the standards stated in the section could apply equally to information in paper form.

The language of this section uses the phrase "seek or retain"[11] because the focus is on the actions of the agency, not of others. Laws that authorize or limit the actions of the government apply when the agency takes action, not when it passively receives information (addressed in Subsection B.4.20 (b)). However, such information, even if unsolicited, cannot be kept unless the appropriate legal standard is met for retaining information.

Subsection (a) states the standard for seeking and retaining information for the type of justice information system covered by the policy. An agency may have different standards for different types of information. If the policy will apply to more than one type of system, this section should include subsections stating the standard for each type of system.

Subsection (a) (1) states a standard for basic RMS, CAD, CMS, JMS, CJIS, or IJIS systems. The language is general and fairly broad in scope.

11 Federal regulations for criminal history records systems use the terms "collecting, storing and disseminating" (28 CFR 20.20(a)), and the regulations for criminal intelligence systems use the terms "collect and maintain" (28 CFR 23.20(a)).

Subsection (a) (2) states a standard for criminal history record systems. It is based on, but not exactly the same as, the definition in the National Crime Prevention and Privacy Compact, 42 U.S.C. §14616, repeated in 28 CFR Part 20, Section 20.3(d). Language suggested here that is not in the CFR section is indicated in italics.

Subsection (a) (3) states a standard for criminal intelligence systems. The language is derived from, but not identical to, 28 CFR Part 23, Section 23.20(a). Language suggested here that is not in the CFR section is indicated in italics. Note that the language an agency adopts must comply with 28 CFR Part 23, if applicable.

Because it also covers the retention of information, the standard in Subsection (a) should also be augmented to address what can be done with information that is received by the agency but was not actively sought. There is often a basis to seek or receive additional information when reasonable suspicion or probable cause has not yet been established (for example, to follow up on an anonymous tip). The standard needs to address the temporary retention and subsequent disposition of information that is received by the agency, along with any further information sought or received by the agency during the review of the unsolicited information but that is subsequently determined not to meet the agency standard for retention. Such information should be kept only long enough to determine whether it can appropriately be retained, and if not, it should be archived or destroyed in accordance with the applicable law or agency policy.

Subsection (b) states that the agency will not seek or receive any information about an individual or organization just because of the individual's or organization's political or religious views or because an individual participated in a particular association or event. Doing so would violate state, tribal, territorial, and federal laws about freedom of religion and association and equal protection. For example, information could not be collected and kept about individuals solely because they belonged to a particular church or had participated in a particular demonstration.

Subsection (c) prohibits an agency from collecting specific types of information about an individual or organization. The types of information that cannot be retained relate to protected activities, such as religion, political affiliation, and membership in an association. A list of local, state, tribal, territorial, and federal laws that might contain statements of information that cannot be collected is provided in Appendices One and Two.

Subsection (c) is not intended to prevent gathering and use of information that is relevant to justice purposes (Subsection (c) (1)) or the agency's operation (Subsection (c) (2)). For example, it does not prevent gathering of information about an organization or its members if the organization is engaged in criminal activity, even if the criminal activity is not the main purpose of the organization. Similarly, it would not prevent the gathering of such information if it is relevant to investigating or preventing criminal, including terrorist, activity—for example, information about witnesses, victims, family members, or associates concerning their credibility or that relates to an element of the crime (such as a hate crime). It also does not prevent an agency from collecting such information if it is needed by the agency to do its work, for example, noting an individual's race for identity purposes or a correctional facility collecting information on the religious practices of those in its custody.

Subsection (d) requires the agency to maintain information about the source of information that it keeps. Source information is relevant to categorizing information regarding its reliability and validity pursuant to Subsection B.4.30 (a). This is also necessary in order to assess, including during an audit, whether the collection of information has been in compliance with this policy and applicable laws. Note that the rules regarding access to and disclosure of source information may be different from the rule about the information provided by the source.

B.4.20 Methods of Seeking or Receiving Information

(a) Information gathering and investigative techniques used by this agency will comply with all applicable laws.

(b) This agency will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernment information provider, who may or may not receive a fee or benefit for providing the information, if the agency knows or has reason to believe that:

- **(1) The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the agency [*include any exceptions regarding illegally obtained information*];**
- **(2) The individual or information provider used methods for collecting the information that the agency itself could not legally use [*include any exceptions regarding illegally obtained information*];**
- **(3) The specific information sought from the individual or information provider could not legally be collected by the agency; or**

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

(4) The agency has not taken the steps necessary to be authorized to collect the information.

(c) Information gathering and investigative techniques used by this agency will be no more intrusive or broadscale than is necessary in the particular circumstance to gather information it is authorized to seek or retain pursuant to Section [*B.4.10*].

Commentary

This section addresses the means of seeking and receiving information as opposed to its content (see Section B.4.10). It expressly states that information gathering will be done in a manner consistent with applicable laws. The limitations relate to both the method or technique of collection (Subsections (a) and (b)) and the breadth of the inquiry or search (Subsection (c)).

Subsection (a) states the general principle that information gathering techniques and methods will comply with applicable law. Federal laws that guide or limit information collection techniques by governmental agencies are identified in Appendix One. There may also be local, state, tribal, or territorial laws that guide or limit information collection techniques by governmental agencies. Lists of possible state laws, topics, and activities that may be covered by state laws are provided in Appendix Two.

By implication, this section also requires the agency to delete information that is subsequently found to have been obtained unlawfully (see Subsection B.5.00 (c) regarding deleting information).

Subsection (b) addresses information from nongovernmental sources, both individuals and third parties. This would include unsolicited information as well as that actively sought by the agency. Unsolicited information would include information received anonymously. Actively sought information would include that from organizations which maintain and make available information about individuals or organizations such as credit agencies or other information brokers. It would also apply to information obtained through the Internet using a search engine. The intent of the subsection is to prevent an agency or its personnel from circumventing the law applicable to it by using an individual or a nongovernmental, third-party source to obtain information.

Subsection (b) states a general requirement that information sought or received from an individual or nongovernmental source must have been obtained legally by the source and in a manner consistent with the agency's information gathering authority and limitations. No detailed legal standard or procedure is specified as to how it is to be established that the information was obtained appropriately and legally by the third party beyond the reference in Subsection (b) to "knows or has reason to believe." In a situation where the information is of a nature or type that the agency itself could not lawfully obtain directly, the agency personnel receiving the information should ascertain whether the information was obtained legally by the third party and that it is legal for the third party to provide the information to the agency. Sometimes, it may not be apparent how the information was obtained or whether it was obtained legally. Finally, Subsection (b) makes it clear that whether or not the third party received a fee or other benefit for the information is not relevant to whether the agency can seek and retain the information.

Subsection (b) (1) provides that the agency cannot use information from this source if it is unlawful for the individual or information provider to obtain the information or to share the information with the agency.

Subsection (b) (2) precludes an agency from obtaining information from third parties who used information gathering methods that the agency itself could not use. Unfortunately, the application of this concept is not as simple as it might appear. For example, what is to be done with an anonymous tip? In this type of situation, the agency can certainly use the information as a basis to investigate further, but the information should not be retained in the justice information system without having met the necessary standard or predicate specified in Subsection B.4.10 (a). A more problematic example involves criminal informants or cooperating defendants who often offer information that was not legally obtained but can be used by law enforcement as long as law enforcement did not direct them to illegally obtain the information. An agency may want to include some sort of exception in this section that states the agency's policy regarding such circumstances.

Subsection (b) (3) prevents an agency from getting information from a third party if it could not get the information itself. The section does not prevent an agency from getting information from a third-party source who has aggregated information from many sources, as long as the source obtained the information lawfully and the agency could lawfully gather the specific pieces of information sought. While the agency itself might not be able to lawfully aggregate information on people or organizations the way an information provider can, if the agency itself could have gathered the specific information about an individual or organization, it can get

the information from the provider under this subsection. Note that the agency should not ask or encourage information to be aggregated if the agency could not collect and aggregate the information itself.

Subsection (b) (4) requires the agency to comply with applicable procedures for obtaining authority to collect information. For example, if a search warrant is required to gather certain information, this provision requires the agency to obtain a proper warrant, even if the information will be provided by a third party.

Subsection (c) states the principle that information gathering will only be as broad as necessary to gather relevant information. Overly broad or intrusive methods are discouraged. Overbroad gathering increases the risk of invading privacy and infringing civil rights and civil liberties, as well as wasting limited agency resources, discouraging cooperation, and undermining the legitimacy of the agency. There may be existing laws or policies regarding specific information gathering techniques, such as for wiretapping, that should be referenced here.

One aspect of seeking and receiving information that is implicated by this subsection is the scope of aggregation of information about people or organizations in a justice information system. A typical system covered by this template represents an aggregation of information about people, organizations, events, property, etc. The collected information may or may not have been readily searchable before being put in electronic form. Once in electronic form, the ability to rapidly search and analyze the information increases the concern about whether the aggregation is legal, reasonable, and cost-effective. The agency should evaluate the scope of the information sought and retained in the aggregate and the accumulation in the entire justice information system, as well as at each stage of gathering each item of information.

B.4.30 Classification of Information Regarding Validity and Reliability

(a) At the time of retention in the system, the information will be categorized regarding its:

(1) Content validity;
(2) Nature of the source; and
(3) Source reliability.

(b) The categorization of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

Commentary

The objective of categorization is to let subsequent users assess the extent to which they can rely on the information. The expectation is that when the information is first retained, it will be coded as to its content validity and source reliability. The section applies to law enforcement, criminal intelligence systems, and other systems in which the person reviewing the information needs to know about its validity and reliability. It does not apply to systems, such as a court case management system, in which validity and reliability are addressed more openly, for example, in a court hearing.

Subsection (a) (1), content validity, has to do with the accuracy or truth of the information itself, as opposed to its source.

Subsection (a) (2), nature of the source, provides an indication of the type or nature of the origin of information. Examples of categories characterizing the source of the information could include 1) an anonymous tip, 2) an informant, 3) law enforcement interviews of individuals—in particular a victim or witness, 4) a public records source, 5) a nongovernmental information provider, etc.

Subsection (a) (3), source reliability, addresses the consistency of the content validity of information obtained from a particular source over time.

Subsection (b) requires updating of the categorization of information when new information clarifies the validity or reliability of previously retained information. This is a significant requirement that may be difficult to maintain when the amount of information in the system is extensive, which may be the case in a typical justice information system, particularly after it has been in use for a period of time. Updating the validity, source, or reliability coding may then only occur as users analyze information in light of new information, but not every time information is added to the system. There is also an issue if the volume of information being added is such that users do not take the time to properly code the information at the time of initial entry because it is too time-consuming. Entering and updating reliability and validity codes is more important in a criminal intelligence system where there is a higher standard regarding when information can be kept.

B.4.40 Classification of Information Regarding Limitations on Access and Disclosure

(a) At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:

(1) Protect confidential sources and police undercover techniques and methods;

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

(2) Not interfere with or compromise pending criminal investigations;
(3) Protect an individual's right of privacy and civil rights; and
(4) Provide legally required protection based on the status of an individual as [*indicate classes of individuals accorded protection regarding access to or disclosure of sensitive information, for example, as a victim of crime or domestic violence or as a witness*].

(b) The classification of existing information will be reevaluated whenever:
(1) New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
(2) There is a change in the use of the information affecting access or disclosure limitations.

(c) The access classifications will be used to control:
(1) What information a class of users can have access to;
(2) What information a class of users can add, change, delete or print; and
(3) To whom the information can be disclosed and under what circumstances.

Commentary

This section requires an explicit classification of information as to the ability of any particular class of persons to access the information or of the agency to disclose the information. This is one of the primary mechanisms for implementing many of the purposes stated in Section B.1.00. The section requires the classification to "attach" to the information when a decision is made to retain the information in the justice information system. The classification could be a flag or field associated with the information, such as some form of XML tag.

Access categorization can be subject to abuse because it allows information to be hidden from view. It should not be used to limit access to information to 1) conceal errors or sloppiness in entering or categorizing information, 2) conceal incompetence or violations of law in seeking or retaining information (for example, for political purposes), 3) prevent embarrassment to a person or agency, or 4) limit access to information that is not required to be protected. An agency may want to add a subsection specifically prohibiting inappropriate or wrongful categorization (see Section B.9.30).

Subsection (b) indicates two circumstances in which the access category may change. The first circumstance occurs when other or newer information becomes known that changes the nature of permitted access. An example would be an instance in which the identity of an alleged criminal becomes known, or new information suggests the imminence of criminal, including terrorist, activity. The second circumstance occurs when the subsequent use of the information results in different rules becoming applicable. An example of this occurs when information that is otherwise nonpublic is introduced into a court case and, by virtue of being in the court file, becomes a public record. The character of information may change again, including returning to a more private state (for example, when a conviction is expunged). The agency needs to determine what other boundaries exist where the transfer or exchange of information changes its categorization.

Subsection (c) states the uses of the classifications. The classification can be used to control both access (Subsection (c) (1)) and dissemination (Subsection (c) (3)). The classification is also relevant to who can add or modify information in the system (Subsection (c) (2)).

B.5.00 Information Quality

(a) The agency will make every reasonable effort to ensure that information sought or retained is:
(1) Derived from dependable and trustworthy sources of information;
(2) Accurate;
(3) Current;
(4) Complete, including the relevant context in which it was sought or received and other related information; and
(5) Merged with other information about the same individual or organization only when the applicable standard [*in Section B.6.20*] has been met.

[or]

(a) The agency will comply with [*cite the applicable state law or policy setting forth information quality standards comparable to those specified above*].

(b) The agency will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.

(c) The agency will make every reasonable effort to ensure that information will be deleted from the system when the agency learns that:

(1) The information is erroneous, misleading, obsolete, or otherwise unreliable;
(2) The source of the information did not have authority to gather the information or to provide the information to the agency; or
(3) The source of the information used prohibited means to gather the information [*note any exceptions; see Subsection B.4.20 (b) (2)*].

(d) The agency will advise recipient agencies when information previously provided to them is deleted or changed pursuant to Subsection (c) when [*specify the circumstances in which notice of change or deletion will be made, for example, when the requesting agency has specifically requested to be notified or for particular types of changes or deletions, the information has been sealed or deleted*].

Commentary

This section lists the attributes of information quality that are required for information to be sought or retained by the agency. The requirement here is that agency personnel not seek unreliable information and not keep information once it has been found to be unreliable. These quality attributes are not required of information that is unsolicited and information that has not yet been evaluated for its quality (that is, when it is first acquired), although the section does apply if the decision is made to keep the information.

The first three subsections of (a) list the commonly understood aspects of information quality—it should be accurate, current, and from a reliable source. "Accuracy" encompasses the truthfulness of the information itself, any coding of the information, correct data entry when the information is added to the justice information system, and the data structures of the justice information system itself. There are several tools and business practices available to improve accuracy. They include such things as edit checks during data entry, the use of table-driven database structures, and referencing external data validity systems, for example, the U.S. Postal Service Address Verification service. Another way to improve accuracy is to allow individuals to see the information about themselves and seek to correct inaccuracies they perceive. However, this is often inadvisable for justice system information because of risks to individual and public safety. This is discussed in more detail in Section B.7.50, particularly Subsection (c).

Subsection (a) (3) refers to the "currency" of the information. Information that is old or stale may no longer have the relevant context and may be misleading or distracting. This is also a concern regarding information obtained from third-party sources, governmental or otherwise (see Subsection B.4.20 (b)).

Subsection (a) (4) addresses the "completeness" of the information. For information to be most useful to law enforcement, criminal intelligence, and justice communities—as well as others responsible for public protection, safety, or health—the full context must be collected and retained. This includes the context in which the information was obtained as well as seeking and retaining the whole story.

Under Subsection (a) (4), information that may be exculpatory should also be gathered and retained. For example, for arrest information, the system should include the disposition of the arrest when it occurs. A specific problem relates to a person's use of someone else's identity when arrested to avoid being discovered as someone with a criminal history or having outstanding warrants or other holds. When the correct identity is established, the arrest record for the person whose identity was misused should be augmented to indicate the misuse and make clear that the person does not have an arrest record.

Subsection (a) (5) refers to the merging of information from more than one source. See Subsection B.6.20 (b) for language on the standard for merging information.

The alternative Subsection (a) is for use when there is an existing law or policy defining information quality, which this policy should refer to rather than restate.

Subsection (b) refers to "authorized users." The implication is that the agency has established processes whereby users are not given authorization to add, change, or delete information until they have been trained and are considered qualified and competent to use the system.

Subsection (c) establishes an affirmative obligation to delete information that no longer has the requisite information quality. It identifies the typical reasons for deleting information. The reasons include factors related to the collection of the information as well as its inherent quality.

Subsection (d) addresses what should be done regarding information that has been shared with others. It requires the agency to inform other agencies about changes or deletions to information under certain circumstances. Requiring notice to every requestor whenever there is a change or deletion may be an onerous requirement, particularly if there has been significant sharing of information on a daily basis. The bracketed language would indicate when notice would be provided, based upon the nature of the inquiry or significance of the information.

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

Subsection (d) does not specify how the notice of change or deletion would be made. Options would include requiring a requestor who wanted notice to provide an e-mail address to which notice could be sent.

B.6.00 Collation and Analysis of Information

B.6.10 Collation and Analysis

(a) Information sought or received by the agency or from other sources will only be analyzed:

(1) By qualified individuals;
(2) To provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals, and organizations suspected of having engaged in or engaging in criminal, including terrorist, activities generally; and
(3) To further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the agency.

(b) Information sought or received by the agency or from other sources will not be analyzed or combined in a manner or for a purpose that violates Subsection [*B.4.10 (b)*].

Commentary

This section is primarily intended for criminal intelligence systems but may be relevant to records management systems or other types of justice information systems.

Subsection (a) (1) requires that the collation and analysis of information be performed by qualified individuals. This is in recognition that knowledgeable and skilled individuals are more likely to conduct the analysis in a professional, efficient, effective, and legal manner.

Subsection (a) (2) incorporates a use-type restriction similar to the collection restrictions described in Section B.4.10.

Subsection (a) (3) is similar to the restriction on gathering and storing information, in that it requires that analysis of information only be done in furtherance of and consistent with the purposes set forth in Section B.1.00.

Subsection (b) reiterates the prohibitions acknowledged in Subsection B.4.10 (b) about not collecting or compiling information based on improper criteria, such as religious or political views.

Recent advances in analytical approaches using anonymized data can provide an alternative to the exchange and analysis of data sets containing personally identifiable information on individuals. Using this technique, the personal identifiers in a set of data are replaced with new, anonymous identifiers before any analysis is done. After the analysis is done and if criminal, including terrorist, activity is detected, the analysts can request from the agency holding the source information the release of the actual personal identifiers for individuals of interest identified through the analysis. Such a process reduces the risk and stigma of investigation with an ulterior motive and the improper use or disclosure of information about specific individuals.

B.6.20 Merging of Information From Different Sources

(a) Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.

(b) The set of identifying information sufficient to allow merging will consist of [*specify a standard or set of information or characteristics that are considered adequate to allow merging of information*].

[*Consider adding the following subsection to allow tentative matching of information from more than one source: (c) If the matching requirements are not fully met but there is a strong partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.*]

Commentary

This section addresses a concern that becomes of greater significance as more information is shared across agencies and with private sector partners and as more information is acquired from third-party sources. For purposes of this section, "merged" means that information from different sources is linked in the system as referring to the same individual or organization.

Justice system effectiveness is leveraged by the ability to combine information from different sources to develop a complete picture of activities and threats—to "connect

the dots"—without duplicating efforts. Accurate merging has a number of benefits, including better identification of individuals, more complete information on persons of interest, fewer false leads, fewer false positives, less opportunity for fraud and abuse by suspects, and less risk of bad press or lawsuits from misidentification or erroneous merging. However, work will be hampered and resources wasted if information that does not relate to the same person or organization is erroneously combined as if it did. This section establishes the basis for a digital due diligence before merging information from separate sources.

A complicating aspect is that matching assumes the data sources both have the same meaning, structure, and coding for the factors upon which matching is to be done; for example, both use the same conventions regarding how to format and spell a person's name.

Subsection (b) requires the agency to specify a standard for merging information. The standard would specify which combination of characteristics would permit information from two or more sources to be linked as referring to the same person or organization. Examples of information, characteristics, or attributes that, in combination, could establish that information from two or more sources is, indeed, about the same individual include:

- *Full name;*
- *Date of birth;*
- *Fingerprints;*
- *Law enforcement or corrections system identification number, usually based on fingerprints;*
- *Photograph;*
- *Physical description: height, weight, eye color, hair color, race, ethnicity, tattoos, scars, etc.;*
- *Social security number;*
- *Driver's license number;*
- *Contact information, such as address, phone number, e-mail, etc.; and*
- *Other biometrics, such as DNA, retinal scan, facial recognition, etc.*

A more generic standard might state, "all available attributes that can contribute to higher accuracy of match."

In a noncriminal setting, one way to verify a match is to check with the person about whom the information is being matched (this is the approach of the Federal Computer Matching and Privacy Act). This is often not advisable and may not be possible in a criminal justice setting.

When considering information about organizations as opposed to individuals, the characteristics or attributes that, in combination, could establish that information from two or more sources is, indeed, about the same organization are more problematic. Possibilities include the organization's name, federal or state tax ID number, and contact information such as office address and telephone number.

Subsection (c) suggests an optional provision to address the circumstance in which it appears that information from different sources relates to the same person or organization, but the standard for merging has not been fully met. A common circumstance in which this is relevant is in gang monitoring. The optional provision requires it to be made clear that the standard has not been met even if the preliminary assessment is that the information appears to be about the same person or organization. Pending the collection of further information to meet the standard, there still may be a value in indicating the possibility of a match for those querying the information system (see Subsection B.4.30 (a)) or categorizing information regarding its validity and reliability.

There are several approaches for indicating the match is incomplete. A disclaimer could be included with the response to a query or with any report containing the information—the electronic equivalent of a red stamp on the file. There could also be a requirement for independent verification of the match by anyone querying and using the information. Another way to reduce negative consequences of hypothesizing such an association is to limit who can access the information.

B.7.00 Sharing and Disclosure of Information

The sections in this subpart address to whom and under what circumstances information in the justice information system may be disclosed. Disclosure may be passive, allowing access through queries to the justice information system, or active, disseminating or publishing the information, for example, in bulletins or notices.

The situations covered in this subpart are organized by the category of person or entity who is seeking access to information: law enforcement officer, specific-use provisions, the public, and the person about whom information is stored in the system. This is based on the assumption that access rules are often stated on the basis of the status of the requesting individual or entity with respect to the information and the system. Alternatively, the concepts in these sections could be organized according to the type of information sought (for example, arrest information, conviction information, or warrant information) or organized according to the

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

relationship of a person about whom information has been retained and may be shared or disclosed (for example, information about a defendant, victim, or witness) to the justice system.

For some types of justice information systems, the access and disclosure rules may provide for very limited access and disclosure. For example, the information in criminal intelligence systems generally is not publicly available.

B.7.10 Sharing Information Within the Agency and With Other Justice System Partners

(a) Access to information retained by this agency will only be provided to persons within the agency or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with the law and procedures applicable to the agency for whom the person is working.

[*Consider adding, if the person who gathered information is allowed to have access to it even if they would not be allowed access if they had not gathered it, the following provision: The person who received, reviewed, or added information to the system may be authorized to view the information he or she provided regardless of the type of access associated with the information or the contributor's access authority.*]

(b) An audit trail will be kept of access by or dissemination of information to such persons.

Commentary

This section governs sharing within the agency and with associated government agency personnel. These are the primary users of the information—generally the information system was created to help them do their job more effectively and at less cost. The allowed uses are intended to include all phases of law enforcement, from crime investigation through prosecution and adjudication to carrying out and monitoring the sentence. This encompasses agencies and entities such as law enforcement, prosecution, defense counsel, courts, pretrial services, probation, parole, and corrections at the local, state, tribal, territorial, or federal level.

Subsection (a) specifies a number of requirements regarding access and use. It states that the agency will only share the information it retains with government personnel who 1) are allowed to have access to this type of information; 2) will use it for law enforcement, public protection, or justice purposes—that is, they have a right to know; and 3) will use it in the performance of their official duties—that is, they have a need to know. The intent is to make it clear that just because a person has access by virtue of where he or she works or his or her role, the information available cannot be used for personal or other non-law enforcement inquiries or for inquiries not related to their work.

Subsection (b) provides that a record be kept of all access, by whom, and to what information. While retaining such a record might have the effect of discouraging access, it is an effective means of discouraging unnecessary or improper access and of tracing improper access for enforcement purposes (see Section B.9.30).

B.7.20 Sharing Information With Those Responsible for Public Protection, Safety, or Public Health

(a) Information retained by this agency may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.

[*Add for a criminal intelligence system: Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.*]

[*Consider adding: (b) The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.*]

(b) An audit trail will be kept of the access by or dissemination of information to such persons.

Commentary

This second disclosure section governs access to information by people and agencies whose duties are to protect the public, ensure public safety, or protect the public health. These individuals and entities may be more successful in preventing or stopping criminal, including terrorist, activities if they have timely access to certain types of information about threats, activities, or individuals. There is a wide range of entities, governmental and private, that might be entitled to information under these circumstances. Public protection would include security forces at locations or events involving large numbers of people (for example, sporting events and amusement parks), at critical facilities such as water and power plants and transportation links, and at installations whose operations, if disrupted, pose a threat to the public, such as chemical plants. It could also include individuals involved with other critical public services, such as transportation, communication, or financial centers. Public safety and public health include such agencies as fire departments, emergency medical and public health departments, and even agencies involved with mental health problems.

This section does not allow unfettered access. Subsection (a) provides for access only to those who have both a "right to know" and a "need to know" information that allows them to better protect public health or safety.

The optional Subsection (b) addresses the question of confirming or denying the existence of information that itself is not subject to public access. The subsection provides that the existence of information will not be confirmed or denied to someone who is not entitled to the information whose existence is being questioned. This prohibition 1) protects any confidentiality or privacy interests in the information, 2) protects the integrity of the investigatory or justice-related processes, and 3) contributes to public confidence in the system.

Subsection (c) provides that a record be kept of access. While retaining such a record might have the effect of discouraging access, it is an effective means of both discouraging unnecessary or improper access and of tracing improper access for enforcement purposes. The access is authorized because of the policy interest in public safety. The threat this access entails to privacy is mitigated somewhat by the requirement in Subsection (c) to maintain a record of who accessed the information so that violations of privacy can be detected and prosecuted.

B.7.30 Sharing Information for Specific Purposes

(a) Information gathered and retained by this agency may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

[*Consider adding: (b) The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.*]

(c) An audit trail will be kept of the requests for access and of what information is disseminated to such persons.

Commentary

Certain individuals or entities, including nongovernmental entities, may be entitled by law to access information contained in justice systems that is not available to the general public. For example, governmental officials, public agencies, licensing boards, and certain nongovernmental agencies may be entitled to information about the criminal history of an individual applying for services, employment, or benefits. Other examples of organizations that may be entitled to access, at least for limited purposes and for only certain information, include:

- *Government officials not in law enforcement or the justice system who are responsible for making public safety decisions on behalf of the public regarding facilities or services;*
- *Government officials not in law enforcement or the justice system who are responsible for making public health decisions;*
- *Government officials not in law enforcement or the justice system who are responsible for making entitlement or allocation decisions for individuals to receive government services or benefits, for example, public housing, health care, or welfare;*
- *Critical infrastructure protection or security entities (public or private);*
- *Professional licensing boards;*
- *Employers (public or private) hiring individuals for specific duties, such as bus drivers, airport workers, child care workers, etc.;*
- *Domestic violence shelters;*
- *Businesses or organizations particularly susceptible to cybercrime and identity theft; and*

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

- *Individuals or organizations conducting research, evaluation, or statistical studies who are monitoring or reporting about the activities or performance of an agency or the clients served by the agency, with appropriate institutional review board oversight.*

Subsection (a) requires that the individual be authorized to have access and that the use must be for the purpose specified in the law permitting access.

The optional Subsection (b) addresses the question of confirming or denying the existence of information that itself is not subject to public access. The subsection provides that the existence of information will not be confirmed or denied to someone who is not entitled to the information whose existence is being questioned. One example of this is criminal convictions that have been expunged or sealed where there are public policy decisions that even the existence of the former conviction should not be revealed. This prohibition 1) protects any confidentiality or privacy interests in the information, 2) protects the integrity of the investigatory processes, and 3) contributes to public confidence in the system.

Subsection (c) provides that a record be kept of all access. While retaining such a record might have the effect of discouraging access, it is an effective means of both discouraging unnecessary or improper access and of tracing improper access for enforcement purposes. The access is authorized because of the policy interest in public safety. The threat this access entails to privacy is mitigated somewhat by the requirement in Subsection (c) to maintain a record of who accessed the information so that violations of privacy can be detected and prosecuted.

B.7.40 Disclosing Information to the Public

(a) Information gathered and retained by this agency [*may/will*] be disclosed to a member of the public only if the information is defined by law to be a public record and is not excepted from disclosure by law, and it may only be disclosed in accordance with the law and procedures applicable to this agency for this type of information.

[or]

(a) The agency will ensure that information gathered and retained by this agency [*may/will*] be disclosed to a member of the public only if the information complies with [*cite the applicable law or policy setting forth public access to information*].

(b) The agency shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

(c) An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

[*(d) Add provisions regarding the fees, if any, that will be charged to those requesting information.*]

[*(e) Add provisions regarding bulk or compiled distribution of information to third parties if the agency will allow such access. Also address charging a fee for information "sold" to third parties.*]

Commentary

This section governs public access—access by anyone who is not entitled to access pursuant to one of the prior sections. Subsection (a) indicates when information may be disclosed to the public (see definition of "public" in Section B.3.40). It permits disclosure to the public of information that is specifically designated as a public record. Examples of this include such things as court records and conviction information. The subsection also permits disclosure of information to the public when such access is specifically allowed by law for information that would otherwise not be public. Examples include such things as police blotters, sex offender registries, and information about fugitives who are subject to arrest. An alternative provision is suggested for which there is a relevant and applicable law covering public access, for example, a public records act or freedom of information act.

The subsection also provides that the information can only be disclosed in the manner permitted by the law authorizing public access. For example, the information cannot be disclosed selectively to some members of the public, but not others. Another example would be restrictions in some jurisdiction that arrest information can only be requested chronologically, not by name, to avoid the ability to build arrest histories retroactively one at a time.

Subsection (b) addresses the question of confirming or denying the existence of information that itself is not subject to public access. The subsection provides

that the existence of information will not be confirmed or denied if the information whose existence is being questioned is not public information. This prohibition 1) protects any confidentiality or privacy interests regarding the information, 2) protects the integrity of the justice processes, and 3) contributes to public confidence in the system.

Subsection (c) provides that a record be kept of disclosure. The record is to indicate both to whom disclosure was made and what information was disclosed. While retaining such a record might have the effect of discouraging access, it is an effective means of both discouraging unnecessary or improper access and of tracing improper access for enforcement purposes. The access is authorized because of the policy interest in public safety and open government records. The threat this access entails to privacy is mitigated somewhat by the requirement in Subsection (c) to maintain a record of who accessed the information so that violations of privacy can be detected and prosecuted, as well as deterred.

Subsection (c) assumes that it is legal to keep records of public access requests. In some instances, this may not be permitted under local or state laws. There may also be limitations regarding access to information about the requestor collected as part of the logging process.

Subsection (d) is included as a placeholder for the agency to use if it will charge a fee for providing information from the system.

Subsection (e) is included as a placeholder for the agency to use if it decides that bulk or compiled disclosure of information from the system is permitted and appropriate. In many states, access to individual records may be allowed, but bulk access is not. In addition, there may be a distinction between information about individuals when the individual is identifiable and information that is more aggregate in nature, and one cannot identify a specific individual from the information provided. The subsection could also contain language about whether information can be "sold" to third parties and what the fee is.

B.7.50 Disclosing Information to the Individual About Whom Information Has Been Gathered

(a) Upon satisfactory verification of his or her identity and subject to the conditions specified in (b), an individual is entitled to know the existence of and to review the information about himself or herself that has been gathered and retained by the agency. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The agency's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual.

(b) The existence, content, and source of the information will not be made available to an individual when:

(1) Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
(2) Disclosure would endanger the health or safety of an individual, organization, or community;
(3) The information is in a criminal intelligence system; or
(4) The information relates to [*specify what types of information are not to be disclosed to an individual under the law applicable to the agency*].

(c) If an individual has objections to the accuracy or completeness of the information retained about himself or herself, the agency will inform the individual of the procedure for requesting review of any objections. The individual will be given reasons if a request for correction is denied. The individual will also be informed of the procedure for appeal when the agency has declined to correct challenged information to the satisfaction of the individual about whom the information relates.

[*(d) Add provisions regarding the fees, if any, that will be charged to those requesting information; for example, the agency may charge a fee for disclosure that reflects the cost to the agency for locating and reproducing the information (specify any exceptions to charging a fee*).]

(e) A record will be kept of all requests and of what information is disclosed to an individual.

Commentary

Subsection (a) states that an individual is entitled to know of and review information about himself or herself that is retained by the agency. The individual must verify his or her identity before obtaining access. The only information to be disclosed is that specifically about the individual requesting disclosure.

Subsection (b) lists exceptions to disclosure of information about an individual. If disclosure would inhibit an active investigation, the information need not be disclosed. If disclosure would endanger someone (for example, a victim, witness, informant, or law enforcement personnel) or some organization, the

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

information need not be disclosed. If the information is part of a criminal intelligence system, it need not be disclosed. Some agencies, for example, correctional institutions, may want to include further restrictions (in Subsection (b) (4)) to avoid such requests interfering with the operations of the institution (see Section B.1.00 (j)). Finally, there may be local or state laws further limiting disclosure of information to an individual, and they should be specified or referred to in this section.

Subsection (c) relates to the process by which an individual may seek review of information that the individual alleges to be incorrect or incomplete.

Subsection (d) is included as a placeholder for the agency to use if it will charge a fee for providing information from the system.

Subsection (e) provides that a record be kept of all disclosure requests. While retaining such a record might have the effect of discouraging access, it is an effective means of both discouraging unnecessary or improper access and of tracing improper access for enforcement purposes (see Section B.9.30).

Provision is made in proposed Subsection B.9.20 (h) for a situation in which information about an individual has been obtained by someone not authorized to have it and this ought to be brought to the attention of the individual so steps can be taken to protect from harm.

B.8.00 Information Retention and Destruction

The following sections on records retention are included because of their impact on the protection of privacy, civil rights, and civil liberties. Once information is deleted or returned according to applicable retention schedules, it is no longer at risk of being improperly accessed, shared, or disclosed. Information that is no longer kept in a justice information system cannot infringe on anyone's privacy rights or interests, civil rights, or civil liberties. If the agency already has a robust records retention policy, the language of Section B.8.20 can contain a reference to the applicable records retention policy.

B.8.10 Review of Information Regarding Retention

(a) Information will be reviewed for purging [*specify periodic basis, such as annually, or reference the applicable law*].

(b) When information has no further value or meets the criteria for removal under applicable law, it will be purged, destroyed, deleted, or returned to the submitting source.

Commentary

This section explicitly states the policy of requiring periodic review of information to determine whether it should be purged from the justice information system. The intent of this section is not only to ensure compliance with any applicable records retention policy (Subsection (a)) but also to encourage a review that may remove information that no longer has value before it would be required to be purged by applicable records retention policies (Subsection (b)). This reflects a proactive approach to managing justice system information.

B.8.20 Destruction of Information

(a) The agency will delete information or return it to the source according to the following schedule:

[*Reference the law(s) specifying the applicable record destruction standard or schedule*]

[or]

[*If there is no applicable law, specify the destruction standard or schedule applicable to the system's records*].

(b) Permission to destroy or return information or records will be obtained from:

[*Reference the law(s) specifying whose permission must be obtained before destroying information or records*]

[or]

[*If there is no applicable law(s), specify whose permission, if any, must be obtained before destroying information or records*].

(c) Notification of proposed destruction or return of records will be provided to:

[*Reference the law(s) specifying to whom notice must be provided about the proposed destruction of information or records*]

[or]

[*If there is no applicable law, specify who, if anybody must be notified about the proposed destruction of information or records*].

[*Consider adding: (d) The time period for purging information concerning an individual may be tolled during the time that an individual is in prison serving a sentence.*]

(d) A record that information has been purged or returned shall be maintained by the agency.

Commentary

This section specifies when review and purging of information in a justice information system is to occur and what the business process should involve. The policy can either reference relevant existing laws or provide the specific language about retention periods, destruction schedules, permission, and notice adopted by the agency if there is no applicable law. An alternative to periodic manual review would be to develop software that automatically purges information at the end of a specified period or notifies someone of the intent to purge.

The section is silent about whether the information is purged only from the live system or also from backups, archived data, or other forms of offline media. Purging from offline media presents an additional set of logistics problems. However, there should be procedures in place that prevent backup media that contains information subsequently deleted from the live system from being reloaded if the live system crashes.

If information has been provided to third parties, in particular to members of the public, notifying them of the subsequent destruction of the information, as required in Subsection (c), can be problematic. If information has been provided in bulk or compiled form, it may be easier to achieve elimination of copies of the information. For example, the agreement allowing bulk requests can require the requestors to regularly update their information to purge information that the agency has destroyed. The most effective way to limit use of purged information is to provide some penalty, fiscal or penal, if someone uses such information without checking to make sure it is still current.

Subsection (d) proposes a provision to suspend the time for purging a record while a person is in prison. The objective is to have the information about a person's criminal activity not be purged because the person is serving a prison term that exceeds the general retention period for this type of information. There may be other circumstances where the retention period should be extended that the agency should consider.

B.9.00 Accountability and Enforcement

B.9.10 Information System Transparency

(a) The policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request and through any public Web sites providing information about the system.

(b) The agency will designate a person responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system and will provide to the public the [*position title*] contact information.

Commentary

Subsection (a) implies that the existence of the justice information system will be known to the public by requiring the privacy policy to be made available to the public. Acknowledging the existence of the system demonstrates the willingness of the agency to be subject to appropriate public scrutiny and contributes to public confidence in the agency and its operations.

Subsection (b) requires the agency to designate who the public can contact regarding inquiries about the justice information system or with whom complaints can be lodged. It also requires that contact information be provided to the public.

B.9.20 Accountability for Activities

(a) Primary responsibility for the operation of this justice information system, including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy is assigned to [*specify position responsible for the system*].

(b) The agency will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with [*provide reference to applicable technical standards or benchmarks specifying generally acceptable security practices*].

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

(c) The agency will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as provided in [*provide reference to applicable technical standards or benchmarks specifying generally acceptable information storage practices*].

(d) The agency will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself with the provisions of this policy and applicable law. [*Consider referencing industry standards or generally accepted practices or adding language describing the mechanisms that will be used to ensure compliance, for example, adoption of information system security practices, logging of access requests and responses, and detection of unauthorized attempts to add, change, delete, or access information, audit practices, and other enforcement mechanisms.*]

(e) The agency will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy.

(f) The agency will periodically conduct audits and inspections of the information contained in the [*justice information system*]. The audits will be conducted randomly by a designated representative of the agency or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information.

(g) The agency will periodically review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations.

[*Consider adding: (h) The agency will notify an individual about whom unencrypted personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens physical or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and to reasonably restore the integrity of the information system. Notice need not be given if doing so meets the criteria specified in Subsection B.7.50 (b).*]

Commentary

This section establishes the basic framework for holding the agency accountable for enforcing its privacy and civil rights policy.

Subsection (a) requires the designation of an individual who is ultimately responsible for the operation of the system, in particular regarding privacy and civil rights provisions.

Subsection (b) requires the agency to maintain and protect information in such a way that its integrity can be preserved and relied upon and to act to prevent unauthorized access, modification, or destruction of information. The information should be physically protected from improper access, intrusion, or destruction whether from humans or natural events. It should also be protected electronically through use of software, network, or other information technology tools. Assistance with both security concepts and implementation can be found in Applying Security Practices to Justice Information Sharing.[12] *The suggestion is made to cross-reference an industry standard or other statement of generally accepted practices covering the subjects of this subsection.*

Subsection (c) requires the agency to store information in a manner that minimizes the opportunity for someone to improperly access, modify, add to, or delete information. Storage refers equally to information in electronic or paper form. The suggestion made is to cross-reference an industry standard or other statement of generally accepted practices.

Subsection (d) requires the establishment of procedures and business practices that implement the intent of the privacy and civil rights policy and that allow compliance with the policy to be effectively monitored. The language suggests adding a reference to specific approaches and techniques. The recitation of tools should increase public confidence that appropriate steps are being taken to protect information.

Subsection (e) requires users to sign a written agreement to comply with the policies provisions. This document can form a basis for enforcement actions

12 Available at http://it.ojp.gov/documents/200404_ApplyingSecurityPractices_v_2.0.pdf.

(see Section B.9.30), whether personnel-related or criminal in nature. "Any individual" would include agency employees; employees of contractors and service providers who assist the agency in developing, maintaining, or using the system; and employees of other agencies authorized to use the system.

Subsection (f) requires periodic and random audits of the information held by the agency. The intent of an audit is both to act as a deterrent and to detect improper access to, retention of, or use of information. It can also reveal problems in data entry that create errors, whether random or systematic. All of these demonstrate public accountability and increase public confidence that the agency is acting responsibly.

Subsection (g) requires periodic review of the privacy and civil rights policy to ensure that it remains in compliance with applicable law, is responsive to changes in technology, and takes advantage of new technology that may assist in monitoring compliance and detecting violations of the privacy and civil rights policy. One way to ensure this is to consider the inclusion of a specific sunset date, thus forcing reevaluation of the effectiveness and scope of the policy.

Subsection (h) is proposed if the agency wants to commit itself to the type of notification of individuals required by law in several states where information held by an entity has been improperly released or disclosed. The unauthorized access ought to be brought to the attention of the individual so that they can take steps to protect themselves from harm. There is a requirement that the release could cause physical or financial harm to the individual, and there are exceptions intended to protect the integrity of the investigation and prosecution processes. The cross-reference to Subsection B.7.50 (b) refers to circumstances in which notice should not be given to a person because doing so might interfere with an existing investigation or potentially harm someone.

B.9.30 Enforcement

If a user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the agency will:

(a) Suspend or discontinue access to information by the user;

(b) Suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies;

(c) Apply other sanctions or administrative actions as provided in agency personnel policies;

(d) Request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or

(e) Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy as stated in [*Section B.1.00*].

Commentary

The policy will not adequately or effectively protect privacy, civil rights, or civil liberties if its provisions are violated with impunity. This section specifies the range of penalties for violations of the policy. Disciplinary action, appropriate to the severity of the offense, should be taken against a user who:

1. *Fails to comply with the provisions about what information may be sought or retained or what may not be sought or retained or who uses improper means or sources to seek or receive information;*
2. *Uses information for unauthorized purposes, including personal use or commercial use, whether or not the person receives a benefit;*
3. *Discloses information to someone not authorized to receive the information;*
4. *Fails to correct information found to be erroneous or to report the error to appropriate personnel;*
5. *Fails to purge information when it is no longer of value or has reached its retention schedule;*
6. *Retains or otherwise fails to destroy information that is scheduled to be destroyed or is no longer relevant to the purposes of the system; or*
7. *Fails to disclose information that an individual or the public is entitled to know the existence of and to review.*

Subsection (d) addresses the situation in which the user is not employed directly by the agency but is employed by or under contract to another entity that uses the system.

Training of agency employees, contractors, and users regarding the policy and consequences for violating it are addressed in Section B.10.00.

B.10.00 Training

(a) The agency will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

(1) Its personnel;
(2) Personnel providing information technology services to the agency;
(3) Staff in other public agencies or private contractors providing services to the agency; and
(4) Users who are not employed by the agency or a contractor.

(b) The training program will cover:

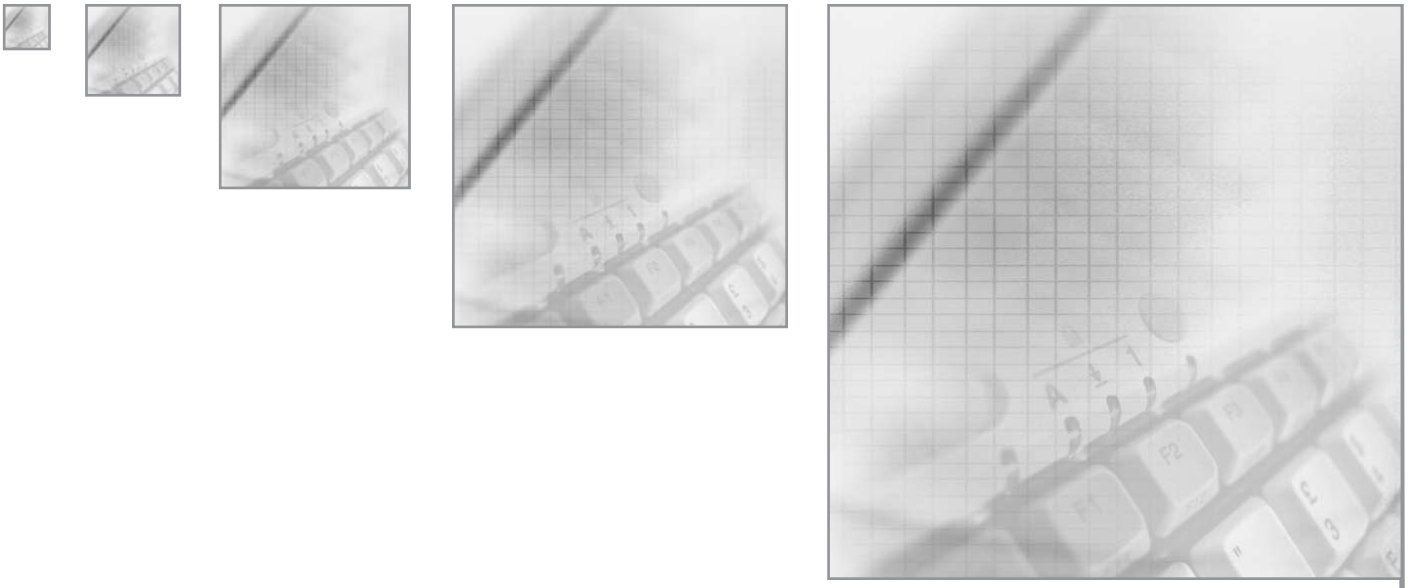
(1) Purposes of the privacy, civil rights, and civil liberties protection policy;
(2) Substance and intent of the provisions of the policy relating to collecting, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency;
(3) The impact of improper activities associated with information accessible within or through the agency; and
(4) The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

Commentary

Subsection (a) requires training not just of agency personnel but of others who may have access to information retained by the agency or that is accessible through the agency. The agency can require contractors to provide the necessary training as part of the contract with the agency. Users can be required to obtain the necessary training before being given authorization to access information retained by the agency.

Subsection (b) describes the subjects the training should encompass. It includes the basic aspects of the policy regarding privacy, civil rights, and civil liberties; why the policy is necessary; and the consequences for failing to comply with the policies. Consideration should also be given to establishing certification for the training, to encourage participation.

Subsection (b) (2) identifies the broad categories that should be covered in the training.



C. Provisions for a Multiagency Agreement for an Information Sharing System

This part contains suggestions for provisions that would be included in an interagency agreement between two or more governmental agencies establishing a justice information sharing system or network. The agencies involved could be local, state, tribal, territorial, federal, or international. The objective of the suggested provisions is to define the roles, responsibilities, and contributions of the agencies participating in the information sharing network relative to protection of privacy, civil rights, and civil liberties. These provisions should be included in the interagency agreement that is signed by the agencies who are participating in the justice information sharing system or network that defines its policies and operation. Any agency subsequently joining a justice information sharing system would also be expected to sign an interagency agreement containing these provisions.

The provisions suggested are stated in terms of principles, not details. The intent is that the interagency agreement state what is expected of the participating agencies regarding protection of privacy, civil rights, and civil liberties. How the participating agencies implement these protections internally is left to the agency, with the expectation that each agency's internal policies will address the requirements stated in the interagency agreement concepts. Adoption of a policy addressing the principles identified in Part B would presumably meet this requirement.

C.1.00 Statement of Purpose

The goal of establishing and maintaining this justice information sharing system is to further the following purposes:

(a) Increase public safety and improve national security;

(b) Minimize the threat and risk of injury to specific individuals;

(c) Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;

(d) Minimize the threat and risk of damage to real or personal property;

(e) Protect individual privacy, civil rights, civil liberties, and other protected interests;

(f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

(g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;

(h) Support the role of the justice system in society;

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

(i) Promote governmental legitimacy and accountability;

(j) Not unduly burden the ongoing business of the justice system; and

(k) Make the most effective use of public resources allocated to justice agencies.

Commentary

See Commentary under Section A.1.00 in Part A.

One justification for sharing information across agencies is that criminal activity and threats to public safety and health often occur across jurisdictional boundaries; thus sharing of information across jurisdictional boundaries is necessary to respond to these threats.

C.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

The employees and users of the participating agencies and of the agency's information service providers will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information through the justice information sharing system.

Commentary

See Commentary under Section A.2.00 in Part A.

C.3.00 Sharing of Information Among Participants

C.3.10 Expectations Regarding Information Gathered and Shared

Participating agencies will adopt internal policies and procedures requiring the participating agency, its personnel, contractors, and users to:

(a) Only seek or retain information that is legally permissible for the agency to seek or retain under laws applicable to the agency;

(b) Only use lawful means to seek information;

(c) Only seek and retain information that is reliably accurate, current, and complete, including the complete, relevant context;

(d) Take appropriate steps when merging information about an individual or organization from two or more sources, to ensure that the information is about the same individual or organization;

(e) Investigate in a timely manner any alleged errors and correct or delete information found to be erroneous;

(f) Retain information sought or received only so long as it is relevant and timely, and delete or return information that is inaccurate, outdated, or otherwise no longer related to known or suspected criminal, including terrorist, activities;

(g) Maintain information and systems containing information in a physically and electronically secure environment and protected from natural or man-made disasters or intrusions;

(h) Engage in collation and analysis of information in a manner that conforms to generally accepted practices;

(i) Establish procedures that comply with the policies and procedures of the justice information sharing system for accessing information through the participating agency;

(j) Only allow authorized users to access the information in the shared system and only for purposes related to the performance of their official duties;

(k) Share information with authorized users of other justice system partners based only on a "right-to-know" and a "need-to-know" basis; and

(l) Establish and comply with information retention and destruction schedules.

Commentary

The objective of this provision is to require participating agencies to adopt policies addressing the issues listed in this section. If an agency adopts a policy based on the provisions in Part B, they will be in compliance with these requirements when joining a justice information sharing system.

Expectations regarding the disclosure of information are provided for in Section C.4.10.

Compliance with and enforcement of the provisions adopted is addressed in Section C.5.00.

C.3.20 Sharing Information With Other Justice System Partners

A participating agency will make information available in response to a query either by:

(a) Providing the requested information directly;

(b) Responding with the contact information of a person in the responding agency whom the individual making the query can contact;

(c) Having a person in the responding agency contact the individual making the query; or

(d) Indicating that no information is available.

The choice of approach as to any particular piece of information shall be at the discretion of the agency that has retained the information.

Commentary

This provision gives a participating agency options regarding how to provide information in response to a query from another participating agency, thus providing an additional layer of protection for information and investigations. Most information from the responding agencies would be made available directly, either through a query to the agency's database or by a query to a data warehouse or a similar approach, to which participating agencies have transferred the information from their databases. If the agency queried desires a higher level of protection of the data, it can provide the person making the query with the contact information of someone in the responding agency. The person contacted can then verify the requestor's need to know and purpose of the inquiry before providing the information. This has the added benefit of letting the person in the responding agency know that others are interested in a particular individual, organization, or information. If the information is of a sensitive nature and not to be disclosed generally (for example, if it is part of an active investigation of a highly sensitive nature), the system could notify a designated contact in the agency that someone has made an inquiry and the decision can be made whether to call the person inquiring and what to disclose, if anything. Finally, the agency queried can simply decline to disclose information or respond that no information is available.

C.4.00 Use and Disclosure of Information Originating From Another Participating Agency

C.4.10 Disclosure of Information According to the Originating Agency's Access Rules

A participating agency will not disclose information originating from another agency except as [*authorized or required by law in the jurisdiction in which the information originated*] OR [*provided for in this agreement or in the operational policies of the shared information system*].

Commentary

This section provides two alternatives for the applicable policy regarding disclosure—either the policy of the agency that is the source of the information in the shared system or the disclosure policy of the justice information sharing system, whichever the participating agencies agree to. Alternatively, the language could state that the applicable policy is the most restrictive of the rules of the participating agencies.

If the provision requires participating agencies to follow the policy of the originating agency, two purposes are served. One is that it will encourage participating agencies to share information. If an agency is concerned that information will be disclosed in violation of their access policies, they may be unwilling to share the information. Second, it implements access and disclosure rules of the originating agency that are consistent with the circumstances and public expectation surrounding the collection of the information.

Implementation of this rule may not be as complicated as it may first appear. A user in another agency need not learn the access rules of the originating agency if an access category is associated with the information when it is included in the justice information sharing system, as required in Section B.4.40. The justice information sharing system will then provide access based on the access categorization.

C.4.20 Reporting Possible Information Errors to the Originating Agency

When a participating agency gathers or receives information that suggests that information originating from another agency may be erroneous, may include incorrectly merged information, or lacks relevant context, the alleged error will be communicated in writing to the person designated in the originating agency to receive such alleged errors

Bold text is template text

[**Bracketed text**] requires user input

Italic text is commentary

pursuant to Subsection [*C.5.10(e)*].

Commentary

The intent of this provision is both to improve the quality of the shared information and to make explicit the obligation of the person uncovering the possible error to report the alleged error back to the originating agency. Subsection C.3.10 (e) obligates the originating agency to investigate alleged errors reported to them and correct any errors found.

The obligation to communicate in writing is to increase the likelihood that something will be done by the receiving agency. Writing should include e-mail as well as any other form of writing; verbal communications should not be considered sufficient.

In order to implement this provision, each participating agency should identify a contact person to whom alleged errors are to be reported. This is required in Subsection C.5.10 (e).

C.5.00 Participating Agency Accountability and Enforcement

C.5.10 Expectations Regarding Accountability and Enforcement

Participating agencies will adopt and comply with internal policies and procedures requiring the agency, its personnel, contractors, and users to:

(a) Have and enforce policies for discovering and responding to violations of agency policies and this memorandum, including taking appropriate action when violations are found;

(b) Provide training to personnel authorized to use the justice information sharing network about the agency's requirements and policies regarding information collection, use, and disclosure;

(c) Make available to the public the agency's internal policies and procedures regarding privacy, civil rights, and civil liberties;

(d) Cooperate with periodic, random audits by representatives of the justice information sharing system; and

(e) Designate an individual within the participating agency to receive reports of alleged errors in the information that originated from the participating agency.

Commentary

The objective of this section is to explicitly state the need for participating agencies to monitor, conduct, and enforce policies regarding protection of privacy, civil rights, and civil liberties. Having a policy is meaningless if it can be ignored with impunity.

Subsection (e) requires each participating agency to identify a contact person to whom alleged errors are to be reported.

C.5.20 Enforcement of Provisions of Information Sharing Agreement

If a participating agency fails to comply with the provisions of this agreement or fails to enforce provisions in its local policies and procedures regarding proper collection, use, retention, destruction, sharing, disclosure, or classification of information, the justice information sharing network may:

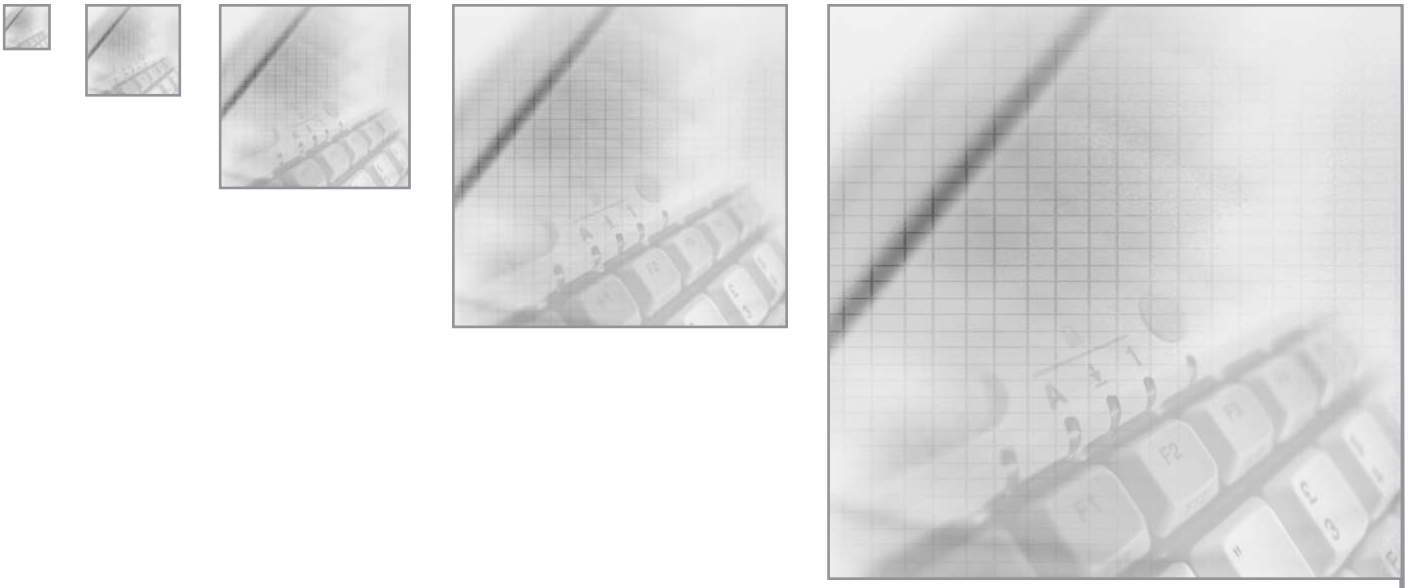
(a) Suspend or discontinue access to shared information by a user in the offending agency who is not complying with the agreement or local policies and procedures;

(b) Suspend or discontinue the offending agency's access to the justice information sharing system; or

(c) Offer to provide an independent review, evaluation, or technical assistance to the participating agency to establish compliance.

Commentary

If a participating agency fails to comply with the law and policies protecting privacy, civil rights, and civil liberties, this section provides alternative responses. The subsections contain an escalating set of options designed to allow the information sharing system to protect information, yet retain the benefits of sharing. At the lowest level, the system terminates access by an offending user. If the problem is more pervasive in the agency, it can terminate access by the agency. Finally, there is the option of maintaining access but working with the agency to improve its practices and compliance.



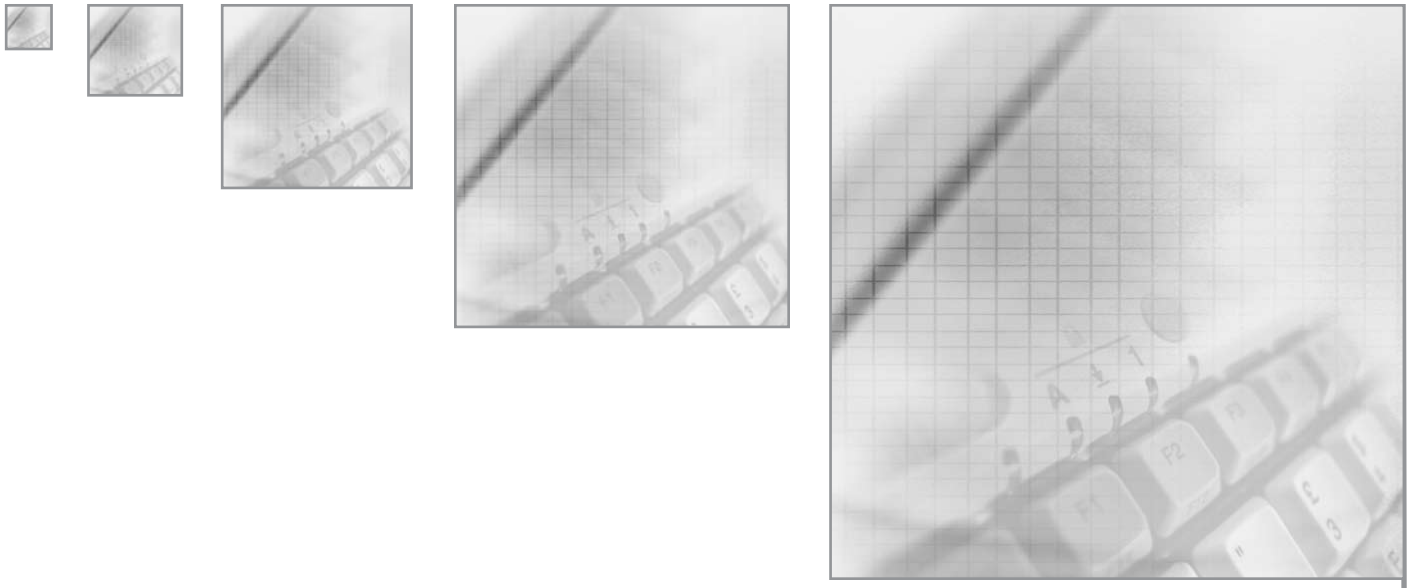
Appendix One

Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

The following federal laws should be reviewed when developing a privacy and civil rights policy for a justice information system. The list is arranged in alphabetical order by popular name.

- **U.S. Constitution**, First, Fourth, and Sixth Amendments
- **Brady Handgun Violence Prevention Act**, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A
- **Computer Matching and Privacy Act of 1988**, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000
- **Confidentiality of Identifiable Research and Statistical Information**, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22
- **Criminal History Records Exchanged for Noncriminal Justice Purposes**, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611
- **Crime Identification Technology**, 42 U.S.C. §14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601
- **Criminal Intelligence Systems Operating Policies**, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23
- **Criminal Justice Information Systems**, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20
- **Disposal of Consumer Report Information and Records**, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682
- **Electronic Communications Privacy Act of 1986**, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508
- **Fair Credit Reporting Act**, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681
- **Federal Civil Rights** laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983
- **Federal Records Act**, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

- **Freedom of Information Act** (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552
- **Indian Civil Rights Act of 1968**, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301
- **HIPAA**, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191
- **HIPAA**, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164
- **National Child Protection Act of 1993**, Pub. L. 103-209 (Dec. 20, 1993), 107 Stat. 2490
- **National Crime Prevention and Privacy Compact**, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616
- **Privacy Act of 1974**, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a
- **Privacy of Consumer Financial Information**, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313
- **Protection of Human Subjects**, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46
- **Safeguarding Customer Information**, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314
- **Sarbanes-Oxley Act of 2002**, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201
- **USA PATRIOT Act**, Public Law No. 107-56 (October 26, 2001), 115 Stat. 272



Appendix Two

Local, State, Tribal, and Territorial Laws Possibly Relevant to Seeking, Retaining, and Disseminating Justice Information

Sources of Local, State, Tribal, and Territorial Law:

The following local, state, tribal, and territorial laws should be reviewed when developing a privacy and civil rights policy for a justice information system:

- Constitution (in particular, provisions regarding information gathering, such as search and seizure)
- Statutes
- Regulations
- Court rules and procedural and practice rules
- Case law (federal and state)
- Attorneys Generals' opinions
- Executive orders and formal procedures and protocols
- Professional codes of ethics
- Local ordinances
- Tribal ordinances, resolutions, and descriptions of tribal customary laws
- Treaties

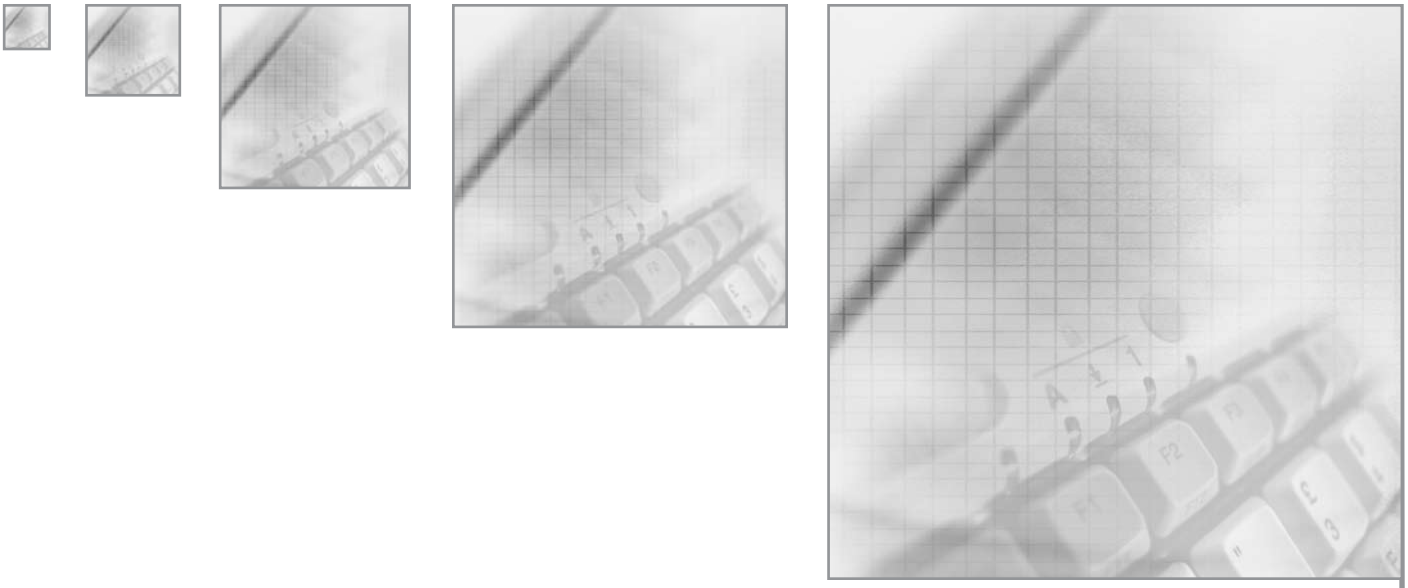
Specific Categories of Local, State, Tribal, and Territorial Laws to Review Regarding Seeking, Retaining, and Disseminating Justice Information:

- Access to criminal history or arrest information of applicants for caregiver positions
- Access to criminal history or arrest information of applicants for regulated professions
- Criminal history repository
- Integrated justice information system
- Criminal intelligence system
- Victim and witness protection
- Juveniles (in particular, regarding confidentiality of proceedings)
- Family relations laws (in particular, child custody and domestic violence)
- Medical records and information
- Civil harassment, restraining, and stay-away orders
- Civil commitments of individuals who pose a threat to themselves or others because of mental illness
- Public records acts (in particular, regarding justice system records and information)
- Open meeting laws as they affect the agency or the governing body of a justice information system

Activities or Events Subject to Local, State, Tribal, and Territorial Laws

The following list describes activities, events, transactions, and information exchanges that typically are the subject of justice information systems:

- Law enforcement contacts (in particular, traffic stops)
- Informants
- Surveillance, including pen registers and packet sniffers
- Search warrants
- Arrest warrants
- Arrests
- Interrogation
- Lineups
- Police logs
- Police reports (field reports, formal reports, and supplemental reports)
- Laboratory or forensic testing or analysis
- Investigation (existence, work products)
- Trial activities
- Information generated during a trial
- Victim-advocate logs
- Convictions (any distinctions based on seriousness of crime)
- Sentencing information, including programs providing alternatives to incarceration
- Treatment programs, including those imposed by problem-solving courts such as drug courts
- Probation (in particular, terms and conditions)
- Parole (in particular, terms and conditions)
- Domestic violence, civil harassment, and stay-away orders
- Enforcement of planning, zoning, environmental, and similar laws
- Other events, transactions, or activities revealed in the project's information exchange analysis



Appendix Three

Bibliography for Sources and References

Applying Security Practices to Justice Information Sharing, Global Justice Information Sharing Initiative Security Working Group, March 2004, Version 2.0, available at

http://it.ojp.gov/documents/200404_ApplyingSecurityPractices_v_2.0.pdf

Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts, Martha Wade Steketee and Alan Carlson, National Center for State Courts, October 18, 2002, available at

http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf or http://www.jmijustice.org/Data/DocumentLibrary/Documents/1141964905.77/CCJ-COSCA%20Access%2018Oct2002FinalReport.pdf

Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New Era, Version 1.0, Global Justice Information Sharing Initiative, July 2005, available at

http://it.ojp.gov/topic.jsp?topic_id=209

IACP Criminal Intelligence Model Policy, International Association of Chiefs of Police, June 2003.

IACP, *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State, and Federal Levels*, International Association of Chiefs of Police, August 2002, available at

http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf

IACP Model Statutes Project: International Association of Chiefs of Police, revised October 2001.

Law Enforcement Analytic Standards, International Association of Law Enforcement Intelligence Analysts, Inc., November 2004.

IIR Sample Operating Policies and Procedures, Institute for Intergovernmental Research, (date unknown), available at

http://www.iir.com/28cfr/sample_operating_policies.htm

Information Privacy: A Spotlight on Key Issues, National Association of State Chief Information Officers (NASCIO), February 2004, Version 1.0, available at

https://www.nascio.org/publications/index.cfm#privacyguide

Information Quality: The Foundation for Justice Decision Making, Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice, slated for imminent release. Please call (850) 385-0600, extension 285, for further information.

NCISP Recommended Outreach Plan: *National Criminal Intelligence Sharing Plan*, Recommended Outreach Plan, July 2005.

National Criminal Intelligence Sharing Plan, Solutions and Approaches for Cohesive Plan to Improve Our Nation's Ability to Share Criminal Intelligence, Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice, issued October 2003, available at

http://it.ojp.gov/documents/NCISP_Plan.pdf

Justice Information Privacy Guideline, Developing, Drafting and Assessing Privacy Policy for Justice Information Systems, NCJA, September 2002, available at

http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/default.htm

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Annex to the Recommendation of the Council of 23rd September 1980, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part Two. Basic Principles of National Application, available at

http://it.ojp.gov/process_links.jsp?link_id=4751

Privacy and Information Quality Policy Development for the Justice Decision Maker, Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice, October 2004, located at

http://it.ojp.gov/documents/200411_global_privacy_document.pdf

Privacy Policy Development Guide and Implementation Templates, Bureau of Justice Assistance, October 2006, available at

http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

Privacy Technology Focus Group: Executive Summary, Bureau of Justice Asssistance, Office of Justice Programs, U.S. Department of Justice, slated for imminent release. Please call (850) 385-0600, extension 285, for further information.

RISS Privacy Policy: Regional Information Sharing Systems Privacy Policy, dated January 2004.

Safe Harbor Privacy Principles: U.S. Department of Commerce, issued July 21, 2000, available at

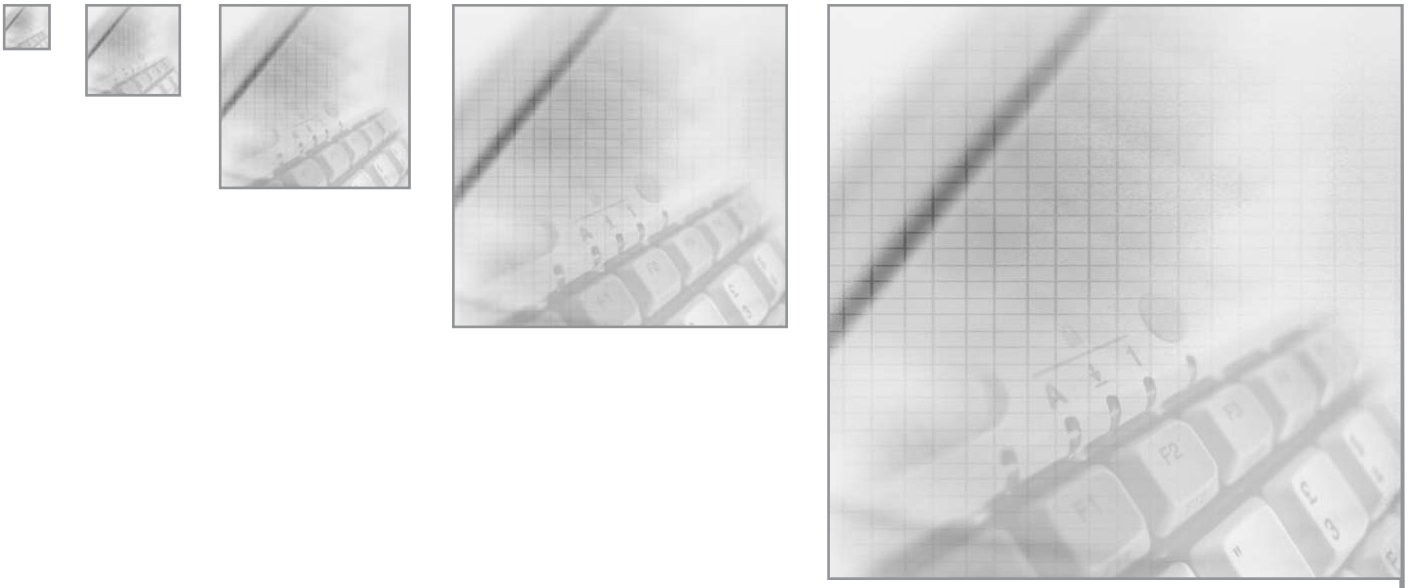
http://export.gov/safeharbor/SHPRINCIPLESFINAL.htm

SEARCH Compendium: *Compendium of State Privacy and Security Legislation: 2002 Overview, Criminal History Record Information*, Bureau of Justice Statistics, November 2003, NCJ 200030, available at

http://www.ojp.usdoj.gov/bjs/abstract/cspsl02.htm

Smith, Robert Ellis, *Compilation of State and Federal Privacy Laws*, The Privacy Journal, 2002, with 2004 Supplement, ISBN 0-930072-17-0, new 13-digit ISBN: 9780930072179, available through

http://www.privacyjournal.net/work1.htm



Appendix Four

Index of Subjects

References are to policy template sections and their associated commentary, not pages.

Access....B.7.00

Accountability....A.1.00 (i), B.1.00 (i), B.9.20, C.1.00 (i), and C.5.00

Agency....Definition in B.3.10

Aggregation (see also Merging)....B.4.20 (c)

Audit....B.9.20 (d) and (f) and C.5.10 (d)

Audit trail (see also Logging)....B.9.20 (d)

Biometrics....B.6.20 Commentary

Bulk distribution or download....B.7.40 (e)

Case management system (CMS)....Introduction, Audience, and B.4.10

Civil liberties....described in Introduction, Scope of Policy Templates

Civil rights....described in Introduction, Scope of Policy Templates

Computer Aided Dispatch (CAD) systems....B.4.10 (a) (1) Commentary

Confidential source....B.4.40 (a)

Corrections....Introduction, Audience, B.6.20 (b), and B.7.10 (a)

Criminal History Records Systems (CHRS).... Introduction, Audience, and B.4.10

Criminal Justice Integrated System (CJIS).... Introduction, Audience, and B.4.10

Critical infrastructure....B.7.30 (a)

Data integrity....B.5.00

Data quality....See Information quality

Defense counsel....Introduction, Audience, and B.7.10 (a)

Disclosure....B.7.00

DNA....B.6.20 Commentary

Enforcement....B.9.20, B.9.30, C.5.10, and C.5.20

Expungement....B.4.40, B.7.30 (b) Commentary, and B.8.20 Commentary

Fingerprints....B.4.10 and B.6.20 Commentary

First responder....A.1.00 (c), B.1.00 (c), B.7.20, and C.1.00 (c)

IAA....Interagency Agreement—Introduction, Organization of Policy Templates, fn. 6, and Part C

Informant....B.4.30 (a) and B.7.50 (b)

Information....Definition in B.3.20

Information quality....described in Introduction, Scope of Policy Templates, and B.5.10

Integrated Justice Information System (IJIS).... Introduction, Audience, and B.4.10

Jail Management System (JMS)....Introduction, Audience, and B.4.10

Joint Powers Agreement (JPA)....Introduction, Organization of Policy Templates, fn. 6, and Part C.

Law....Definition in B.3.30

Logging (see also Audit trail)....A.1.00 (i), B.7.10 (b), B.7.20 (b), B.7.30 (c), B.7.40 (c), B.7.50 (d), and B.9.20 (d)

Matching....see Merging

Merging....B.6.20

MOA....Memorandum of Agreement – Introduction, Organization of Policy Templates, fn. 6, and Part C

MOU....Memorandum of Understanding – Introduction, Organization of Policy Templates, fn. 6, and Part C

National Criminal Intelligence Sharing Plan (NCISP)....Introduction, Answering a Critical Need, Responding to the Field, fn. 2 and Introduction, Scope of Policy Templates

Need to know....B.7.10 (a), B.7.20 (a), C.3.10 (k), and C.3.20

Offender-Based Tracking System (OBTS).... Introduction, Audience

Parole....Introduction, Audience, and B.7.10 (a)

Pretrial Services....Introduction, Audience, and B.7.10 (a)

Privacy....described in Introduction, Scope of Policy Templates

Probation....Introduction, Audience, and B.7.10 (a)

Prosecution....Introduction, Audience, and B.7.10 (a)

Public....Definition in B.3.40

Public access....B.7.40

Public health....B.7.30

Public protection....B.7.30

Records Management System (RMS)....Introduction, Audience, and B.4.10

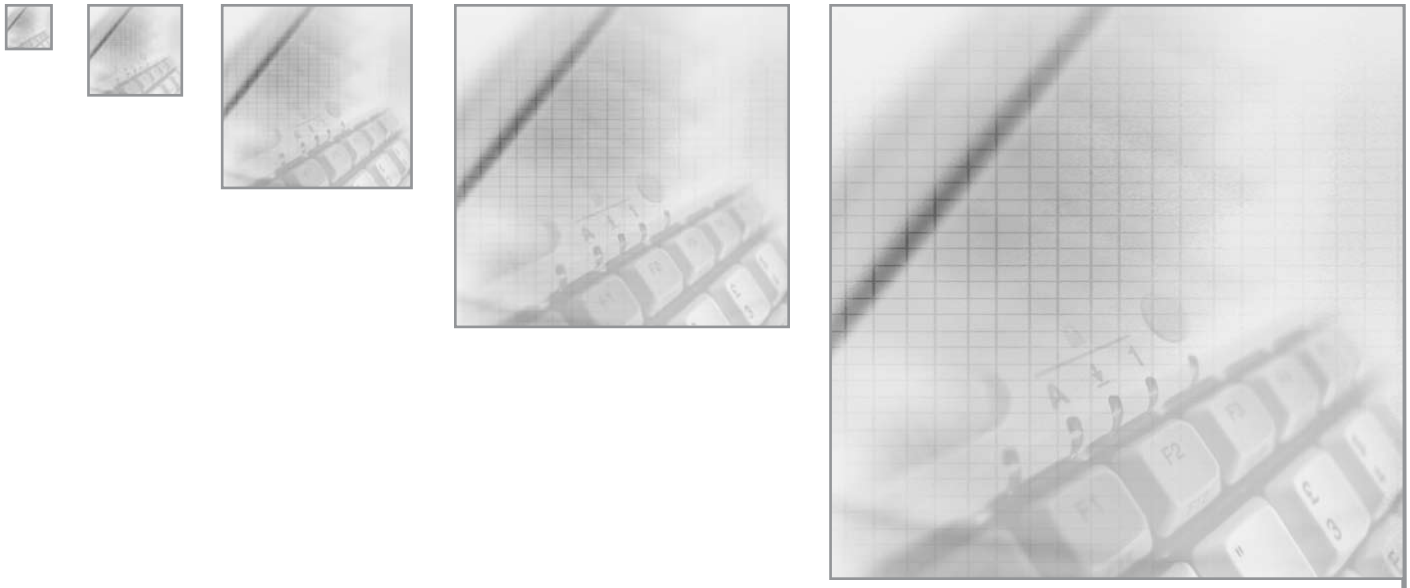
Right to know....B.7.10 (a) and C.3.10 (k)

Silent hit....C.3.20 (c)

Training....B.6.00 (a) (1), B.10.00, and C.5.10 (b)

Victim....A.1.00 (b), B.4.10 (b), B.4.30 (a), B.4.40 (a), B.7.00, and B.7.50 (b)

Witness....A.1.00 (b), B.4.10 (b), B.4.30 (a), B.4.40 (a), B.7.00, and B.7.50 (b)



Appendix Five

Cross-Reference to Privacy-Related Laws and Other Policies

The following list provides references to laws, policies, and other statements of policy addressing similar policy issues to those addressed in the template sections here. They are provided as examples from comparable policy situations, even though many of these are not applicable to justice information systems. Bibliographic information for the references is provided in Appendix Three. The items listed under each section heading are in alphabetical order.

A. Elements of Enabling Legislation or Authorization

A.1.00 Statement of Purpose

- 16 CFR Part 314, Section 314.3(b)
- 28 CFR Part 20, Section 20.1
- 28 CFR Part 23, Sections 23.1 and 23.30(e)
- CCJ/COSCA Guidelines, Section 1.00
- *Fusion Center Guidelines*, Mission Statement and Goals, Guideline 2
- IIR Sample Operating Policies and Procedures, Goals

A.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

- 28 CFR Part 23, Sections 23.1 and 23.2
- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 6.f
- NCISP, Recommendations 6 and 9
- RISS Privacy Policy

A.3.00 Agency Transparency and Accountability

- NCISP, Recommendation 14
- NCISP Recommended Outreach Plan, generally

B. Elements of a Basic Internal Operations Policy

B.1.00 Statement of Purpose

- See References under Section A.1.00

B.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

- See References under Section A.2.00

B.3.00 Definitions

B.3.10 Definition of Agency

- 28 CFR Part 23, Section 23.3(b)(4)
- DOJ Order on Safeguarding Unclassified Sensitive Information, Sections 2.a., 4.a., and 4.b

B.3.20 Definition of Information

- CCJ/COSCA Guidelines, Sections 3.10 and 3.40
- Computer Matching and Privacy Act, 5 U.S.C. § 552a(a)(4)

B.3.30 Definition of Law

- 28 CFR Part 20, Section 20.21(b)(2)

B.3.40 Definition of Public

- CCJ/COSCA Guidelines, Section 2.00

Other Definitions

Administration of Criminal Justice

- 28 CFR Part 20, Section 20.3(b)

Collect

- 16 CFR Part 313, Section 313.3(c)

Criminal Activity

- IIR Sample Operating Policies and Procedures, Definitions

Criminal History Record Information

- 28 CFR Part 20, Section 20.3(d)
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article I (4)

Criminal History Record Information System

- 28 CFR Part 20, Section 20.3(e)

Criminal Intelligence

- 28 CFR Part 23, Section 23.3(b)(1) and (3)
- IACP Model Policy, Section III
- *Law Enforcement Analytic Standards* definitions

Criminal Intelligence Information

- 28 CFR Part 23, Section 23.3(b)(3)
- IIR Sample Operating Policies and Procedures, Definitions

Criminal Intelligence System

- 28 CFR Part 23, Section 23.3(b)(1)
- IIR Sample Operating Policies and Procedures, Definitions

Dispose

- 16 CFR Part 682, Section 682.1(c)

Need to Know

- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 4.e
- IIR Sample Operating Policies and Procedures, Definitions

Nonpublic Personal Information

- 16 CFR Part 313, Section 313.3(n)(1)

Personal Identifiable Financial Information

- 16 CFR Part 313, Section 313.3(o)(1)

Personal Identifiable Information

- Alaska Statutes, Section 44.99.350 (2)
- California Business and Professions Code, Section 22577(a) regarding Internet sites
- California Civil Code, Section 1798.81.5 (d)(1)—"personal information" in databases
- Federal Internal Revenue Service, 26 U.S.C. 6103(b)(6), definition of "Taxpayer information"
- Washington Governor's Executive Order 00-03
- Wisconsin Statutes, Sections 19.62(5)

Publicly Available Information

- 16 CFR Part 313, Section 313.3(p)(1)

Reasonable Suspicion

- 28 CFR Part 23, Section 23.20(c)
- IIR Sample Operating Policies and Procedures, Information Submission Criteria
- IIR Sample Operating Policies and Procedures, Definitions

Right to Know

- IIR Sample Operating Policies and Procedures, Definitions

B.4.00 Seeking and Retaining Information

B.4.10 What Information May Be Sought or Retained

Generally

- Computer Matching and Privacy Act, § 552a(e)(1)
- IACP Model Statutes Project, section on Racial Profiling
- OECD Collection Limitation Principle Number 7
- OECD Purpose Specification Principle Number 9
- RISS Privacy Policy
- Safe Harbor Privacy Principles, Notice, Choice, and Data Integrity principles
- Washington Governor's Executive Order 00-03, item #4

B.4.10 Subsection (a) (2) – Criminal History Information Systems

- 28 CFR Part 20, Section 20.3(d)
- Arizona Revised Statutes, Section 41-1750

B.4.10 Subsection (a) (3) – Criminal Intelligence Systems

- 28 CFR Part 23, Sections 23.20(a), (b), and (n) and 23.3(b)(3)
- IACP, Criminal Intelligence Model Policy, Sections II, IV.C.3. and IV.F.1
- IIR Sample Operating Policies and Procedures, Information Submission Criteria and Inquiry Procedures

B.4.10 Subsection (c) – Improper Basis for Collecting Information

- IACP Model Statutes Project, section on Racial Profiling

B.4.10 Subsection (c) – Information Not to Be Collected

- 28 CFR Part 23, Section 23.20(l)
- Computer Matching and Privacy Act, § 552a(e)(7)

B.4.20 Methods of Seeking or Receiving Information

- 28 CFR Part 23, Sections 23.20(d) and (k)
- Computer Matching and Privacy Act, § 552a(e)(2)
- IACP, Criminal Intelligence Model Policy, Section IV.C.2
- IACP Model Statutes Project, section on Racial Profiling
- IIR Sample Operating Policies and Procedures, Information Submission Criteria
- OECD Collection Limitation Principle Number 7
- OECD Purpose Specification Principle Number 9
- RISS Privacy Policy

B.4.30 Classification of Information Regarding Validity and Reliability

- 28 CFR Part 23, Sections 23.3(b)(6) [definition of "validation of information"] and 23.20(g)
- GSWG, *Applying Security Practices to Justice Information Sharing*, Section 2-4 Data Classification, pp. 2-43 to 2-47
- IALEIA, *Law Enforcement Analytic Standards*, Standard Number 13, Evaluation Standard
- IIR Sample Operating Policies and Procedures, section on Content Validity
- IIR Sample Operating Policies and Procedures, section on Source Reliability
- OECD Purpose Specification Principle Number 9

B.4.40 Classification of Information Regarding Limitations on Access and Disclosure

- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 7.a
- IACP, Criminal Intelligence Model Policy provides classification categories for criminal intelligence information (see Section IV. H.1.)
- IALEIA, *Law Enforcement Analytic Standards*, Standard Number 23, Data Source Attribution Standard
- IIR Sample Operating Policies and Procedures, section on Dissemination Level
- OECD Purpose Specification Principle Number 9
- Safe Harbor Privacy Principles, Notice, Choice and Onward Transfer principles

B.5.00 Information Quality

Generally

- 20 CFR Part 20, Sections 20.1, 20.21(a) on completeness, 20.21(a)(2) on accuracy, 20.21(a)(2) on advising recipient agencies of errors, and 20.21(f)(3)(i)(a) on only authorized users changing data
- 28 CFR Part 23, Sections 23.20 (g) and (h)
- Computer Matching and Privacy Act, § 552a(e)(5) and (6)
- GSWG *Applying Security Practices to Justice Information Sharing*, Chapter 2, Section 3

- IIR Sample Operating Policies and Procedures, section on Notification Prior to Purge
- IALEIA, *Law Enforcement Analytic Standards*, Standard Number 12, Legal Constraints Standard, Standard Number 13, Evaluation Standard, and Standard Number 15, Analytic Accuracy Standard
- NCISP, Recommendations 11 and 12
- OECD Data Quality Principle Number 8
- Safe Harbor Privacy Principles, Data Integrity principle

B.6.00 Collation and Analysis of Information

B.6.10 Collation and Analysis

- IACP, Criminal Intelligence Model Policy, Sections IV. A. and E
- IALEIA, *Law Enforcement Analytic Standards*, Standard Number 14, Collation Standard
- NCISP, Recommendation 12

B.6.20 Merging of Information From Different Sources

- Colorado Rev. Stats., Section 24-72-305.4—Access to criminal history or arrest information for applicants for regulated professions—fingerprints for matching
- Computer Matching and Privacy Act, § 552a; definition of matching, § 552a(a)(8); matching agreement, § 552a(o); Data Integrity Boards, § 552a(u); law enforcement exception, § 552a(a)(8)(B)(iii), (v), and (vi)
- IIR Sample Operating Policies and Procedures, Information Submission Criteria
- Minnesota Statutes 2004, Chapter 13B—Matching Programs; Computerized Comparison of Data
- NASCIO Compendium, pp. 78-80
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article I (20) "positive identification," Article V (a), and Article V (e)
- Wisconsin Statutes, Sections 19.62(3) [definition of matching program] and 19.69

B.6.20 Subsection (b) – Independent Verification of Match

- Minnesota Statutes 2004, Section 13B.03
- Wisconsin Statutes, Section 19.67(b)

B.7.00 Sharing and Disclosure of Information

- Dissemination according to applicable laws
  - Florida Statutes, Section 934.053(1)

B.7.10 Sharing Information Within the Agency and With Other Justice System Partners

- 28 CFR Part 20, Sections 20.21(b)(1), (b)(3), (f)(2), and (f)(3)(i)(b), and Section 20.33(a)
- 28 CFR Part 23, Sections 23.20(e), (f), and (g)
- Florida Statutes Section 943.053(6) to public defenders
- Florida Statutes Section 943.053(7) to private entities contracting with a sheriff to run a detention facility; 943.053(8) to private entities operating correctional facilities for the state; and 943.053(9) to contracted juvenile assessment center or detention facility
- GSWG *Applying Security Practices to Justice Information Sharing*, Chapter 2, Section 2
- IACP Criminal Intelligence Model Policy, Section IV. C.4
- IIR Sample Operating Policies and Procedures, sections on Access Rights, Inquiry Procedures, and Dissemination of Information Procedures
- NCISP, Recommendation 27
- OECD Use Limitation Principle Number 10
- OECD Security Safeguards Principle Number 11
- Safe Harbor Privacy Principles, Onward Transfer principle

B.7.20 Sharing Information With Those Responsible for Public Protection, Safety, or Public Health

- 28 CFR Part 20, Sections 20.21(b)(2) and 20.33(a)
- 28 CFR Part 23, Sections 23.20 (f)(2) and (g)
- OECD Use Limitation Principle Number 10
- OECD Security Safeguards Principle Number 11
- Safe Harbor Privacy Principles, Inward Transfer principle

B.7.30 Sharing Information for Specific Purposes

- 28 CFR Part 20, Sections 20.21(b)(2) and (c)(1) on specific users and information they are entitled to access, and 20.21(b) (4) on research, evaluation and statistical uses
- 28 CFR Part 20, Section 20.21(c)(2) on nondisclosure of existence of information
- 28 CFR Part 20, Section 20.33(a) on information made available for specific uses
- 28 CFR Part 23, Section 23.20(f)(2) and (g)
- CCJ/COSCA Guidelines, Section 4.10

- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article IV (a)
- OECD Use Limitation Principle Number 10
- OECD Security Safeguards Principle Number 11

B.7.30 Access to Criminal History or Arrest Information for Applicants for Caregiver Positions

- Colorado Rev. Stats., Section 24-72-305.3 (2)(B)–clear language about what types of criminal information is available

B.7.30 Access to Criminal History or Arrest Information for Applicants for Regulated Professions

- Colorado Rev. Stats., Section 24-72-305.4; use of fingerprints for matching in Subsection (1)
- Safe Harbor Privacy Principles, Inward Transfer principle

B.7.30 Access to Criminal Records Information for Child Support Enforcement Agency

- Florida Statutes Section 943.053(5)

B.7.40 Disclosing Information to the Public

- 28 CFR Part 20, Section 20.20(b) on exceptions and 20.20(c) on disclosing criminal history information about an individual
- 28 CFR Part 23, Section 23.20(g)
- Federal Freedom of Information Act, 5 U.S.C. Section 552 (b) on exceptions to disclosure
- Federal Freedom of Information Act, 5 U.S.C. Section 552(a)(2) on redaction and disclosing existence of information not made available
- Florida Statutes Section 119.07(1)(b) and (c)—redaction of exempt portion of record and citation of authority to not provide
- New Jersey Statutes, Section 47:1A-3.b
- OECD Use Limitation Principle Number 10
- OECD Security Safeguards Principle Number 11
- Safe Harbor Privacy Principles, Onward Transfer and Security principles
- Washington Governor's Executive Order 00-03, item #3
- Wisconsin Statutes, Section 19.71 – sale of names and addresses

B.7.40 Subsection (d)—Fees for Obtaining Information

- CCJ/COSCA Guidelines, Section 4.30 and 4.40 on bulk and compiled access and section 6.00 on fees
- Federal Freedom of Information Act, 5 U.S.C. Section 552(a)(4) on charging fees

B.7.40 Subsection (e)—Bulk Access to Information

- CCJ/COSCA Guidelines, Sections 4.30 and 4.40

B.7.50 Disclosing Information to the Individual About Whom Information Has Been Gathered

- 28 CFR Part 16, Sections 16.30 – 16.34
- 28 CFR Part 20, Sections 20.21(g) and 20.34
- 28 CFR Part 23, Section 23.20 (g)
- Computer Matching and Privacy Act, § 552a Subsections (e)(3) and (f)
- Fair Credit Reporting Act
- New Jersey Statutes, Section 47:1A-3.a
- OECD Individual Participation Principle Number 13
- Safe Harbor Privacy Principles, Notice, Choice and Access principles

B.7.50 Subsection (c)—Review and Correction

- Computer Matching and Privacy Act, § 552a (p)

B.8.00 Information Retention and Destruction

B.8.10 Review of Information Regarding Retention

- 28 CFR Part 23, Section 23.20(h)
- IIR Sample Operating Policies and Procedures, section on Review and Purge Procedures
- RISS Privacy Policy
- Washington Governor's Executive Order 00-03, item #4

B.8.20 Destruction of Information

- 16 CFR Part 682, Section 682.3
- Federal Records Act, 44 U.S.C. Chapter 33, Sections 3303 (3) and 3303a (d)
- IIR Sample Operating Policies and Procedures, sections on Review and Purge Procedures, Procedures for Purge of Information, Purge Without Notification to Submitting Agency, Notification Prior to Purge, and Destruction of Information
- RISS Privacy Policy

B.9.00 Accountability and Enforcement

B.9.10 Information System Transparency

Generally:

- NCISP Recommended Outreach Plan
- OECD Openness Principle Number 12

B.9.10 Subsection (a)—Existence of System

- Computer Matching and Privacy Act, § 552a, Subsections (e)(4), (11) and (12) and Subsection (r)

B.9.10 Subsection (b)—Designating Responsible Person:

- 16 CFR Part 314, Section 314.4(a)
- Executive Order 12334 – President's Intelligence Oversight Board, Section 2
- IACP Criminal Intelligence Model Policy, Section IV.B.2—concept of "officer-in-charge" (OIC)
- IIR Sample Operating Policies and Procedures, Coordination and Control
- OECD Accountability Principle Number 14

B.9.20 Accountability for Activities

- 16 CFR Part 314, Section 314.4(b)
- 28 CFR Part 20, Sections 20.21(e) on audits, (f) on security provisions, (f)(3)(i)(a) on who can change information, (f)(3)(i)(d) on detecting attempted unauthorized use, and (f)(3)(i)(g) on protecting the system
- 28 CFR Part 23, Sections 23.20(g), (i), and (n), and 23.30(c) and (d)(1)
- Computer Matching and Privacy Act, § 552a(e)(9)
- IACP, Criminal Intelligence Model Policy, Section IV.B
- IIR Sample Operating Policies and Procedures, section on Inspection and Audit of Files
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article III (a)(1) and (b)(1)
- NCISP, Recommendation 15
- RISS Privacy Policy
- Safe Harbor Privacy Principles, Enforcement principle

B.9.20 Subsection (a)—Person/Position Responsible

- DOJ Order on Safeguarding Unclassified Sensitive Information, Sections 5.c. and 6.h

B.9.20 Subsection (b)—Protection From Destruction or Unauthorized Access

- GSWG *Applying Security Practices to Justice Information Sharing*

B.9.20 Subsection (d)—Compliance and Subsection f) – Audit

- 16 CFR Part 314, Section 314.4(c)
- Computer Matching and Privacy Act, § 552a (u)(3)(B)
- Washington Governor's Executive Order 00-03, item #5
- Wisconsin Statutes, Section 19.65(2)—Rules of conduct for employees

B.9.20 Subsection (g)—Updating of Policy

- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 8

B.9.20 Subsection (h)—Notification of Breach and Release of Information

- California

B.9.30 Enforcement

- 28 CFR Part 20, Section 20.21(f)(4)(ii)
- 28 CFR Part 23, Sections 23.20(g)(5) and (m)
- Computer Matching and Privacy Act, § 552a(q)
- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 5.b
- Federal Freedom of Information Act, 5 U.S.C. Section 552 (a)(4)(F)
- Safe Harbor Privacy Principles, Enforcement principle
- Washington Governor's Executive Order 00-03, item #5
- Wisconsin Statutes, Section 19.80

B.10.00 Training

- 28 CFR Part 20, Section 20.21(f)(5)
- CCJ/COSCA Guidelines, Section 8.30
- Computer Matching and Privacy Act, § 552a(e)(9)
- DOJ Order on Safeguarding Unclassified Sensitive Information, Section 5.b
- IACP Model Statutes Project, section on Racial Profiling
- IALEIA, *Law Enforcement Analytic Standards*
- NCISP, Recommendations 13, 18, and 19
- Washington Governor's Executive Order 00-03, item #5
- Wisconsin Statutes, Section 19.65

C. Provisions for a Multiagency Agreement for an Information Sharing System

C.1.00 Statement of Purpose

- See References under Section A.1.00

C.2.00 Compliance With Laws Regarding Privacy, Civil Rights, and Civil Liberties

- See References under Section A.1.00
- 28 CFR Part 23, Sections 23.1 and 23.2
- National Crime Prevention and Privacy Compact, 42 U.S.C. §14616, Article III (c)
- RISS Privacy Policy

C.3.00 Sharing of Information Among Participants

C.3.10 Expectations Regarding Information Gathered and Shared

- 28 CFR Part 20, Sections 20.21(a), 20.21(f)(3)(i)(f) and (f)(3)(i)(g), and 20.37
- 28 CFR Part 23, Sections 23.20(e) and (h) and 23.30(d)(2)
- IIR Sample Participation Agreement
- National Crime Prevention and Privacy Compact, 42 U.S.C. Section 14616, especially Article III (c)

C.3.10 Subsection (g)—System Security

- For a summary of security provisions, see IIR Sample Operating Policies and Procedures, section on Security of SIS Files

C.3.10 Subsections (i), (j) and (k)

- *Applying Security Practices to Justice Information Sharing*, Chapter 2, Section 2

C.3.20 Sharing Information With Other Justice System Partners

- IIR Sample Operating Policies and Procedures, section on Dissemination Level

C.4.00 Use and Disclosure of Information Originating From Another Participating Agency

C.4.10 Disclosure of Information According to Originating Agencies Access Rules

- Florida Statutes, Sections 119.071(2)(b) and 934.053(2)
- IIR Sample Operating Policies and Procedures, Section on Dissemination Level
- Washington Governor's Executive Order 00-03, item #5

C.4.20 Reporting Possible Information Errors to the Originating Agency

- 28 CFR Part 23, Section 23.20 (h)

C.5.00 Participating Agency Accountability and Enforcement

C.5.10 Expectations Regarding Accountability and Enforcement

- IIR Sample Operating Policies and Procedures, section on Inspection and Audit of Files
- IIR Sample Operating Policies and Procedures, Participation—on designated contact person for receiving reports of alleged errors
- National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, Article II (5), Article III (c), and Article IV (c)

C.5.20 Enforcement of Provisions of Information Sharing Agreement

- 28 CFR Part 20, Section 20.38.

Appendix B
Privacy and Information Quality Policy Development for the Justice Decision Maker

Geared toward the justice executive to engender awareness about the privacy and privacy policy development, *Privacy and Information Quality Policy Development for the Justice Decision Maker* is a high-level, easy-to-read booklet that makes the case for privacy policy development and underscores the *imperativeness* of leadership in promoting privacy issues within justice agencies. Developed by the Global Privacy and Information Quality Working Group (GPIQWG) and supported by the U.S. Department of Justice's (DOJ) Office of Justice Programs (OJP), this paper is an excellent primer and educational tool that applies settled privacy principles to justice information sharing systems, addresses applicable legal mandates, and makes recommendations on best practices to ensure privacy and information quality.

Recognizing the need for tiered privacy policy-related material, GPIQWG members produced the two documents, *Privacy Policy Development Guide and Implementation Templates* and the *Privacy and Information Quality Policy Development for the Justice Decision Maker*, as companion resources that can be used in tandem or separately, depending on the audience.

Privacy and Information Quality Policy Development for the Justice Decision Maker

Global Justice Information Sharing Initiative

United States Department of Justice

Highlights

- Since 9/11, virtually all agree that enhanced justice information exchange is critical. While pursuing a broadscale sharing capability, decision makers within the justice and public safety communities must vigorously protect our constitutional privacy rights and ensure information quality and accuracy. In short: *you need privacy and information quality policies to guide your agency's information sharing efforts.* Difficult? Yes. Insurmountable? No. Many good resources already exist to help justice and public safety leaders make the best possible business decisions on privacy and data quality for their information sharing practices. This document serves as an additional tool.

- Privacy and information quality policies protect your agency and make it easier to do what is necessary—share information. Focus on these policies will (1) strengthen public confidence in your agency's ability to handle information appropriately, (2) strengthen support for your agency's information management efforts through developing technologies, and (3) ultimately promote effective and responsible sharing of information that supports those fundamental concepts of the justice system we embrace as Americans.

- In today's information sharing environment, well-developed privacy and information quality policies help an agency prevent problems. Failure to develop, implement, and maintain dynamic privacy and information quality policies can result in:

  - Harm to individuals.
  - Public criticism.
  - Lawsuits and liability.
  - Inconsistent actions within agencies.
  - Proliferation of agency databases with inaccurate data.

  Each agency should evaluate and strengthen privacy and information quality policies to make them more relevant to twenty-first century technology.

- Privacy and information quality concerns directly affect the whole justice community, including law enforcement, prosecution, defense, courts, parole, probation, corrections, and victim services, as well as members of the public having contact with the justice system. The personally identifiable information maintained by agencies—if handled inappropriately—can cause problems for those affected. In worst cases, personal safety is jeopardized.

- Success of privacy and information quality policy improvement efforts depends on appointing a high-level member of your agency to champion the initiative. That person should assemble a policy development-and-review team of agency stakeholders, including managers, legal staff, system operators, technical support staff, and other personnel responsible for information management. The team must have the power to both develop and analyze a plan and then implement that plan. The plan must include input and review from interested and/or affected persons outside of the agency.

- Processes developed when most records were on paper may not translate well in the electronic and digital age. A privacy and information quality policy development-and-review effort will promote and facilitate modern information management and help you remain in control of your agency's technologies.

- The process promoted here does not require you to "start from scratch." There are historical and increasingly accepted "Fair Information Practices" to guide your agency's efforts.

- This document introduces the framework for a systematic consideration of privacy and information quality policies and practices within your agency. A companion *Privacy Policy Development Guide* has been designed by the U.S. Department of Justice's Global Privacy and Information Quality Working Group to assist your team in its efforts to develop or revise agency privacy and information quality policies.

Foreword: What's in This for Me?

You would be hard-pressed to find an opposing view: justice and public safety leaders—indeed, the American public—want justice-related entities to do a better job of sharing information to promote the well-being of our citizens and local neighborhoods and to protect homeland security. With the continually advancing field of technology, the technical capability to solve information sharing challenges now exists. If you can access your bank account as easily in Duluth, Minnesota, as you can in Tokyo, Japan, surely an officer in one county can share sex offender data with a parole worker in the neighboring town. But justice leaders know all too well the unfortunate truth—sharing information is not a given. While pursuing a critical, broadscale justice information sharing capability, decision makers must simultaneously ***vigorously*** protect citizens' constitutional rights. In short, *privacy and information quality policies are needed to guide agency information sharing efforts.* We may want our justice leaders to exchange information, but we want that sharing to be *appropriate*, we want that information to be *accurate,* and we demand safeguards be in place to protect our individual rights. Difficult? Yes. Insurmountable? Not at all.

Many good resources and guidelines have been created to assist justice leaders in making the best business decisions for information sharing.

Since 1998, the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ), has supported a group of your peers to tackle these exact concerns. DOJ's Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) addresses timely justice-related information sharing issues, such as questions of privacy and information quality. What follows, developed by the Global Privacy and Information Quality Working Group, is a sound first step in this area: a blueprint for initiating and completing a process to ensure that your agency develops and maintains essential privacy and information quality policies involving the collection, use, and dissemination of information. Additional resources that address the range of justice and public safety leaders' information sharing challenges and opportunities are included in "Global Resources for the Justice Decision Maker," concluding this document.

Introduction

Should you be concerned about developing or reviewing your agency's privacy and information quality policies? Ask yourself:

1. ***Does my agency control, disclose, or provide access to information to persons or agencies outside of my organization?***

2. ***Does my agency's information system(s) contain data or information connected to or shared with other information systems or agencies?***

3. ***Does my agency collect, use, or provide access to "personally identifiable information" (information that identifies individuals by reason of the content)?***

4. ***Does my agency have a stake in the accuracy of the information it manages?***

A "yes" to any of the above questions suggests that your agency should make it a priority to review privacy and information quality practices. Government policymakers and agency heads must take action to cause that review to occur.

Increasingly, the sharing of information is ***key*** to agency success in the twenty-first century. The ease of sharing information promoted by new technologies and the vital importance of ensuring that information is accurate make the implementation and maintenance of privacy and information quality policies and practices essential to any agency's information operations. With the growth in the assimilation, utilization, and sharing of **personally identifiable information**—information that can be linked to individuals—that has come with modern technologies, effective measures to ensure appropriate levels of privacy protection are increasingly important. Additionally, information created or compiled by your agency must be accurate or it is of little value. When you share information with another entity, there is the implicit expectation that the data you provide is *accurate* and that there are steps to ensure *information quality*; likewise, you expect the same from other agencies when receiving information. Promoting information quality by internal safeguards and procedures helps to ensure the accuracy of the information you handle.

Unless effective privacy and information quality safeguards are being utilized at every level of your agency's information and data-handling operation, you may be exposing yourself and others to unacceptable risks from inaccurate information or problems caused by failing to honor essential privacy expectations. When agencies collectively maintain appropriate levels of attention to privacy and information quality, the sharing of information is facilitated in a responsible and effective manner.

Having a "security policy" related to data or information is not enough. Security policies alone do not adequately address the privacy and information quality issues contemplated in this discussion. Although *privacy* and *security* both relate to handling data and information—and are both essential to justice-related information sharing[1]—they have different implications and considerations. "Security" relates to how an organization protects information during and after collection. "Privacy" addresses why and how information is collected, handled, and disclosed and is concerned with providing reasonable quality control regarding that information. Considering the breadth of the issue, some existing "privacy policies" may

fail to address these concerns in that they relate to *access to records* instead of defining privacy protections.[2]

Using computers to share databases and cross-reference digital information has heightened privacy and information quality concerns. Yet, as a practical matter, privacy and information quality policies and procedures affect every aspect of an agency's work, not just technology and operations. These concerns involve agency policy aspects, legal considerations, public relations, and interagency relationships. It is essential that agency leaders demonstrate an appreciation of the importance of these issues by appointing an influential member of agency management to champion the policy development initiatives proposed herein. Because adoption of a privacy policy may require a change in an agency's procedures, it may require a corresponding shift in agency "mind-set." The involvement of a high-level member of the administration will help ensure that the necessary changes are accepted and implemented.

As a justice or public safety leader, if you are still unsure about the fundamental importance of privacy and information quality safeguards, picture your agency in the following scenarios.

Case Studies: Is Privacy and Information Quality an Issue?

In December 2002, former U.S. Drug Enforcement Administration agent Emilio Calatayud was sentenced to prison and fined on charges related to his use of protected law enforcement computer systems and databases. He obtained information from these protected systems, which he then provided to a Los Angeles private investigation firm in return for at least $22,500 in secret payments.

Ensuring that those within your agency honor privacy restrictions is essential. They cannot honor that which is not clearly defined and articulated.

A private investigator hired by an obsessed fan was able to obtain the address of television and film star Rebecca Schaeffer through her California motor vehicle records. The fan used this information to stalk and to kill Schaeffer. The Driver's Privacy Protection Act (Public Law 103-322) was passed in 1994 in reaction to this stalking death, enhancing the privacy protections for driver's license information.

Having good information quality and privacy controls in place will help to reduce the possibility of agency criticism and can help defer criticisms when they occur.

An Ohio man's social security number was accidentally associated with another individual's criminal history record. After losing his job, home, and family, the man became aware of the mistake within a law enforcement information system. While the man was able to have the data corrected within the law enforcement system, he was unable to reverse—or even stem—the continuing damage caused by the mistake. The false information was contained in data sold to private information vendors that was, in turn, distributed nationally. There was no way to trace all disseminations of the erroneous information. At any time, the erroneous information can resurface to falsely attribute this man with a criminal history record.

Ensuring the accuracy of data your agency creates, compiles, and distributes is crucial. Failure to do so can have severe impact on the lives of innocent people.

Recently, the Texas Department of Public Safety proposed incorporating facial recognition biometrics into its driver's license photograph database to help stop the issuance of licenses to those using deception or fraud. The proposal passed with little debate in the Texas Senate but came to an abrupt halt in the Texas House of Representatives. Privacy-related concerns about the use of new technology, raised by the American Civil Liberties Union (ACLU) and others, led to a lopsided defeat of the proposal. Concerns about what the system "might" do overshadowed the value of what it was intended to do.

Ensuring that controls are in place for how information is used in your agency will assist your agency in justifying new initiatives and answering concerns about potential abuses of information.

These case studies highlight the importance of addressing privacy concerns when collecting, using, and disseminating **personally identifiable information**. Privacy and information quality ***are*** issues that ***must*** be addressed within every agency in the criminal justice system.

Moving From Concept to Action

The case for maintaining effective policies related to privacy and information quality has been made. Now, how should an agency respond? By ensuring that it has in place appropriate and relevant policies addressing the management of information. The following is a blueprint for agency action.

Start Right: Assign the Task to an Influential Member—

The development of privacy policies must be assigned to someone with the ability to "stick to the task" and remain focused on what needs to be done. Unless the person assigned this task is recognized as having a high level of authority, it may be difficult to obtain acceptance of the efforts made. This project manager should be a person who has the power to enlist the assistance of others within the organization to undertake the analysis and implement the efforts needed to systematically develop the policies and procedures. The project manager should be a person who can directly report to chief policymakers and chief administrators, while at the same time holding others accountable for their efforts, in order to ensure that the project remains on task. The project manager must be able to build an effective project team to make the effort successful in a reasonable length of time.

Have a Good Foundation: Establish a Project Team—

A project team should include stakeholders from within the agency

who are affected by privacy and information quality issues. A typical team will include technical staff familiar with system development and operation; those who use the system(s) regularly in their work; agency legal staff; persons able to craft policy language in a manner consistent with agency formats and expectations; and others having a key role in the agency's collection, maintenance, use, dissemination, and retention of information.

Use a Systematic Approach: Begin the Efforts—

- *Recognize the Stakes:* Implementation of new technologies may promote cost savings and efficiency yet still run afoul of privacy concerns and objections. Unaddressed privacy issues can overwhelm the arguments of benefits and cost savings in support of new technologies. If policymakers and the public are not comfortable with an agency's ability to responsibly handle information, the concerns and fears expressed by even a few opponents can lead to rejection of sensible initiatives.

- *Define Broad Objectives and Risks:* Early in the process, in considering the agency's mission and the substance of its initial efforts, the team should develop broad policy objectives and determine the risks to both public safety and protection of individual rights. Do not forget to include analysis of victims' issues when defining risks. Victim-related information requires careful privacy policy consideration; violations of personal privacy may mean life or death for victims of domestic violence and other crimes.

  Once the policy objectives are developed, the agency's top policy leaders (e.g., key legislators, executive branch heads, court administrators, or chief judges/justices) should be given an opportunity to endorse the objectives. With this agency buy-in of broad objectives and goals, actual policy development or revision can begin. Decisions should reasonably balance efforts to protect individual rights against the overall public safety mission of the agency and justice system. The risks inherent in any determination should be carefully evaluated and considered.

- *Capitalize Upon the Value of External Input:* An important early step in the development or revision efforts is to seek outside input from legislators, community advocates, victims' advocates, media representatives, privacy advocates, commercial information services sector members, representatives of agencies with whom you share information, and citizens or other interested parties. Broad stakeholder input will help define the focus of your efforts, provide innovative ideas, and support final decisions and plans. You should invite input from those who will use the information your agency maintains, as well as from those who may be critical of your agency's efforts.

  The input of these "outside sources" can help the project team obtain a balanced perspective and become aware of areas or concerns that might otherwise be overlooked. Opposition to or support for initiatives can come from unexpected places; therefore, including sources in the information-gathering stage that are likely to criticize, oppose, or support your policy efforts may help you identify and address issues more effectively. Involvement in the process that leads to a sense of policy "ownership" promotes the overall integrity of the initiative.

- *Define Applicable Laws and Regulations:* An essential early task is the review and identification of all relevant privacy laws and regulations. Every agency should be mindful of legal and regulatory obligations or restrictions applicable to agency operations. Privacy impact assessments may be required by law or regulation. Major policy issues, such as those related to public access to information, disclosure of information solely at agency initiative, protection of sensitive or confidential information, and public notification laws, need to be considered. Provisions of law or rule will need to be interpreted and applied to agency actions. This may be one of the more difficult steps in the overall effort, since there are a myriad of laws and regulations that affect information management and privacy. Some states and other jurisdictions now have chief privacy officers who may provide assistance in these efforts.

- *"Chart" Your Information Flow and Processes:*[3] Having a comprehensive understanding of the flow of information and information processes within your agency is essential. Creating "data and information flowcharts" that identify key points when privacy issues are implicated will assist in gaining that understanding. The chart should indicate when privacy or information quality issues are

implicated by the collection, use, or dissemination of personal information. To the extent possible, your agency should create audit logs or trails to track what personal information is being accessed and by whom. When an agency shares or obtains information with others outside the agency, a separate analysis of that data and information flow should be completed. Any comprehensive privacy or information quality policy must address the key points in the flow of information.

- *Apply "Fair Information Practices" Guidelines:* Any review of privacy and information quality principles should consider what are referred to as "Fair Information Practices," or FIPs. These eight basic FIPs were developed and formalized in the early 1980s to address issues related to the commercial use and sharing of personally identifiable information. Although the FIP guidelines are over 20 years old and were developed in a commercial context, they still constitute the basis upon which sound information quality and privacy policies can be developed. Since the FIPs are well known and widely accepted, outside interests reviewing your policies are likely to use them when providing input or voicing criticism. The FIPs are designed to:

  1. Define agency purposes for information to help ensure agency uses of information are appropriate. ("Purpose Specification Principle")
  2. Limit the collection of personal information to that required for the purposes intended. ("Collection Limitation Principle")
  3. Ensure data accuracy. ("Data Quality Principle")
  4. Ensure appropriate limits on agency use of personal information. ("Use Limitation Principle")
  5. Maintain effective security over personal information. ("Security Safeguards Principle")
  6. Promote a general policy of openness about agency practices and policies regarding personal information. ("Openness Principle")
  7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. ("Individual Participation Principle")
  8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. ("Accountability Principle")

  Each agency must evaluate the applicability and appropriateness of these FIPs in the context of its mission and responsibilities. The FIPs provide a framework for a systematic review of privacy and information quality policies and practices. They help agency leaders to understand which information quality and privacy protection efforts are important and needed. However, the FIPs are guidelines, not absolutes. For example, some agencies may need to ensure that articulation and policy implementation of the "Use Limitation Principle" do not unduly restrict the agency's use of information. The eight FIPs are summarized at the end of this document.

- *Implement, Train, and Hold Accountable:* The team should develop a training plan that will reach all within the agency who will be responsible for implementing or abiding by the privacy policies.

  The training plan should take into account the role and duties of those being trained. Methods of holding agency members accountable for abiding by the policies should be identified and incorporated into training. For example, unauthorized access to an agency's data or information by an agency member may form the basis for internal discipline but may *also* constitute a criminal violation of state law. The ramifications of a violation of the agency privacy policy should be clearly identified in agency training. Agency personnel should be required to engage in "refresher training" from time to time.

- *Test and Evaluate:* Finally, once implemented, the developed policy should be tested to determine whether it truly results in the anticipated privacy protections. A programmed review of the results of the policy implementation, including a planned feedback mechanism, should be factored into the policy itself. Each policy should be reviewed on a regular basis to ensure it continues to address changes in the law, as well as current agency practices. In addition, the review should include analysis of technological advancements that may enhance implementation of the policy. One method of ensuring such review is to "sunset" the policy on a certain future date, requiring the policy to be reviewed and renewed prior to its expiration.

Conclusion

Modern information management realities demand that agencies develop and implement comprehensive privacy and information quality policies, incorporating good information practices and design principles. Many agencies have few (if any) policies in place, while others may be dealing with privacy and information quality issues on a case-by-case basis. A systematic, developmental approach will ensure that issues and concerns are addressed before individual harm occurs or practices become a matter of agency or administrator embarrassment, criticism, or liability.

By initiating the development of comprehensive privacy and information quality policies in a systematic manner, policymakers and chief administrators can help ensure that their operations reasonably and fairly address privacy and information quality concerns. The careful selection of a high-level project manager and implementation of a balanced project team approach will significantly enhance the opportunity for the effort to be successful. Use of generally recognized FIPs to structure the policy development will facilitate the overall effort.

To assist those assigned the responsibility of implementing the approach suggested here, a ***Privacy Policy Development Guide*** is being developed to better outline the process and provide access to supplementary resources. These additional tools will facilitate actual privacy and information quality policy development or the review of these efforts. The Guide is designed to help those in charge handle their important privacy-related activities efficiently and effectively.

Footnotes

1 DOJ's Global Advisory Committee has formed working groups to handle both information sharing "security" and "privacy" issues. Please see "Global Resources for the Justice Decision Maker" at the end of this document for further information.

2 Many agencies have what is labeled a "privacy policy." In reality, many of these policies simply address the process by which outside entities obtain information from the agency under the federal Freedom of Information Act or the local "public records access" equivalent. While having a policy that defines information disclosure under applicable public records law is an aspect of a systematic approach to privacy and data management, such a policy does not address the issues and concerns that are the focus here. Such a policy is a step in the right direction but does not complete the journey.

3 SEARCH, The National Consortium for Justice Information and Statistics (with funding from the Bureau of Justice Assistance) has done extensive work with the Justice Information Exchange Model (JIEM) Project to facilitate the charting of your information flow. Information about the JIEM Project, including project documents and training opportunities, is available at www.search.org/integration/info_exchange.asp.

Fair Information Practices—Basic Principles

1. *Purpose Specification Principle*
   Identify the purposes for which all personal information is collected, and keep subsequent use of the information in conformance with such purposes.

2. *Collection Limitation Principle*
   Review how personal information is collected to ensure it is collected lawfully and with appropriate authority, and guard against the unnecessary, illegal, or unauthorized compilation of personal information.

3. *Data Quality Principle*
   Implement safeguards to ensure information is accurate, complete, and current, and provide methods to correct information discovered to be deficient or erroneous.

4. *Use Limitation Principle*
   Limit use and disclosure of information to the purposes stated in the purpose specification, and implement realistic and workable information-retention obligations.

5. *Security Safeguards Principle*
   Assess the risk of loss or unauthorized access to information in your systems, and ensure ongoing use conforms to use limitations.

6. *Openness Principle*
   Provide reasonable notice about how information is collected, maintained, and disseminated by your agency, and describe how the public can access information as allowed by law or policy.

7. *Individual Participation Principle*
   Allow affected individuals access to information related to them in a manner consistent with the agency mission and when such access would otherwise not compromise an investigation, case, court proceeding, or agency purpose and mission.

8. *Accountability Principle*
   Have a formal means of oversight to ensure the privacy and information quality policies and the design principles contained therein are being honored by agency personnel.

Global Resources for the Justice Decision Maker

Visit www.it.ojp.gov/global

United States
Department of Justice

Since 1998, the U.S. Department of Justice's (DOJ) **Global Justice Information Sharing Initiative (Global) Advisory Committee** (GAC or "Committee") has concentrated its diverse expertise on challenges to and opportunities for justice and public safety data exchange. Members of this federal advisory committee actively pursue broadscale information sharing, communicating their recommendations directly to the nation's leading justice official—the U.S. Attorney General.

Being intimately acquainted with practitioners' demands, GAC representatives are particularly gratified to support the development and distribution of resources for those in the field—they, too, are producers, consumers, and administrators of the same crucial justice-related data.

To use an automobile analogy, ***Privacy and Information Quality*** concerns are just one wheel on the Global car. ***Intelligence, Infrastructure/Standards,*** and ***Security*** solutions are necessary to drive justice information sharing forward. To that end, GAC's advice and counsel have yielded the following resources to help justice officials make the best business decisions possible:

- The ***National Criminal Intelligence Sharing Plan*** (Plan) provides a cohesive vision and practical solutions to improve law enforcement's ability to detect threats and protect communities. The office of the U.S. Attorney General has endorsed the Plan and is committed to making the resources available to carry out its goals.

- The **Global Justice Extensible Markup Language (XML) Data Model (Global JXDM)**—What began in March 2001 as a reconciliation of data definitions evolved into a broad endeavor to develop an XML-based framework to enable the entire justice and public safety community to effectively share information at all levels of government—laying the foundation for local, state, tribal, and federal justice interoperability.

- ***Applying Security Practices to Justice Information Sharing*** is a field compendium of current best practices and successful models for justice-related information technology (IT) security. The publication covers key IT security topics from detection and recovery to prevention and support.

- The **Justice Standards Clearinghouse for Information Sharing** is a Web-based standards clearinghouse promoting a central resource of information sharing standards and specifications that have been developed and/or implemented across the nation.

- The **OJP IT Initiative/Global Justice Information Sharing Initiative Web site** is a comprehensive "one-stop shop" developed for interested justice and public safety practitioners at all levels of government and all stages of the information sharing process. In addition to housing the resources outlined above, topics include:

  - GAC publications, minutes, presentations, and announcements.
  - Featured information sharing initiatives and organizations.
  - Computer system information exchange processes.
  - New policy and technology developments.
  - Model information sharing systems.
  - Information sharing "lessons learned."
  - Promising practices.
  - Peer-to-peer networking.
  - Events calendar.
  - Latest justice IT news.

For updates and access to all above resources, visit www.it.ojp.gov/global. To speak with someone about DOJ's Global Initiative or GAC events—including biannual GAC meetings open to the public—or obtain hard copy documents, please call Global staff at (850) 385-0600, extension 285.

BJA

This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Appendix C
Case Study

Illinois Criminal Justice Information Authority (ICJIA) and Illinois Integrated Justice Information System (IIJIS)

Introduction

In 2002, the Illinois Criminal Justice Information Authority (ICJIA) and the Illinois Integrated Justice Information System (IIJIS) Implementation Board initiated development of a privacy policy for all criminal justice entities in the state of Illinois. Leaders of the Illinois project also serve on the Global Privacy and Information Quality Working Group (GPIQWG) and contributed significantly to the development of this *Privacy Policy Development Guide and Implementation Templates*. This case study memorializes the Illinois effort and includes information on planning, project team development, project process, products produced, and lessons learned.

The Illinois initiative convened a project team, identified the scope of existing privacy policy and laws, and identified gaps in the law and issues to address for the development of an effective and comprehensive privacy policy. The Illinois project team is currently finalizing its privacy policy and will make it available through the ICJIA Web site www.icjia.state.il.us/public.

Background

Illinois Criminal Justice Information Authority (ICJIA)

Created in 1983, the Illinois Criminal Justice Information Authority (ICJIA) is a state agency dedicated to improving the administration of criminal justice. The ICJIA works to identify critical issues facing the criminal justice system in Illinois and proposes and evaluates policies, programs, and legislation that address those issues. The ICJIA also works to ensure that the criminal justice system in Illinois is as efficient and effective as possible. Created by the Illinois Criminal Justice Information Act, 20 ILCS 3930/1-14, ICJIA is charged with, among other things:

- Developing and operating comprehensive information systems for the improvement and coordination of all aspects of law enforcement, prosecution, and corrections;
- Defining, developing, evaluating, and correlating state and local programs and projects associated with the improvement of law enforcement and the administration of criminal justice;
- Monitoring the operation of existing criminal justice information systems in order to protect the constitutional rights and privacy of individuals about whom criminal history record information has been collected; and
- Providing an effective administrative forum for the protection of the rights of individuals concerning criminal history record information.

Illinois Integrated Justice Information System (IIJIS)

In 2001, Illinois Executive Order Number 12 created the Illinois Integrated Justice Information System (IIJIS) Governing Board. The IIJIS Governing Board, charged with coordinating and directing the state's integrated justice planning efforts, developed the *IIJIS Strategic Plan* and identified the stated goal of serving "justice, public safety, and homeland security needs while protecting privacy, preventing unauthorized disclosures of information, and allowing appropriate public access" (www.icjia.state.il.us/IIJIS/public/pdf/strategicplan_final.pdf). The IIJIS Strategic Plan further stated:

> *The broad interests of justice, public safety, and homeland security initiatives must be addressed while respecting individual privacy interests, preventing unauthorized disclosures of information, and enabling appropriate public access to relevant information. To prevent unauthorized disclosures of information while allowing appropriate access, a uniform privacy policy must be developed based upon fair information practices and adopted by all Illinois justice agencies.*

As in many states, Illinois has a patchwork of existing privacy statutes, regulations, rules, and policies that control the sharing and protection of justice information. While each Illinois justice entity had some experience and expertise in protecting and managing privacy issues of the information they owned based on the statutes, regulations, policies, and practices that governed that agency, there was no comprehensive privacy policy that applied to all Illinois justice agencies or that facilitated sharing of justice information among different justice entities. To address this problem and to implement the *IIJIS Strategic Plan*, Illinois Executive Order Number 16 (2003) created the Illinois Integrated Justice Information System (IIJIS) Implementation Board. The IIJIS Implementation Board's role is to:

- Coordinate the development, adoption, and implementation of plans and strategies for sharing justice information;
- Establish standards to facilitate the electronic sharing of justice information;
- Develop policies that protect individuals' privacy rights related to the sharing of justice information; and
- Secure and administer the funding of integration projects.

The *IIJIS Strategic Plan* called for development of a comprehensive IIJIS Privacy Policy. The effort involved initial adoption of privacy principles and development of a statewide privacy policy. The project team's process, products, and lessons learned are the subject of this case study.

A Comprehensive Privacy Policy

The project team's initial objective (refer to Section 6.1.4, Goals and Objectives) was to draft an original comprehensive privacy policy for all Illinois justice agencies, from the ground up, building from the Fair Information Practices (FIPs). Over time, the project team recognized that certain privacy polices already existed in the form of enacted statutes, regulations, policies, and procedures. As a result, the team added this objective to include the identification of existing laws and policies, analyses of this existing framework, and the identification of gaps or areas in the framework that remained unaddressed.

Project Team

Two staff members of the Illinois Criminal Justice Information Authority (ICJIA), an analyst and the ICJIA General Counsel, led the project team. These two team members prepared all of the materials for the project team meetings and led the initiative. In determining team membership, the team leaders relied upon preexisting relationships with agencies. The team leaders determined in advance what entities should be represented and then made their selections. Individual team members were selected based on the need for certain stakeholders to be represented but also for their expected contributions to the group effort. Team members' skills and abilities to contribute to the process were primary selection criteria for team leaders (refer to Section 5.4.1, Project Team).

The members of the project team included representatives from:

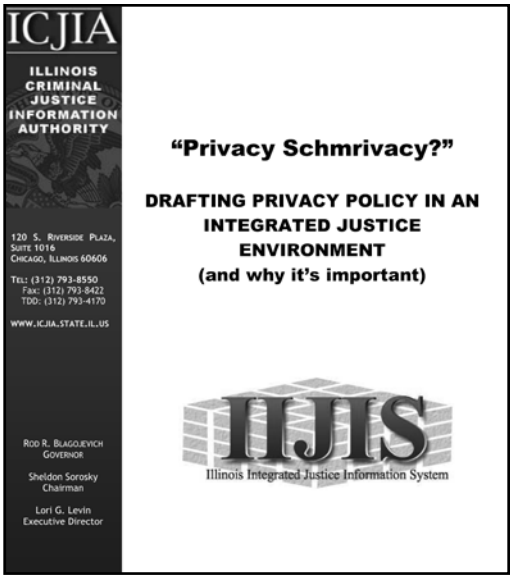
- Illinois Press Association
- Illinois State Police
- Chicago Police Department
- Illinois Association of Chiefs of Police
- Illinois Public Defender Association
- Office of the State Appellate Defender
- Metro Chicago Health Care Council
- Law school professors from Chicago-Kent College of Law and The John Marshall Law School
- Illinois Attorney General's Office
- Administrative Office of Illinois Courts
- Office of the Chief Judge, Circuit Court of Cook County
- Illinois Probation and Court Services Association
- Illinois Association of Court Clerks
- Illinois State's Attorneys' Association
- Illinois Coalition Against Domestic Violence
- Illinois Coalition Against Sexual Assault
- Illinois Sheriffs' Association

The team also sought representation from the following agencies:

- Chicagoland Chamber of Commerce
- Illinois Retail Merchants Association
- Illinois Department of Corrections
- Illinois Secretary of State's Office
- American Civil Liberties Union

Planning

At the outset of this initiative, the project leaders wrote a guidance document, *Privacy Schmrivacy: Drafting Privacy Policy in an Integrated Justice Environment (and why it's important)*, published in June 2004, as a primary planning document. It made the case for why the development of a privacy policy was necessary, provided background information, and laid out the process: www.icjia.state.il.us/iijis/public/pdf/PRV/PrivacySchmrivacy_FINAL.pdf (refer to Section 6, Planning). It was used as a primer on the privacy issues, both for the project team members and project team leaders. It provided team members with an understanding of the fundamentals of the privacy issue, including background on the fair information practices, and recommendations for the work of the team and how that work would take place.


ICJIA
ILLINOIS CRIMINAL JUSTICE INFORMATION AUTHORITY

120 S. Riverside Plaza, Suite 1016
Chicago, Illinois 60606

Tel: (312) 793-8550
Fax: (312) 793-8422
TDD: (312) 793-4170

www.icjia.state.il.us

Rod R. Blagojevich
Governor

Sheldon Sorosky
Chairman

Lori G. Levin
Executive Director

"Privacy Schmrivacy?"

DRAFTING PRIVACY POLICY IN AN INTEGRATED JUSTICE ENVIRONMENT
(and why it's important)

IIJIS
Illinois Integrated Justice Information System

At the same time, the project team identified the purpose and scope of the project team's work. *Privacy Schmrivacy* included an introduction to the need for a privacy policy, an explanation of the types of people who should participate, and an outline of the process the project team should use to develop a privacy policy. This document served as the foundational document for the IIJIS privacy project team.

Project Process

Project Team Meetings

The project team met approximately five times over an 18-month period. Project team leaders met in advance of each meeting to determine the meeting objectives and to create a checklist of items to address

within the two-hour team meetings. The team leaders were successful in their goal to break the mold of the same old meeting by focusing the meetings on the items outlined on the checklist and completing these goals within the two-hour meeting time frame.

Preparation for the meetings was very important to the success of this initiative. Team leaders strived to ensure that team members knew the purpose of each meeting and that team members were educated about privacy issues. Most importantly, project team leaders used meetings to learn about issues faced by the team members in their respective agencies and to understand their concerns and recommendations in relation to privacy.

To ensure discussions moved along during the meetings, team leaders analyzed in advance the particular interests of each of the designated participants and the input each member could potentially provide regarding particular agenda items to ensure participation by all team members. Project team leaders also sought creative ways to either present information or obtain information from the participants. For example, team leaders used PowerPoint presentations to demonstrate that the state's statute on expungement was confusing and used images of cartoon characters with criminal histories to demonstrate the complexity of the laws related to background checks for employment purposes. As a result, the meetings were productive, interesting, and informative.

Project team leaders limited meetings to two hours, even if the meeting agenda was not completed. Nonetheless, the team leaders attempted to maintain control over the timing of the agenda items so that the group would finish on time. The leaders used the checklist prepared in advance to ensure that the goals of the meeting were accomplished and held a debriefing after each team meeting to assess how future meetings could be improved. The following is a list of the topics addressed in meetings from December 2003 through February 2005.

December 17, 2003	**Introductory team meeting.**
March 31, 2004	**Discussed spreadsheet of federal and state privacy laws.**
June 2, 2004	**Summarized the Illinois State Police's implementation of the FIPs and discussed expungement as a privacy policy.**
June 23, 2004	**Privacy issues brainstorming session. Arranged the room so all participants could see each other and lined the walls with paper to document brainstorming.**
February 24, 2005	**Outlined transitional process and highlighted the outline of the privacy policy.**

Individual Personal Meetings

Between team meetings, project team leaders attempted to meet one-on-one with each team member to obtain additional insight and to reduce the length of team meetings by doing research and preparation in advance. Individual meetings were used both before upcoming meetings to expand specific agendas and afterwards to debrief and process issues that were raised during the meeting. The project team members were an exceptional source of information, and the team leaders made efforts to listen to their concerns and leverage their knowledge. Individual meetings with team members usually lasted approximately an hour and, in some instances, required additional time for travel. Project team leaders met with about 15 team members for a total of approximately 15 hours. These meetings occurred during April and May 2004, prior to the brainstorming session.

When issues that were relevant to the entire team were raised during these individual meetings, the leaders made a note to raise them during the next team meeting in order to solicit team feedback and explore other team members' thoughts on these issues.

Staff Preparation and Workload

Preparation for team meetings was dependent on the goals of the meeting. If the goal was to educate members on a particular topic, team leaders expended time to master that subject. When the team invited the

Illinois State Police to discuss how the criminal history repository safeguards its information and implements the FIPs, the team leaders held several meetings with the presenters at their offices prior to the project team meeting.

Project team members were informed of meeting dates approximately four to six weeks in advance of each meeting. Also prior to each meeting, team leaders met to plan the meeting agenda and identify materials that would be mailed to team members. Leaders invested additional preparation time to compile the mailings and develop presentations to share at meetings.

Research and writing required considerable staff resources. For example, the Illinois team created a study comparing unofficial and official sources of CHRI (criminal history record information). The initial preparation, Institutional Review Board (IRB) approval, and subsequent reduction in study scope took at least 80 staff hours.

Developing and revising the 20-page document that outlined all of the privacy issues identified by the team required approximately 30 hours: 10-12 hours to compile the document from brainstorming session notes and about 20 hours for revisions, since it was essential that comments from many different groups be combined to create an easy-to-read document.

Products Produced

The guidance document, entitled *Privacy Schmrivacy: Drafting Privacy Policy in an Integrated Justice Environment (and why it's important)*, was developed and revised between 2002 and the official publishing date of June 2004.

Another product, *Criminal History Record Information in Illinois: Access and Review Provisions*, analyzed 39 distinct statutory privacy provisions and indicated whether each provision implements an FIP. Displayed in table format, this product visually depicts the policy choices made by the U.S. Department of Justice (DOJ), the Illinois General Assembly, and the Illinois State Police. It was created to help the team understand not only current privacy decisions but also why and where those decisions were made. Understanding the rationale for a privacy decision helps agencies implement it and also provides guidance to policymakers on whether the decision should be applied in other contexts. Knowing where a decision was made can influence the amount of deference granted to it.

Criminal History Record Information in Illinois: Access and Review Provisions

	Code of Federal Regulations				Illinois Compiled Statutes				Illinois Administrative Code			
Provision No.	FIP Implementation?	Citation	Regulation	Substance of the Regulation	Citation	Statute	Substance of the Statute	Does this Reflect a Policy Choice? What is the policy?	Citation	Regulation	Substance of the Regulation	Does this Reflect a Policy Choice? What is the policy?
A	FIP 5: Individual Participation Agencies should allow individuals access to data about them to review the information, challenge incorrect data, and if successful have the data erased, rectified, completed, or amended with notification to all parties who received the incorrect information.	28 C.F.R. § 20.21(g)(1)	"(g) Access and review. Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that - (1) Any individual shall, upon satisfactory verification of his identity, be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;"	An individual is entitled to review any criminal history record information maintained about that individual once his identity has been verified. This right of review may not unduly burden either the individual or the agency.	20 ILCS 2605/7	"(1) Whenever an individual requests the Department to correct information which the individual asserts is incorrect, the Department shall within 30 days of receiving the request, review the person's file to determine whether the information in the person's file is accurate or complete. The Department shall make such changes in the person's file as are necessary to correct any inaccurate information. The Department shall notify the person making the request. The Department shall establish reasonable fees and rules to allow an individual to review and correct any criminal history record information the Department may hold concerning that individual upon verification of the identity of the individual. Such information is subject to the provisions of the Illinois Administrative Procedure Act."	Upon verification of the individual's identity, that individual may request that the Department of State Police release information as to the existence or nonexistence of any criminal history record he might have. The Department of State Police is charged with establishing reasonable fees and rules to allow an individual, once his identity is verified, to access any criminal history record information pertaining to him for purposes of review and correction.	No in part; Yes in part. No. The Illinois General Assembly was required by the Department of Justice to ensure to individuals the right to review any criminal history record information maintained regarding him. Yes. Instead of legislating the CHRI access and review procedures themselves, the Illinois General Assembly delegated the responsibility to promulgate reasonable access and review procedures to the Department of State Police. Why: The General Assembly chose to delegate the responsibility to the Illinois State Police because it is the state's central repository for criminal history record information.	11 Admin. Code El 20 § 1210.30	"1210.30 Procedures a) Any individual may approach any Illinois law enforcement or correctional facility during regular business hours for the purpose of obtaining his individual's criminal history transcript. b) In response to a request for a criminal history transcript, the facility shall obtain fingerprints from the individual and other identification information. c) Within 30 days after the request, the facility shall forward to the Department the fingerprints and identifying information. d) Upon receipt of the corresponding fingerprints and identifying information, the Department shall provide the facility with the individual's criminal history transcript, or, if no criminal history is found, another statement so stating. e) The facility shall contact the individual and allow the individual to view the criminal history	A criminal history transcript is a printed record of CHRI maintained by the repository with respect to a particular individual. a) An individual can access and review his criminal history transcript at any Illinois law enforcement or correctional facility. b) The facility must fingerprint the individual to verify his identity before providing CHRI. c) The facility will then forward the fingerprints to the Illinois State Police within 30 days. d) The Illinois State Police must provide to the	No in part; Yes in part. No. the Illinois State Police were required by the Illinois General Assembly to promulgate reasonable access and review procedures. Yes. The Illinois State Police made several policy choices in the access and review procedures such as; (a) where an individual can go to request access and review of his criminal history transcript; (b) the selection of fingerprints as the means of identity verification; (c) the creation of time frames for responding; and (d) the prohibition on showing the individual to receive a copy of his criminal history transcript. Why: (a) The Illinois State Police and the Illinois Criminal Justice Information Authority determined that

This document is housed within an Excel spreadsheet that the project team is continuing to complete by adding references to administrative rules implementing those statutory provisions.

The *Privacy Policy* is currently in the drafting process. Once released in draft form, this policy will go through a vetting process and incorporate revisions.

Lessons Learned

- ❒ **Be flexible.** Although the Illinois team identified initial goals and objectives, they recognized the need for flexibility as their team effort developed and expanded or amended goals and objectives. When the team realized that drafting a policy starting with the FIPs would not work, the team recognized the need to shift their approach and asked team members to identify privacy issues that were currently affecting their agencies, as well as indicate any information needs that they thought were not being addressed.

- ❒ **Limit scope and identify phases.** IIJIS began with the traditional criminal justice transactions that were currently under way. This helped limit the initial scope and served as a building block for next phases, e.g., intelligence information and juvenile justice information.

- ❒ **Include the correct participants.** When working on the traditional justice information exchanges, ensure that the current team contains the expertise to address these issues. When the team moves to the next phase and begins to address intelligence and other issues, the team will need to alter the composition of its members.

- ❒ **Avoid jargon and acronyms.** Professional jargon and terms can make participants feel like they are not qualified to work on the project. Define terms in meetings and create a project glossary, if necessary.

- ❒ **Recruit law students.** Due to the amount of research and writing, more law students would have been extremely helpful to this effort

- ❒ **Identify participants by constituency and their unique skills.** Attempt to involve stakeholders that both care about privacy and also bring skills that will assist in the process, such as legal analysis skills, a foundation in criminal justice process, people skills, writing skills, team dynamics, etc.

- ❒ **Ensure clear leadership.** Help the team understand the leadership process and team roles. Ensure that the identified project team leaders have the organizational authority to lead this process.

- ❒ **Recognize limitations.** If there is not sufficient staff assigned to support the team's work, there may be time delays between meetings and in reaching goals. The Illinois team had a large gap between their brainstorming session and the beginning of policy development due to time constraints on their limited staff. If possible, assign dedicated full-time staff with enough autonomy to be able to visit committee members.

- ❒ **Arrange the meeting room to facilitate discussions.** For example, the Illinois team rearranged the room on more than one occasion to eliminate the feeling of attending the same old meeting. Move chairs and tables so that all participants can see each other—arrange in a circle, square, or U-shape.

- ❒ **Prepare in advance for meetings.** Be prepared with questions for each member to keep everyone involved and to jumpstart the discussion. Let the team know the expectations for the meeting and let them know that the meeting will end on time.

- ❒ **Begin the meeting focused on achieving certain goals.** Plan in advance what you must accomplish at the meeting, use a checklist and work to be sure that you accomplish what you set out to accomplish by the end of the meeting.

Additional Reading and Resources

- Illinois Criminal Justice Information Authority was created by the Criminal Justice Information Act, 20 ILCS 3930/1-14 and is available at www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=397&ChapAct=20%26nbsp%3BILCS%26nbsp%3B3930%2F&ChapterID=5&ChapterName=EXECUTIVE+BRANCH&ActName=Illinois+Criminal+Justice+Information+Act%2E.

- The mission statement and organizational structure of the Authority can be readily located in the most recent annual report. As of August 1, 2005, the most recent annual report is the 2005 Annual Report available at www.icjia.state.il.us/IIJIS/public/pdf/IMB/2005AnnualReport_final.pdf.

- Illinois Executive Order Number 16 (2003) creating the Illinois Integrated Justice Information System Implementation Board is available at www.illinois.gov/Gov/pdfdocs/execorder2003-16.pdf.

- The *IIJIS Strategic Plan* is another foundational document guiding the initiative's activities. It is available at www.icjia.state.il.us/iijis/public/pdf/strategicplan_final.pdf.

- Additional foundational documents, including the first executive order calling for the development of the strategic plan and the Authority resolution in support of integrated justice in Illinois can be found at www.icjia.state.il.us/iijis/public/index.cfm?metasection=foundation.

- Committee meeting agendas and materials are posted on the IIJIS Web site at www.icjia.state.il.us/iijis/public/index.cfm?metasection=oversight. Scroll down to the section on the Privacy Policy Subcommittee. Meeting materials are located with the meeting notes.

- PowerPoint presentation about the "Illinois Expungement/Sealing Statute" used at the June 2, 2004, meeting is available at www.icjia.state.il.us/iijis/public/PowerPoint/expungementReadability_icjia.ppt.

- PowerPoint presentation with newspaper headlines used at June 23, 2004, meeting is available at www.icjia.state.il.us/iijis/public/PowerPoint/PRV_headlines_06232004.ppt.

- *Criminal History Record Information in Illinois: Access and Review Provision* is available in a poster-sized PDF that can be accessed at www.icjia.state.il.us/iijis/public/PDF/PRV/chri_AccessAndReview3d.pdf.

- *Privacy Schmrivacy: Drafting Privacy Policy in an Integrated Justice Environment (and why it's important)* is available at www.icjia.state.il.us/iijis/public/pdf/PRV/PrivacySchmrivacy_FINAL.pdf.

- The IIJIS Executive Steering Committee asked all IIJIS committees to draft a work plan. The Privacy Committee's plan can be found at www.icjia.state.il.us/iijis/public/pdf/PRV/PRV_12monthPlan.pdf.

Appendix D
Glossary of Terms and Definitions

The following terms and definitions are provided as a reference for use during the privacy policy development process and as a resource for the project team, project team leader, and project champion or sponsor. Not all of the terms listed were specifically discussed within this guide but are terms relative to the subject of privacy and may contribute to an understanding of privacy-related issues.

A

Access
In respect to privacy, an individual's ability to view, modify, and contest the accuracy and completeness of personally identifiable information collected about him or her. Access is an element of the Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs). See *Fair Information Principles (FIPs).*

Access Control
The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Accountability Principle
One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, a data controller should be accountable for complying with measures that give effect to the principles stated above.

Accuracy of Information
In addition to providing individuals with the ability to correct factual inaccuracies in their personally identifiable or prospect information, an organization must also take reasonable steps to ensure that the personally identifiable and prospect information that it collects is accurate, complete, and timely for the purposes for which it is used. See *Prospect Information*.

Administrative Vulnerability
Failure to observe administrative best practices, such as using a weak password or logging on to an account that has more user rights than the user requires to perform a specific task.

Anonymity
A condition in which an individual's true identity is unknown.

Appropriate Security
An organization is required to take appropriate data security measures to protect personally identifiable information and prospect information. These measures must include physical security measures, such as doors and locks, as well as electronic security and managerial controls that limit the potential for unauthorized access or misuse by employees and contractors. The security measures necessary to protect information sufficiently will vary based on the risks presented to the individual by an organization's collection and use of the data. See *Prospect Information*.

Attack
A deliberate attempt to compromise the security of a computer system or deprive others of the use of the system.

Audit Trail

Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication

Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See *Biometrics*.

Authentication of Identity

The process whereby an organization establishes that a party it is dealing with is:

- A previously known real-world entity (in which case, it can associate transactions with an existing record in the relevant information system).
- A previously unknown real-world entity (in which case, it may be appropriate to create a new record in the relevant information system and perhaps also to create an organizational identifier for that party).

Authorization

The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See *Authentication*.

B

Biometrics

Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

C

Certificate

An encrypted file containing user or server identification information that is used to verify identity and to help establish a security-enhanced link.

Charter (Project Team)

A collection of the project team's written vision, mission, and values statements, as well as the stated goals and objectives. The charter serves as a reference and resource throughout the course of the project team's effort. The most critical feature of the charter is that it memorializes the planning efforts and agreements of the team members to achieve specific goals and, thus, serves as an historical record of team plans and efforts.

Collection Limitation Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this 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.

Computer Security

The protection of information assets through the use of technology, processes, and training.

Confidentiality

Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See *Privacy*.

Cookie

A small data file that is stored on a user's local computer for record-keeping purposes that contains information about the user that is pertinent to a Web site, such as a user preference.

Credentials

Credentials are information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Cryptography
The study or analysis of codes and encoding methods used to secure information. Cryptographic techniques can be used to enable and ensure confidentiality, data integrity, authentication (entity and data origin), and nonrepudiation. See *Nonrepudiation*.

D

Data
Inert symbols, signs, or measures.

Data Controller
A party who, according to domestic law, is competent to decide about the contents and use of personal data, regardless of whether or not such data is collected, stored, processed, or disseminated by that party or by an agent on its behalf.

Data Protection
Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Data Quality Principle
One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this 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 up to date.

Data Transfer
As a key principle of privacy, it is the movement of personally identifiable information between entities, such as a customer list being shared between two different companies.

Degaussing
A process of destroying computerized data by leaving the domains in random patterns with no preference to orientation, which then renders previous data unrecoverable.

Digital Certificate
A digitally signed statement that binds the identifying information of a user, computer, or service to a public/private key pair. A digital certificate is commonly used in the process of authentication and for securing information on networks. See *Authentication*.

Digital Signature
A digital signature is data that binds a sender's identity to the information being sent. A digital signature may be bundled with any message, file, or other digitally encoded information or transmitted separately. Digital signatures are used in public key environments and provide nonrepudiation and integrity services. See *Nonrepudiation*.

Disclosure
The release, transfer, provision of access to, or divulging of personally identifiable information in any other manner, electronic, verbal, or in writing, to an individual, agency, or organization outside of the agency who collected it.

Download
To transfer a copy of a file from a remote computer to a requesting computer by means of a modem or network.

E

Electronically Maintained
Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted
Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail. See *Extranet*.

Enforcement
A privacy principle that provides mechanisms for assuring compliance with the Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs), recourse for individuals affected by noncompliance, and consequences for noncompliant organizations. Methods for enforcement include a review by independent third parties.

Extranet
An extension of an organization's intranet used to facilitate communication with the organization's trusted partners. An extranet allows such trusted partners to gain limited access to the organization's internal data.

F

Fair Information Principles (FIPs)

The Fair Information Principles (FIPs) are contained within the Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Filter

A pattern or mask through which data is passed to separate specified items. For instance, a filter used in e-mail or in retrieving newsgroup messages can allow users to automatically discard messages from designated users.

Firewall

A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

G

Goals (Project)

Project goals are the desired long-term end results that, if accomplished, will mean the team has achieved their mission. Goals provide a framework for more detailed levels of planning. Goals are more specific than mission statements but remain general enough to stimulate creativity and innovation.

H

Health Insurance Portability and Accountability Act (HIPAA)

A U.S. law that gives patients greater access to their own medical records and more control over how their personally identifiable information is used. The law also addresses the obligations of health-care providers and health plans to protect health information. In general, covered entities such as health plans, health-care clearinghouses, and health-care providers that conduct certain financial and administrative transactions electronically had until April 14, 2003, to comply with this act.

I

Identification

A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or may be a compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

Individually Identifiable Health Information (IIHI)

Information, including demographic information, that relates to past, present, or future physical or mental health or condition of a member and can be used to identify the member.

Individual Participation Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). As stated in the FIPs, according to this principle, an individual should have the right:

a) To obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) To have communicated to him, data relating to him:
   - Within a reasonable time;
   - At a charge, if any, that is not excessive;
   - In a reasonable manner; and
   - In a form that is readily intelligible to him;

c) To be given reasons if a request made under subparagraphs a) and b) is denied, and to be able to challenge such denial; and

d) To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Individual Responsibility

Since a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Information

The use of data to extract meaning.

Information Disclosure

The exposure of information to individuals who normally would not have access to it.

Information Privacy

Information privacy is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.

Information Quality

The accuracy and validity of the actual values of the data, data structure, and database/data repository design. The elements of information quality are accuracy, completeness, currency, reliability, and context/meaning.

Invasion of Privacy

Invasion of privacy can be defined as intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also *Right to Privacy.*

K

Key

In encryption and digital signatures, a key is a value used in combination with an algorithm to encrypt or decrypt data.

L

Least Privilege Administration

A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform.

Logs

Logs are a necessary part of an adequate security system as they are needed to assure that data is properly tracked and only authorized individuals are getting access to the data.

M

Maintenance of Information

The maintenance of information applies to all forms of information storage. This would include electronic systems, like databases, and nonelectronic storage systems, like filing cabinets. To meet access requirements, an organization is not required to create new systems to maintain information or maintain information beyond a time when it no longer serves an organization's purpose.

Mission Statement

A succinct, comprehensive statement of purpose of an agency, program, subprogram, or project that is consistent with a vision statement. See *Vision Statement*.

N

Nonrepudiation

A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

O

Objectives (Project)

Objectives are specific and measurable targets for accomplishing goals, which are usually short term with a target time frame. In contrast to goals, objectives are specific, quantifiable, and time-bound statements of desired accomplishments or results. As such, objectives represent intermediate achievements necessary to achieve goals. See *Goals*.

Online Collection

A Web site or online service is deemed to collect personally identifiable information or prospect information online, even though that information may be immediately deleted and not maintained for further use by an organization.

Openness Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, there should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for 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.

P

Permissions

Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data

Personal data refers to any personally identifiable information that relates to an identifiable individual (or data subject). See also *Personally Identifiable Information*.

Personal Information

See *Personally Identifiable Information*.

Personally Identifiable Information

Personally identifiable information is one or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is sufficient to specify a unique individual.

The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Privacy

The term privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.

Other definitions of privacy include the capacity to be physically alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Compromise

A privacy compromise is a scenario in which an unauthorized individual, or group of individuals, is able to gain access to personally identifiable information about another.

Privacy Policy

A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection

This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Project Champion (or Sponsor)

The project champion or sponsor is a high-level individual within the organization who has been selected to drive the privacy policy development effort. The champion helps steer the development of the privacy policy, identifies and allocates the necessary resources (both human and other support), and oversees policy

implementation. This person provides a strong voice for the team effort, particularly when there is competition for scarce resources, and provides the mechanism for efficient decision making when the project team leader or project manager does not have the authority to make decisions in selected areas.

Project Team

The project team is a multidisciplinary group of individuals, representing a broad array of perspectives, who collaborate on the development of the privacy policy. This team represents the core agencies that are entrusted with the protection of private information for justice information sharing. See *Stakeholder*.

Project Team Leader

A project team leader is someone who will direct and manage the privacy policy development project on a day-to-day basis. The project team leader should possess the following essential characteristics: organizational credibility, organizational authority, ability to build and manage coalitions, and ability to manage day-to-day tasks over an extended period of time.

Prospect Information

Prospect information is defined the exact same way as personally identifiable information except that it is submitted by an individual who is not the subject of the data and who is giving personally identifiable information about someone else. This personally identifiable information about someone else is considered prospect information.

Purpose Specification Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, the purposes for which personal data are collected should be specified no later than at the time of 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.

R

Record

Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Repudiation

The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retrievable Information

Information is retrievable in the ordinary course of business if it can be retrieved by taking steps that are taken on a regular basis in the conduct of business with respect to that information or that an organization is capable of taking with the procedures it uses on a regular basis in the conduct of its business.

Information is not considered retrievable in the ordinary course of business if retrieval would impose an unreasonable burden or violate the legitimate rights of a person that is not the subject of the information. The unreasonableness of burden is balanced against the significance of the information's use.

Right to Privacy

The possible right to be let alone, in the absence of some reasonable public interest in a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

The right to privacy as a matter of constitutional law is understood to have begun with a pioneering law review article in the *Harvard Law Review* in the 1890s written by lawyers Samuel D. Warren and future Supreme Court Justice Louis D. Brandeis. See *Privacy*.

Role-Based Authorization

A type of authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

S

Safeguard

A safeguard is considered a technology, policy, or procedure that counters a threat or protects assets.

Secondary Data Uses

Uses of personally identifiable information for purposes other than those for which the information was originally collected. The Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles (FIPs) state that a person can provide personally identifiable information for a specific purpose without the

fear that it may later be used for an unrelated purpose without that person's knowledge or consent.

Secure Sockets Layer (SSL)

A protocol that provides secure data communication through data encryption. This protocol enables authentication, integrity, and data privacy over networks through a combination of digital certificates, public-key cryptography, and bulk data encryption. This protocol does not provide authorization or nonrepudiation.

Security

Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes.

Computer and communications security efforts also have the goal of assuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Security Policy

A security policy is different from a privacy policy. A security policy alone may not adequately address the protection of personally identifiable information or the requirements of a privacy policy in their entirety. A security policy addresses information classification, protection, and periodic review to ensure that information is being stewarded in accordance with an organization's privacy policy. See *Privacy Policy*.

Security Safeguards Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this 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.

Stakeholder

A stakeholder is an agency or individual that is essential to the development and implementation of the privacy policy and who contributes to, but is not a member of, the project team. Stakeholders have interests in the outcome of the privacy policy and provide input (for example, focus groups, surveys, documents for public comment, or invited speakers at team meetings). See *Project Team*.

T

Transborder Flows of Personal Data

Movements of personal data across national borders. See *Fair Information Principles (FIPs)*.

U

Use

With respect to personally identifiable information, the sharing, employment, application, utilization, examination, or analysis of such information within the agency or organization that maintains the designated record set.

Use Limitation Principle

One of the eight Fair Information Principles (FIPs) developed by the Organisation for Economic Co-operation and Development (OECD). According to this principle, personal data should not be disclosed, made available, or otherwise be used for purposes other than those specified in accordance with the Purpose Specification Principle, except with the consent of the data subject or by the authority of law. See *Purpose Specification Principle*.

V

Values Statement

The core principles and philosophies that describe how an agency conducts itself in carrying out its mission.

Virtual Private Network (VPN)

The extension of a private network that provides encapsulated, encrypted, and authenticated logical (not physical) links across shared or public networks. VPN connections typically provide remote access and router-to-router connections to private networks over the Internet.

Virus

A code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or data. See *Worm*.

Vision Statement

A compelling and conceptual image of the desired, successful outcome.

Vulnerability

Any weakness, administrative process, act, or physical exposure that makes a computer susceptible to exploitation by a threat.

W

Worm

A self-propagating malicious code that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such as consuming network or local system resources, possibly causing a denial-of-service attack.

Cited Resources for Glossary of Terms and Definitions

- Better Business Bureau, BBBOnLine Privacy Program, *Privacy Terms and Definitions,* www.bbbonline.org/privacy/help.pdf.
- University of Miami Ethics Programs, Privacy/Data Protection Project, Encyclopedia, Index, http://privacy.med.miami.edu/glossary/index.htm.
- Privacilla.org, Privacy and Government, Organisation for Economic Co-operation and Development (OECD) Guidelines, www.privacilla.org/government/oecdguidelines.html.
- Organisation for Economic Co-operation and Development (OECD), OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980, www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html.
- Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy," *Harvard Law Review* 4, 1890:193.
- Clarke, Roger. Privacy Introduction and Definitions, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, September 16, 1999, www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.
- Birnbaum, Adam. Blue Cross Blue Shield Association (BCBSA), Health Insurance Portability and Accountability Act (HIPAA), *Helpful HIPAA Terms and Definitions,* www.fepblue.org/privacyhipaa/privacyhipaadefined.html.
- Law.com, ALM Properties, Inc., *Law.com Dictionary,* http://dictionary.law.com/.
- Microsoft Corporation, *Microsoft Security Glossary*, October 29, 2002 (Revised May 20, 2005), www.microsoft.com/security/glossary.mspx.

www.it.ojp.gov