Justice Information Privacy Guideline

Developing, Drafting and Assessing Privacy Policy for Justice Information Systems

September 2002

National Criminal Justice Association

720 7th Street, NW , 3rd Floor, Washington, DC 2000, Tel.: (202) 628-8550, Fax: (202) 628-0080, http:// www.ncja.org

This document was supported by Grant Number 1999-LD-VX-K002 awarded by the Bureau of Justice Assistance (BJA) to the National Criminal Justice Association in furtherance of the U.S. Department of Justice (DOJ) integrated justice information initiative. BJA is a component of DOJ's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Table of Contents

Section I

Introduction and Basic Considerations

Introduction

Recent advances in information technology have dramatically increased the ability of civil and criminal justice agencies to collect, receive, organize, access, analyze, and disseminate information electronically. At the same time, the public, elected officials, and justice leaders have expressed growing concern about information privacy—and for good reason.

The public endures the risk that personal information, that is, information about an identifiable individual contained in a justice information system, may be accessed or released inappropriately, causing possible loss of employment, diminished social status, or other highly adverse consequences. As for justice agencies that operate information systems without assessing possible privacy impacts, the possibility looms that public concern or a damaging privacy incident may bring their multimillion-dollar information systems to a screeching halt. Ongoing privacy policy development, therefore, is critical to protecting the public's privacy and the justice system's technology investment.

The goal of a justice agency privacy policy is to preserve the integrity and effectiveness of public safety and civil justice functions, protect the individual from inappropriate use or release of personal information, and promote public access for oversight of the justice process. Privacy policy requires balancing the competing interests of justice agencies, individuals, the media, and the commercial sector. The terrorist attacks of September 11, 2001, heightened the urgency for development of such a policy, given subsequent steps and ongoing proposals to increase law enforcement information sharing and intelligence capabilities in the fight against terrorism.

Justice system leaders are being asked to develop justice information privacy policy often with, at best, only a patchwork of established laws, regulations, or policy precedents. They must weigh the costs of developing and adhering to a privacy plan against the costs of future privacy intrusions, loss of public confidence and legislative funding, and belated modification of information systems to include privacy protections after system implementation.

The goal of the *Justice Information Privacy Guideline* (*Guideline*) is to provide assistance to justice leaders and practitioners who seek to balance public safety, public access, and privacy when developing information privacy policies for their agencies' systems, whether already operating or being planned and whether independent of or integrated with those of other agencies. Providing insights on difficult issues faced by justice leaders in developing privacy policy, the *Guideline*

was prepared through a national and international collaboration of nearly 100 state, local, and tribal justice leaders, as well as academia, elected officials, the media, and the commercial sector.

After an introductory section, the *Guideline* addresses three major areas of privacy policy—developing it, drafting it, and assessing it.

Chapter One:

What Is the Justice Information Privacy Guideline?

Purpose: to explain the goal and intended use of this document, outline its scope and organization, and present an overview of preparing privacy policy

Public safety. Public access. Privacy. The American justice system requires a careful balancing of these concepts as they relate to people, processes, and information.

In the context of this report, "public safety" refers to justice agencies' collection, use, and disclosure of information to promote criminal or civil justice functions. "Public access" refers to the public's interest in monitoring justice system processes through access to justice information. "Privacy" refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information in the justice system. Balancing these concepts requires assessing the often competing information needs of a variety of groups, including justice agencies, individuals, the media, and the commercial sector, and developing proactive privacy policy to serve these interests.

Goal and Use of This Report

The goal of the *Justice Information Privacy Guideline (Guideline)* is to provide assistance to justice leaders and practitioners who seek to balance public safety, public access, and privacy when developing information policies for their individual agencies or for integrated (multiagency) justice systems. For continuity throughout the *Guideline*, the balancing of the three concepts (public safety, public access, and privacy) is embodied in the term "privacy policy."

Some privacy issues can be addressed through basic tenets of information collection and use, and the *Guideline* provides specific direction on how to employ good collection and use practices. Other privacy issues are not as clearly solved from agency to agency or jurisdiction to jurisdiction—for example, determining the sensitivity or public accessibility of certain data elements. The *Guideline* cannot offer specific answers to these policy questions but rather provides discussion on a variety of subjects intended to inform the decision-making practices of justice leaders when developing privacy policies. In this way, the discussion sections are critical to using the policy drafting templates contained in this document.

The *Guideline* is the product of two years of discussion and development by nearly 100 state, local, and tribal justice leaders, nationally and internationally, as well as representatives from academia, elected officials, the media, and the commercial sector. The drafters of this resource encourage all justice agencies to consider whether their information system strategies should include privacy policy by answering the following questions:

1. Do you disclose or provide access to information to persons or agencies outside of your organization?
2. Is your information system connected to other information systems?
3. Do you collect, use, or provide access to personally identifiable information?
4. If the information you have in your system was about you or your family, would you want it to be kept private?

If you answered "yes" to any of these questions, your agency should be concerned about privacy and should develop a privacy policy and prepare a privacy impact assessment.

Guideline Scope and Organization

Issues relating to information privacy in the justice system are vast and complex. The drafters of this document are aware of the need to address privacy implications in various contexts, including criminal justice, civil, and juvenile justice. The term "justice information" as used in this *Guideline* is intended to reflect criminal and civil information, generally. To separate out "civil information" from "criminal information" in discussing the development of privacy policies would require an artificial distinction by agencies (e.g., courts) that must develop policies in both contexts.

The key to developing policy for both civil and criminal justice information is to consider "content and context"; i.e., the type of information and the context in which it is shared within or released outside the justice system. For purposes of focusing the discussion, however, this *Guideline* concentrates on information privacy in the general adult criminal and civil justice contexts.

The *Guideline* provides background discussion on information privacy policy issues, followed by tools, or templates, to assist in drafting privacy policies, and a privacy impact assessment to test their effectiveness. The *Guideline* consists of four sections comprising eight chapters:

- Section I, consisting of Chapters One and Two, presents introductory material, background on factors influencing policy development and use of advanced information technologies in the justice system, and a discussion of the "justice record."
- Section II, which focuses on developing privacy policy (Chapters Three, Four, and Five), outlines eight privacy design principles applicable both to the formulation of privacy policy and to the related technology. Also discussed are rules for, and risks associated with, interagency information exchange and public access to justice data, including personally identifiable information.

- Section III deals with drafting privacy policy. To aid that process, use of a privacy drafting template is suggested (Chapter Six).
- Section IV presents an approach to assessing, or testing, the impact of privacy policy developed and drafted by justice agencies and explains the importance of privacy policy education and training (Chapters Seven and Eight).

Chapter Two:

Privacy and Justice Information Systems

This chapter focuses on the nature of information privacy and the rationale underlying an information privacy policy. Also discussed are integrated justice systems, the justice record, how new technology affects privacy law, and the duties of an information steward.

Purpose: to explain information privacy, provide background on factors influencing policy development and the use of advanced information technologies in the justice system, and to describe the set of information at issue, known as the "justice record"

What Is Information Privacy?

The concept of privacy is broad, encompassing different personal values and interests. Information privacy as discussed in this *Guideline* is defined by the following ideas:

- "Privacy" is described as the interrelated values, rights, and interests unique to individuals. Privacy interests come in a variety of flavors, including privacy of the person, privacy of personal behavior, privacy of personal communications, and privacy of personal data (information privacy).
- Privacy of personal data (information privacy) is described as when, how, and to what extent you share personal information about yourself. Information privacy involves the right to control one's personal information and the ability to determine if and how that information should be obtained and used. It entails restrictions on a wide range of activities relating to personal information: its collection, use, retention, and disclosure. The concept of information privacy is sometimes lumped together with terms such as confidentiality and security. The terms are not synonymous, however.
- Confidentiality is only one means of protecting personal information, usually in the form of safeguarding the information from unauthorized disclosure to third parties. Confidentiality comes into play well after the information in question has been obtained by the "data user." It is in this sense that privacy is a much broader idea than confidentiality. Data users are expected to be responsible for the safekeeping of the personal information entrusted to them. Confidentiality is about limiting access to personal information to

those with specific permission and preventing its disclosure to unauthorized third parties.[1] This is where confidentiality intersects with security.

- Security encompasses data security, computer and network security, physical security, and procedural controls. All of these must be deployed to protect personal information from a wide range of threats. Measures that enhance security also enhance privacy; however, while these two concepts are complementary, they are not the same. Simply focusing on security alone does not ensure privacy, even though it is an essential component of protecting privacy.

The concept of information privacy relates to one's personal information. Personal information[2] is information about an identifiable individual which may include:

- Information relating to race, national or ethnic origin, religion, age, sex, sexual orientation, or marital or family status;
- Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- Any identifying number, symbol, or other particular assigned to the individual; and
- Name, address, telephone number, fingerprints, blood type, or DNA.

Why Have an Information Privacy Policy?

In recent years, information technology advancements have dramatically increased the ability to collect, receive, organize, access, and analyze information electronically in the civil and criminal justice arenas. There is little doubt that such capabilities improve the day-to-day operation of justice agencies and their responsiveness to the public. Law enforcement, prosecution, defense, courts, corrections, probation and parole, and related justice service agencies, however, are acknowledging that the way data is collected, used, and shared in today's information environment poses significant privacy questions not realized in the past. In addition, as the implementation of electronic information collection and sharing capabilities increases, so does public concern over the use, or potential misuse, of personal information contained in these systems.[3]

---

[1] As discussed in Chapter Six, information can be categorized as "discloseable," "nondiscloseable," or "publicly accessible." Confidential information covers that information which is discloseable or nondiscloseable because it requires limiting access according to the requester's authority to receive the information. Publicly accessible information does not carry this limitation.

[2] For statutory guidance in defining "personal information," the authors looked to the United States Federal Privacy Act. Although the Privacy Act does not include a definition of "personal information," its definition of "record" includes information pertaining to education, financial transactions, medical history, criminal or employment history, name, and any identifying number, symbol, or other identifying particular assigned to an individual, such as a finger or voice print, or a photograph. See The Privacy Act of 1974, as amended, 5 U.S.C. §552a (1999).

Many other recent legislative and regulatory acts have defined or given examples of "personal information." These include the Children's Online Privacy Protection Act, 15 U.S.C.A. §6501 and the Federal Trade Commission's "Privacy Online: A Report to Congress,"http://www.ftc.gov/reports/privacy3/toc.htm. In addition, please see the European Union Directive on Data Protection 95-46.

[3] See Opinion Research Corporation International, Privacy, Technology and Criminal Justice Information, Public Attitudes Toward Uses of Criminal History Information, Summary of Survey Findings, prepared for the U.S. Department of Justice, Bureau of Justice Statistics and SEARCH, The National Consortium for Justice Information and Statistics (May 2000).

Information privacy is a growing concern among the public, elected officials, and justice leaders for a good reason. The inability or lack of desire to address privacy concerns associated with information management systems can result in dire consequences for the general public as well as government agencies.

For example, the public endures actual risk that one's personal information contained in a justice information system may be accessed or released inappropriately, causing possible loss of employment or social status. The public also incurs the risk that inaccurate justice information may be released and subsequently used to one's detriment. Such was the case with an Ohio man whose social security number was accidentally associated with another individual who possessed a criminal history record.[4] Subsequent sale of the incorrect information by a sheriff's office to a private information reseller made correction of this error virtually impossible.

Failing to adequately identify and address privacy concerns can be detrimental to justice agencies as well. It is no secret that justice agencies nationwide have spent billions of dollars on information technologies to improve the operation of the justice system. Justice agencies that apply new information technologies or continue to operate information systems without assessing their possible privacy effects, however, may find that public concern or a damaging privacy incident can bring their multimillion dollar information systems to a screeching halt. Therefore, ongoing privacy policy development that addresses intrajustice system information sharing, as well as public access to justice information, is critical to protecting the public's privacy and the justice system's technology investment.

Today, in addition to the challenges of new technology, the criminal justice system faces privacy policy challenges resulting from the events of September 11, 2001. In the wake of September 11, political leadership has focused on increasing law enforcement information sharing and intelligence capabilities in the fight against terrorism. At both the federal and state level, measures have been adopted to increase government powers to gather information on individuals, such as through surveillance and wiretaps, and to facilitate the sharing of such information among agencies and between governments.[5] The revisions have ignited a serious debate between privacy advocates and the law enforcement community—privacy advocates seeing the expansion of law enforcement "information powers" as irreparably curtailing civil liberties and privacy rights, and law enforcement seeing the expansion as critical to ensuring our physical safety. These issues are not new ones. They are, however, being pushed to the extreme by the current threat—both to our citizens' physical safety and to principles that are the basis of the American way of life.

As justice agencies take advantage of increased information collection capabilities, their responsibility for assuring proper use and dissemination of this information is paramount. This can be achieved by adopting information practices that benefit not only the public but are also good for justice agencies internally. The idea is to

[4] In this instance, the man lost his job, home, and family before becoming aware of the mistake within a law enforcement information system. Although he was successful in having the information corrected in the law enforcement system, the false information had been sold by law enforcement to private information vendors. The incorrect information was not able to be traced or corrected on a national basis. Therefore, the man in this case must continue to live with the knowledge that at any time he could be mistaken, in electronic form, for another individual with a damaging criminal history record. See, *Stolen Identity: Could It Happen to You?* (MSNBC television broadcast, April 18, 2000), http://www.msnbc.com/news/397082.asp.

[5] See the USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

develop an information collection, use, and dissemination policy that meets the needs of the agency and incorporates steps to avoid privacy intrusions.

Developing and implementing privacy policy is not easy. Identifying and assessing privacy issues requires commitment from justice policymakers, information management specialists, and operational employees. Additionally, the costs associated with developing and implementing privacy policy are real and can be substantial. Justice leaders must, however, weigh the costs of developing and implementing a privacy plan against the costs of future privacy intrusions, loss of public confidence and legislative funding, and real costs of modifying information systems to include privacy protections after system implementation.

As part of justice agencies' duties to citizens, national and international justice leaders have placed a priority on information privacy policy development and implementation. In 2000, Office of Justice Programs (OJP)—a component of the U.S. Department of Justice—and the National Criminal Justice Association (NCJA) initiated a program to assist state, local, and tribal governments to develop justice information privacy policies, specifically those privacy policies related to the development of integrated justice information systems. OJP and NCJA, in partnership with the Office of the Ontario, Canada, Information Privacy Commissioner (IPC), worked with leaders from various justice agencies in the United States; privacy experts from Canada, the United Kingdom, and Australia; and representatives from academia, the media, and the commercial sector. A series of workshops produced the *Privacy Guideline for Justice Information Systems*. The *Guideline* addresses privacy concerns associated with new and emerging information collection, access, use, storage, and dissemination capabilities of justice information systems, including integrated information systems.

What Is an Integrated Justice Information System?

The traditional justice system includes law enforcement, prosecution, defense, courts, corrections, probation, and parole agencies.[6] The mandate of the justice system requires these agencies to balance the interests of protecting society and protecting the privacy of individuals. To accomplish this mandate, personal information is collected and used by justice system agencies within a framework intended to identify and apprehend offenders, adjudicate guilt or innocence of adult or juvenile defendants, manage and resolve domestic and family legal issues, settle civil disputes, manage pretrial activities, manage post-conviction and post-judgment activities, support the rehabilitation of the offender and restoration to victims, address repercussions to victims' and offenders' families, manage external risks, and maintain the integrity of the justice process.

Current information systems in the justice sphere range from predominantly paper driven to those that are highly automated and interactive. Increasingly, justice agencies are working together to plan, design, and implement integrated justice information sharing systems. These systems enhance the ability to collect, access, and use information, including personal information, and allow information to be entered once and used across and between many different agency systems.

[6] As used here, the "traditional justice system" refers to the idea of arrest and prosecution of adult, criminal offenders. In modern instances, the criminal justice process includes specialized courts, such as drug courts, juvenile courts, traffic courts, and probation courts, and also interfaces with family courts and probate courts.

The term "integrated justice system" may describe different levels of justice information sharing, depending upon the context in which it is used. In 1999, the NCJA and the Search Group, Inc., developed a definition of integrated justice systems that has been adopted by OJP and its counterparts. As used in this document, the term "integrated justice systems" encompasses *interagency*, *interdisciplinary*, and *intergovernmental* information systems that access, collect, use, and disseminate critical information at key decision points throughout the justice process, including building or enhancing capacities to automatically query regional statewide and national databases and to report key transactions regarding people and cases to local, regional, statewide, and national systems. Generally, the term is employed in describing justice information systems that eliminate duplicate data entry, provide access to information that is not otherwise available, and ensure the timely sharing of critical information.

The desire for the integration of justice systems has grown from the need to improve the operation of the justice enterprise by eliminating duplication of effort, delays in information transmittal, barriers to accessing information, and scheduling and case management bottlenecks. Many of these problems resulted from implementing individual technology solutions in the past without assessing how these technologies interoperate across the justice enterprise. Today's technologies, when applied in a strategic fashion, hold the promise of reduced paperwork, quick information capturing, broad transmittal and access capabilities, improved information quality, and reduced long-term costs.

Information systems are often planned and implemented according to a designated "technology architecture." The architecture is the underlying technology structure and protocols that determine the specifications to which the technology is built and that describe how information can be stored and accessed. A technology system that spans law enforcement, the courts, and corrections, as well as other justice components is characterized as an "enterprise-wide technology." The development of an enterprise-wide technology is even more complex than a single-agency technology architecture. Due to the complexity of enterprise-wide technologies, they are often designed within a conceptual framework, called an enterprise-wide framework.[7] The enterprise-wide framework is a conceptual tool that allows the necessary analysis from various perspectives to take place prior to committing actual resources to implement information technology. It is the detailed planning phase of any multiagency or integrated information system.

Justice agencies need to address privacy issues during the planning stages (enterprise framework) of their individual information systems or the integrated justice system. By agencies addressing privacy at the planning stages, the resulting technology has the best chance of providing desired privacy protections. Implementation without privacy planning can result in having to manage unintended privacy effects and having to retool the system to address these effects.[8] For example, failure to implement privacy policy could result in releasing personal information that could jeopardize the right to a fair trial (e.g., release of address, family affiliation, or criminal

---

[7] See John A. Zachman, *Enterprise Architecture: The Issue of the Century* (last modified June 1988), http://www.zifa.com; John Zachman has developed a multiperspective model critical for the successful design and implementation of an enterprise-wide information technology architecture. See Appendix A for a discussion of what an enterprise technology architecture is and the framework needed to manage implementation of an enterprise-wide technology.

[8] See Niel Postman, *Technopoly* (Vintage Books, New York, 1992)(explaining unintended effects of technologies).

history). Likewise, using inaccurate information that misidentifies a person as an accused or suspected criminal would have potentially vast repercussions in an integrated justice system. The problem compounds when the system itself has difficulty authenticating or correcting information, and in fact has the contrary effect of legitimizing and perpetuating incorrect information: garbage in, gospel out.

Unintended effects have the immediate downside of diverting limited available intellectual capital and financial resources from the goal of implementing and using a justice information system to addressing policy and making technological changes retroactively. Given that privacy continues to grow as a public issue, unaddressed privacy concerns will likely absorb an increasing amount of limited resources allocated to issues management and hasty coding changes.

Therefore, privacy policy should be considered at the design and developmental stages of any agency information system, especially as part of an enterprise-wide architecture. Used in this way, privacy policy is the first step in protecting personal privacy concerns of individuals within the justice system, including persons suspected, accused, convicted, and acquitted, as well as victims, witnesses, and their families. The goal is to operate the system without unintended impacts on individual privacy that could hamper the effective carriage of justice.

What Is the Justice Record?

Justice information systems contain administrative information (information about the agency and its processes), as well as substantive information. The category of substantive justice information, such as arrests, indictments, civil pleadings, civil and criminal court proceedings, dispositions and settlements, incarceration, release and related information, traditionally has been referred to as the justice record. The means by which electronic information systems create, store, and share information requires us to ask, "What is the justice record today?"

Before the advent of electronic information technologies, the answer to this question was fairly concrete. The record was the paper documentation and physical evidence produced or collected by the justice system on a particular matter. Generally, information was shared by transferring or copying documents between agencies, and public access to information in the record could be had by appearing in person at the agencies where various parts of the record were kept and requesting to see the file. Access to information in the record was ultimately controlled by the individual producing the file. Dissemination of the information was controlled by the receiving person's ability to copy documents or remember what he or she had seen. The justice record of an individual relating to one matter was not easily linked with other records of that individual or with records of other individuals on a similar matter. Analysis of information was conducted at "human speed" and based on personal knowledge and association of data. Practicality limited the ability to collect and analyze information across counties, states, territories, and international boundaries.

Enter the information age. Computerization has changed the concrete notion of "papers in a file" into a concept that includes pieces of electronic information created or gathered from various sources and organized by an identifier. This electronic information can be multimedia, including documents, photographs, and audio and video recordings. The pieces of information are indexed, according to the preferences

and needs of the agency. Information once organized and indexed can be shared by justice agencies, analyzed, and distributed worldwide with astonishing speed and efficiency.[9]

Information contained in the justice record is two-dimensional, meaning information must be considered by its type, as well as the context in which it appears. Information contained in the justice record can be "large or small," such as a personal identifier (name) or the sum of many elements (i.e., documents, such as arrest reports, indictments, pleadings, court orders). In order to control the privacy and public safety impacts of releasing information, privacy policy must be applied to each data element in the justice record. Additionally, each element needs to be considered in context.

For example, general information describing dates, places, and events may be deemed discloseable between justice agencies and to the public as part of a justice record. If this information is contained in a document in an ongoing investigation, however, under a public safety function analysis, it may not be discloseable to other justice agencies or publicly accessible until the investigation is concluded. Similarly, a data element such as "address" may be deemed discloseable or publicly accessible, generally. If, however, the address is that of a victim and appears in the victim statement or a court exhibit, a privacy analysis may determine that it is not suitable for interagency sharing and probably not suitable for public access. For a detailed discussion of how to do an element-by-element privacy/public access/justice function analysis, please refer to Chapter Six.

The traditional record consisting of paper reports and other documents, therefore, is being replaced by an electronic "data element compilation." The notion of a compilation of data also has ramifications for existing law and policy relating to specific types of justice information, in particular the official criminal history record. (See discussion below.)

As is evident when one compares the justice record in the old sense with the new, "inconvenient or impossible access" that was an accepted part of paper record systems' privacy and public access policies no longer provides presumed protections in an electronic age. Broader access to justice information, including personally identifiable information, is an inherent result of new information technologies, and privacy policies must reflect the new information access, sharing, and analysis capabilities.

How Does New Technology Affect Information Privacy Law?

Although there exists no explicit federal constitutional right to privacy,[10] privacy rights have been articulated in limited contexts by the Supreme Court. These "zones

[9] Theoretically, sharing of information between various entities is possible through indexing. Currently, lack of indexing standards may impede the seamless exchange of information. This discussion is attempting to articulate the concept of electronic information sharing capabilities, recognizing that technologies are rapidly catching up to this capability.

[10] The most closely related constitutional right is that under the Fourth Amendment, which prohibits unreasonable search and seizure of individuals and their houses, papers, and effects. U.S. Const. amend. IV. Some states, such as California, recognize a right to privacy in their state constitutions. See Cal. Const. art. 1, §1 (West 1983).

of privacy" include "matters relating to marriage, procreation, contraception, family relationships, child rearing, and education."[11]

Historically, individuals' information privacy rights have been articulated in federal and state case law and statutes governing the areas of medical, financial, educational, and consumer data.[12] Privacy interests have also been recognized and protected in statutes and regulations governing collection, use, and sharing of justice information, specifically relating to the official criminal history record,[13] information collected for research or statistical purposes, criminal intelligence systems, and juvenile justice record keeping.[14] Today's expanded information sharing capabilities are blurring the lines between traditional criminal, civil, juvenile justice, social service, education, and medical records, giving rise to a new generation of privacy issues by causing these new types of information sets to fall outside existing legal frameworks.[15]

For example, the "criminal history record" is a subset of the entire justice record containing individuals' arrest and disposition information. Traditionally, an official criminal history record was created and maintained at a state repository. With the advent of information technologies allowing integrated sharing of information between justice agencies, creation of "unofficial" compilations mirroring the information of the criminal history record are possible to obtain from state or local justice agencies, such as the courts, or from private information purveyors. In addition to the traditional arrest and disposition information, such compilations may include information relating to probation, social services, child custody, and drug treatment, among other things. These unofficial compilations may not fall under laws intended to protect a specific privacy interest, such as an official criminal history record, medical, financial, or educational information. Proper use and disclosure of these compilations may require attention to a number of state and federal privacy laws.

Who Is Responsible for Assessing and Implementing Privacy Policy in the Justice System?

As noted above, successful privacy policy development and implementation requires a combined effort of policy leaders, information technology managers, and line system

---

[11] Paul v. Davis, 424 U.S. 693, 713 (1976). For a discussion of federal case law relating to information privacy interests in justice information, see Paul F. Kendall, Neal J. Swartz, Anne E. Gardner, *Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: The Need for Principles of Responsible Use*, 21st Annual International Conference on Data Protection and Information Privacy, Hong Kong (Sept. 1999), http://www.pco.org.hk/english/infocentre/conference.html.

[12] See, id; see, e.g., Health Insurance Portability and Accountability Act of 1996, 42 U.S.C.A. §201 note, §1320d (Supp. 2000); Family Education Rights and Privacy Act of 1974, as amended, 20 U.S.C. A. § 1232g (2001); Children's Online Privacy Protection Act, 15 U.S.C.A. §6501 (Supp. 2000); Fair Credit Reporting Act, 15 U.S.C. §1681 (1998); Digital Millennium Copyright Act, 17 U.S.C.A. §101 note (Supp. 2000); Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999), Pub. L. No.106-102, 113 Stat 1338 (1999). In addition, see http://www.epic.org/privacy/billtrack.html for a summary of current privacy legislation. Federal statutes can be accessed at www.washlaw.edu. Federal public laws and bills can be accessed at http://rs9.loc.gov/home/thomas.html. A current summary of state and federal statutes can be found in Robert Ellis Smith's *Privacy Journal*, Post Office Box 28577, Providence, Rhode Island 02908, 401-274-7861, 5101719@mcimail.com.

[13] Traditionally, a report created and held by a state repository showing criminal arrests and dispositions of each offender. Juvenile records are typically not a part of the criminal history record.

[14] See *e.g.*, 28 CFR Parts 20, 22, 23 (2001); 34 CFR Part 99 (2001).

[15] For a discussion on implications and effects of advanced information sharing capabilities in the justice system, see Paul F. Kendall, Neal J. Swartz, Anne E. Gardner, *Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: The Need for Principles of Responsible Use*, supra n.11.

users. This combined effort is needed in developing and implementing privacy policy in a single justice agency system, as well as in an integrated justice system.

Justice information privacy policy development is largely the responsibility of high-level policy executives within the justice system. This person or group of persons is sometimes referred to as the "information steward" for the justice agency or integrated system. The information steward will be guided by jurisdictionally applicable law or regulation and may look to sources of policy guidance, such as the privacy design principles described below. The information steward may also determine that certain policy questions rise to a level that require public discussion and political attention. In these instances, privacy policy development may need to be supplemented by legislative action.

Implementation of the privacy policy and identified law rests with justice agency policy and technology managers, as well as technology and line staff. Tools, such as the privacy policy template and the privacy impact assessment for justice information systems, described later, are available to assist in this process. It is imperative that privacy policy implementation be a cooperative effort of justice managers and technology staff. For effective implementation, there must be a keen understanding of justice business practices, as well as technology design. Therefore, in most cases, responsibility must be divided between these two areas of expertise, rather than both areas assigned to either managers or technology staff.

Section II

Developing Privacy Policy

Chapter Three:

Privacy Design Principles for Justice Information Systems

Purpose: to present privacy design principles that apply to the design and implementation of justice information systems, as well as specific privacy issues associated with integrated justice systems

This discussion of the design principles focuses on the adult criminal justice process. The principles, however, are applicable to civil, juvenile, family court, and other justice records in single-agency systems or in the context of an integrated justice system architecture.

A History of Privacy Codes

The following history is provided to inform the discussion surrounding the development of privacy design principles and technology design principles that best address state, local, and tribal justice systems.

The basis for privacy design principles worldwide is the Organization for Economic Cooperation and Development's (OECD) fair information practices (FIPs), developed in the 1960s and 1970s to address technology implications at the time. The FIPs were codified in the OECD guidelines in 1980 (see Appendix A). Despite advances in technology, the FIPs remain universally recognized as a solid foundation on which to build everything from privacy legislation to self-regulated privacy standards for the private sector.

The FIPs[16] place restrictions on the collection, use, and disclosure of personal information. Their goals are summarized as follows:

1. Limiting the collection and use of personal information for the purposes intended;
2. Ensuring data accuracy;
3. Establishing security safeguards;
4. Being open about the practices and policies regarding personal data;

[16] Http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM#3. See Appendix A for full description.

5. Allowing individuals access to their personal data and the ability to have it corrected; and

6. Identifying persons accountable for adhering to these principles.

The FIPs have been adopted by the commercial sector in the United States, and many commercial privacy policies have been drafted using the FIPs as a guide. With some modification, the FIPs form the basis for the privacy design principles for justice information systems set forth below.

Subsequent to the OECD guidelines, the European Union (EU) released its Data Protection Directive in 1995, which went into practice in 1998.[17] Under the directive, data subjects are granted a number of important rights and may appeal to independent national authorities if they consider their rights are not being respected. These rights include:

1. Information from subsequent data users about where the data originated (where such information is available), the identity of the organization processing data about them, and the purposes of such processing.

2. A right of access to personal data relating to him/her.

3. A right of rectification of personal data that are shown to be inaccurate.

4. The right to opt out of allowing their data to be used in certain circumstances (for example, for direct marketing purposes) without providing any specific reason.

In cases where data are transferred to non-EU countries, the directive includes provisions to prevent the EU rules from being circumvented. The basic rule is that the data should only be transferred to a non-EU country if it will be adequately protected there, although a practical system of exemptions and special conditions also applies—such as for data where the subject has given consent or which is necessary for performance of a contract with the person concerned, to defend legal claims, or to protect vital interests (e.g., health) of the person concerned.

To interact with the EU directive, both Canada and the United States have pursued different strategies. The Canadian federal government has chosen to pursue legislation based on the Canadian Standards Association Model codes. These codes have clear parallels with the OECD guidelines and the EU Data Protection Directive. The United States Department of Commerce, however, has taken a different approach to interacting with the EU through the development of the International Safe Harbor Privacy Principles (Safe Harbor).[18]

The Safe Harbor is a voluntary compliance program that allows American companies to exchange information with European businesses. To be a part of the Safe Harbor, an organization can join an existing self-regulatory privacy program that adheres to

---

[17] For a more detailed description of the EU directives, see http://europa.eu.int/comm/internal_market/en/dataprot/index.htm.

[18] The Safe Harbor became effective November 1, 2000 (see Appendix B). The Safe Harbor was developed in consultation with the European Union as a way to 'bridge the gap' between the comprehensive legislative protections required under the EU Directive on Data Protection and the United States' more loosely defined legislative and self-regulatory framework. For more information on the Safe Harbor, see http://export.gov/safeharbor. Other non-EU countries have developed legislation similar to that discussed above or continue with self-regulation. See http://www.pco.org.hk/conproceed.html.

the Safe Harbor's requirements, or develop its own self-regulatory privacy policy that conforms to the Safe Harbor principles. The Safe Harbor requires that organizations comply with seven principles: notice, choice, onward transfer, access, security, data integrity, and enforcement. (See Appendix B.) These principles are based on the FIPs described above.

Unique Privacy Characteristics of the Justice System

The FIPs are a good starting point for developing privacy design principles. However, the justice system has a set of unique characteristics that must be taken into account. For a start, the right to privacy must be balanced with the need to carry out the administration of justice and its prime goal: protection of society. Without overly dramatizing the situation, the way in which a justice agency uses personal information in the administration of justice is vital to the protection of society and can result in life or death situations. In addition, there is a need for the public to access personal information where it directly relates to the integrity and effectiveness of the justice system process. This includes public access to information on the accused, witnesses, and victims, as well as an agency's daily operating information.

Therefore, although important, privacy design principles should not be viewed as changing the balance or diminishing the value of fairness inherent in the justice system. In other words, privacy design principles themselves cannot create an advantage or a disadvantage to any part of the justice system or serve to "close" the system to the public.

Rules and protocols

For these reasons, a justice agency or integrated justice system must have privacy rules that recognize and distinguish the different mandates of specific justice agencies. The privacy rules must also recognize the status of the individual and the relationship of that person to the various justice agencies. Information must be assessed in context, rather than just by its "type," when gathered. For example, a convicted criminal's personal information would be dealt with differently than a witness's personal information. Furthermore, treatment of personal information collected for investigation may differ from information collected and used in a case processing system.

In addition, different information sharing rules apply. Rules, or protocols, for sharing information within the criminal justice system (e.g., police, prosecutors, defense, courts, and corrections) would differ from rules used to determine the disclosure of that information to parties outside the justice system. For example, the police and prosecutors must share more information between themselves than is publicly available regarding an arrest.[19]

This discussion, while pointing to the complexities of information privacy policy in an integrated justice system, should not cause one to jettison the value of undertaking such policy development. The privacy design principles and other tools in this *Guideline* are intended to assist in the development of policies and technologies for responsible information management in an agency or integrated justice system.

[19] See Chapters Four and Five on public access.

Legislative context

Most information systems worldwide are required to work within some type of legislative framework. However, an integrated justice system in the United States has to work within a detailed patchwork and array of legislation and regulations. One is federal legislation, such as the Crime Control and Safe Streets Act,[20] as well as state-specific legislation that requires greater and lesser degrees of control of personal information.

There is also a body of case law governing privacy and public access challenges by persons against various state and federal legislation and agency practices. In addition, different states and tribes have varying policies and laws regarding the degree of privacy a person can expect if he or she has a relationship with the justice system. Therefore, the legal context needs to be mapped clearly for each agency or integrated justice system technology project according to the laws governing the jurisdiction.

Eight Privacy Design Principles for Justice Information Systems

To be effective, a privacy policy should be built into the technology design at the outset of every information system's initiative. This requires the development of a privacy policy and the communication of this policy to the technology implementers.

The privacy design principles below provide an ideological basis for designing and implementing privacy policy. Therefore, it is important for policy drafters and technology implementers alike to read and have an understanding of these principles.

The drafters of the following eight privacy design principles have undertaken two steps to structure the principles for practical use and understanding:

1. The internationally accepted FIPs are used as a base from which to develop justice-specific privacy design principles.
2. A set of technology design principles are introduced to assist a project's "technology design architect" to bring each privacy principle into the enterprise architecture.[21]

1. Purpose Specification Principle

The purpose specification principle requires the identification of the purpose for which personal information is collected.

When personal information is collected by a justice agency system, the system's purpose[22] should be specified in writing, not later than at the time of data collection.

---

[20] See Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 1968 U.S.C.C.A.N. 237, as amended. See also 28 C.F.R.23.1 (1999). (The Office of Justice Programs is authorized to promulgate policy standards to assure that criminal intelligence services funded by the Omnibus Crime Control and Safe Streets Act "are not utilized in violation of the privacy and constitutional rights of individuals.")

[21] "Enterprise architecture" refers to the specifications of an information technology that spans multiple organizations and allows those organizations to share and use information in a seamless and transparent way; i.e., no "stovepipe" technologies.

[22] The purposes for the criminal justice system are well-established. They include law enforcement, criminal investigation, public protection, and the justice process. For this principle, these purposes need to be specified to ensure that the resultant technology design fosters adherence to the principle.

The subsequent use (see principle 4) must be limited to the fulfilment of those stated purposes or other compatible purposes[23] that are specifically identified. As well, the personal information collected should be pertinent to the stated purposes for which the information is to be used.

The purpose statements also need to address various third-party and private sector partnerships or relationships where personal information is or will be disclosed.[24]

For example, each component of the justice system (law enforcement/investigative systems, prosecutorial systems, defense systems, court systems, corrections systems, and probation and parole systems) would have a set of stated purposes for collecting information. These purposes need to be articulated prior to the technology design and prior to the outset of data collection.[25]

In an integrated system, these purpose statements must be harmonized during the technology design. Even though information in an integrated system can be easily reused, the purposes for collection by each component of a justice system should be relatively stable, thus providing a benchmark to determine appropriate secondary use.

Generally, the purpose statements should directly relate to the mandate of the relevant sector of the justice system. For example, the purpose of law enforcement agencies for collecting personal information is to investigate (suspected) criminal activity to bring suspects to trial, whereas the purpose of the court system is to process cases, provide accurate and complete information for judicial decisions, and produce dispositions for complete criminal history records. The purposes of these systems should be harmonized to provide a "privacy framework" governing collection, use, and reuse of personal information.

Technology design principle. Organizations must clearly identify and document the purposes for collecting personal information. System design must ensure that the system's outcome is limited to the purposes for which the personal information was lawfully collected and disclosed. We must pay attention during the design stage in all instances where personal information is disclosed regularly to one or more parts of the justice system. We must also pay attention to the building of a technology that easily enforces access restrictions to personal information available to parties outside the justice system. Information can be publicly available through two methods: information released by a component of the justice system; e.g., for public safety, or requested by a third party; e.g., the media.

---

[23] A compatible purpose is one that matches or is in harmony with the original stated purpose. The underlying logic in this thought is that the reuse of personal information is restricted to original stated purposes or similar purpose statements that are required prior to reuse of data. This will be critical in situations where third parties wish to access or purchase justice information. This will also be critical to manage data use. For example, the privacy design principles need to address third parties' (ranging from strictly private sector to quasi-justice system) access and use of information; for example, third parties wishing to scan justice information to look for potential drug rehabilitation customers, or a credit-rating agency wishing to access court data. Use of the purpose principle is a way to have third parties contractually bound to how they can use the data.

[24] Assistance for developing policy for these types of disclosures is addressed in Chapters Four and Five on public access.

[25] An example of a purpose statement for a law enforcement body would be as follows: the state police collect personal information in the pursuit of suspected offenders, for public safety, and to bring offenders to trial.

2. Collection Limitation Principle

The collection limitation principle requires agencies to carefully review how they collect personal information to avoid collecting personal information unnecessarily.

There should be some limits[26] placed on the collection of personal information. Personal information should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent[27] of the data subject. It is important to remember that an individual's knowledge and consent rights will be limited depending on his or her relationship to the justice system (e.g., suspect, offender, victim, witness, juror, or offender's family).

A test of relevance should also be applied (e.g., by an independent third party or as authorized in legislation) when collecting personal information on individuals without their knowledge or consent, or when the individual is not charged with a crime; i.e., under investigation, or when an investigative body is "information gathering."

This principle differentiates between the knowledge and consent rights of an offender, arrestee, the victim, witness, juror, offender's family, or victim's family. Special consideration must be made to limit collection of personal information on victims, witnesses, and jurors (e.g., to test their credibility). For suspects or accused persons, although broader, the collection limits should be set by the legislative framework and legal precedent. However, obtaining a person's consent to collect their personal information is generally not applicable during case[28] investigation or prosecution.

The "collector" of personal information varies. For example, in the criminal justice system, the collector is generally law enforcement, while in the civil justice system, it is the parties. In the criminal justice system, personal information is collected by law enforcement, prosecutors, defense attorneys, and pretrial services officers on suspects and those associated with the suspects, including victims, witnesses, and family members. As well, personal information is generated by the workings of the justice system itself, as the offender moves through the various components of the justice system. For example, an arrestee's fingerprints are taken and an identification number issued. These identifiers are created by the justice system, pass through it, and are maintained as part of an official record.

Technology design principle. The limits and special circumstances set out in the collection of personal information principle must be incorporated into the design of information systems to ensure that extraneous personal information is not collected. We must define extraneous information for each relationship an individual has with the justice system. Generally, information is extraneous unless it has relevance to the integrated justice system's purpose statements. This definition is critical, as technology has the ability to automatically search for information on a person in an ever-increasing number of databases.

---

[26] Determining limits is a difficult task in the justice system. A test of necessity; i.e., what is necessary to collect, would need to be developed by state and local justice systems. This would involve stating and assessing "why" a component of the justice system would need to collect (i.e., "know") that information.

[27] Consent from victims prior to data collection needs to be addressed.

[28] State and local justice systems need to define "case" under various components of the justice system; i.e., probation case, corrections case.

3. Data Quality Principle

The data quality principle requires agencies to verify the accuracy, completeness, and currency of their information.

Personal information contained in an information system should be accurate, complete, current, and verified.[29] This normally assumes that the individual has some means of accessing his or her own information in the system to ensure it is accurate and up-to-date.

However, because in the justice system "notice to and access of" the individual may not be available, other methods are needed to ensure that the information held is accurate and up-to-date. These methods can involve passive data analysis, including cross-referencing, that identifies anomalies, plus authorized human correction that could involve the data subject.

Separate from privacy concerns, data source identification, data management, and record retention need to be addressed as part of data quality. Inaccurate personal information can have a devastating impact on the person and the integrity of proceedings within the justice system. The accountability for data quality lies with the system's information steward as further described in principle eight.

Technology design principle. We must design the technology to ensure efficient data access and correction. As well, the technology requires a streamlined methodology for logging or tagging the access and correction of information, recording changes, by whom, when, and for what reason, to ensure accountability. Where a record of corrections is retained, the inaccurate information should not be routinely disclosed within the justice system.

To ensure data quality, the technology design must foster "data verifiability." This is the process of ensuring data is sought where missing, and flagged or excluded where found inaccurate. This process of data verification also demands a technology design that tags data as confirmed and either accurate or inaccurate, or "to be confirmed."

For example, the technology design must have standardized security routines that address how certain people access the data and what standard of proof is required to amend data. For instance, the types of questions that need to be asked are: Does a victim have access to all the data in the file or just his/her statement? Does technology allow for redaction of nonvictim data? If an error is found, who decides what the correct information should be? Is there an administrative process with a legal standard—preponderance of the evidence (more likely than not)—for amending the information?

Finally, technology must support data standardization across various data systems.[30] This would support use of same or comparable terms, data entry fields, data definitions, and data structures. For example, data fields need to be interoperable, and field edits and meta-data definitions need to be consistent.[31]

---

[29] Reliability of information is a key priority that needs to be designed into an integrated justice technology system. For example, raw investigative information could be fraught with inaccuracies until verified or cross-checked with other data.

[30] This does not eliminate the need for case comments, or text boxes, as they are needed; e.g., for probation. However, free-flowing text needs to be restricted as much as possible. Advances in XML standards offer a method to share more robust data fields. For more information on XML, see http://it.ojp.gov/global/standards/xml.html.

[31] Certified court transcripts pose a challenge, as they cannot be corrected.

4. Use Limitation Principle

The use limitation principle requires agencies to limit use and disclosure to the purposes stated in their purpose statements.

Personal information should not be used or disclosed for purposes other than those specified in accordance with principle 1, except (a) with the consent of the data subject; (b) by the authority of law; (c) for the safety of the community, including victims and witnesses; or (d) pursuant to a public access policy.

Generally, personal information should be retained as necessary, but its use must be limited to its original purpose for collection as outlined in principle 1. Use limitation, generally, is more applicable where information is disclosed outside the justice system, where issues of safety, risk, and the right-to-know by the public are factors applied in the use limitation principle. Within the criminal justice system, applying the purpose for collection stipulated in principle 2, the use limitation principle between agencies applies under exception (b); that is, when provided by the authority of law. Additionally, the use limitation principle has effect in an integrated justice system where various components' systems "use purposes" are limited by having been harmonized.[32]

A general pattern of the use of personal information suggests that within the justice system, use is determined by access authorization and by assuming the doctrine of "consistent use." Consistent use means that the way in which the data is used or reused stems directly from the stated purpose(s) for which the data was collected initially. Where information is not being handled under "consistent use" within an information system or between systems, notification and specific authorization might be warranted.

Outside the criminal justice system, use is increasingly limited as the audience migrates from victims to the public. Public access issues are complex and problematic. Policy guidelines addressing public access issues are set out in Chapters Four and Five.

It is important to note that there are a growing number of "gatherers" who make a living from uncovering personal information about citizens from government databases. Often referred to as "bulk data," the sale of government databases to the private sector changes data's intended use and accessibility, thus dramatically increasing the likelihood of abuse. In addition, compilations of legal data prepared by the private sector may result in unintended consequences for citizens exercising their right to participate in the judicial system. For example, it is not uncommon for rental or housing associations to develop databases of persons who have filed an unlawful detainer claim. These legal actions are likely to be based on a valid claim by the renter or homeowner; i.e., for lack of repair. The information in the database, however, follows an individual forever and may result in denial of housing.[33]

A third area of concern is information sharing between "closed-record" states and "open record" states, where the information not available to the public in the closed-record state becomes publicly available once it is shared with the open-record state. This type of availability has created a market for private information gatherers to

[32] Use limitation also includes access limitation and levels of authority to access certain types of information within the justice system. Part of this can be developed using the need-to-know principle. Other parts can be developed through access and security protocols. For example, distinctions should be made for certain types of information (pre- and post-guilty information), who has access to that information, as well the types of access (e.g., read only).

[33] See Chapter Five for a discussion of bulk data issues.

use justice system access in one state to provide nonaccessible information to parties in their home state.

These types of data gathering have privacy implications that need to be addressed up front in integrated justice systems. Managing the sale and access to justice information may be difficult given the legislative framework in some states. Ideally, the sale of information in bulk should be limited to recognized justice system purposes as enumerated in principle 1, and contracts for the sale of bulk information should require compliance with privacy principles.

Through a privacy impact assessment, a justice system can be reviewed by the government for the impacts of information-handling practices. Ongoing reviews are necessary as future changes increase the ability to gather and use information and as market forces control these processes.

Technology design principle. Privacy policy should drive the design and development of technology, rather than technological capability dictating the formation of privacy policy. We cannot assume that personal information collected for one purpose should be used or shared for an unrelated purpose. Information systems must be designed to halt unauthorized uses of personal information. This involves authorization procedures for access to information, even within the justice system, that in turn involves a protocol for tracking who accesses information and for what purpose. The circumstances of additional use need to be recorded and attached to the record. As well, a record of data linkage needs to be created and attached to the record, allowing for the development of an audit trail and enabling a use assessment.

The technology design also needs to address issues of disclosure. There are occasions where historical data are appropriate for disclosure within the justice system (former aliases, addresses, etc.), but perhaps not outside the justice system. The decision rests on whether the most recent data are "updates" or "corrections." This is an area where this technology design principle dovetails with principle 3, data quality design.

Data matching and data mining, where personal identifiers have been stripped from the record, fall outside of this design principle.

5. Security Safeguards Principle

The security safeguards principle requires agencies to assess the risk of loss or unauthorized access to information in their systems.

Reasonable security safeguards against risks[34] should protect personal information against loss or unauthorized access, destruction, use, modification, or disclosure. These safeguards should be provided according to the sensitivity of the information and risks to all involved parties. This principle recognizes that personal information collected by the justice system is highly sensitive and a natural target for compromise. The adage of Robert Morris Sr., former Senior Scientist, National Security Agency, should always be remembered in the design of the security architecture of a justice information system: never underestimate the time, expense, and effort someone will expend to break your technology. This principle is not designed to cover all

[34] Risk assessment is an integral part of this process. It needs to identify all the potential data users as well as intruders. It also needs to include disaster recovery strategies.

aspects of security for a justice agency. It focuses on the access security of information systems.

An example of risk assessment and the application of security safeguards is federal regulation 28 CFR Part 20, dealing with criminal history information, and 28 CFR Part 23, dealing with law enforcement intelligence systems. These regulations, promulgated in the late 1970s, address specific security procedures for state and local justice information systems and require the implementation of these procedures on systems that are funded in whole or in part with federal dollars from the Office of Justice Programs (OJP). OJP acknowledges the need to update 28 CFR Parts 20 and 23 to correspond to the capabilities of today's information technology. In revising the current regulations, it is important to note that security is an area that will be constantly driven by technology. Although security policy, like privacy policy, should not be based on specific technology, the implementation of security safeguards will necessarily be dependent upon current technological capabilities.

Technology design principle. Organizations need to conduct information classification reviews to determine the appropriate level of security to apply, taking into account certain types of personal information, as well as the auspices under which the information was collected. The level of security is dependent on the sensitivity of the information and its value to both authorized and unauthorized parties. As well, methods should be in place to record failed attempts to alter information or attack the system.

Some of the current methods to maintain security include:

- Public key infrastructures;
- Data encryption;
- Access controls;
- Remote access, two-way user authentication;
- Log-in and password management;
- Procedures for monitoring records of access to information; and
- Risk assessment.

6. Openness Principle

The openness principle requires that agencies provide notice about how they collect, maintain, and disseminate information.

There should be a general policy of openness about developments, practices, and policies with respect to the *management* of personal data (apart from the actual data). Openness includes public access to the management practices of the data, except where it directly relates to an investigation, a pending or open case, or involves safety concerns and other factors that a government determines as necessary exceptions.

Openness also includes public access to establish the existence of personal data and access to the actual data pursuant to an official public access policy. Access should

provide the main purposes of the data's use, as well as the identity and office of the data controller responsible for that data.

In an investigation or prosecution of an offense, established legal precedent and evidentiary rules will determine the openness principle or exceptions to it.

The openness principle also requires clear communication to affected individuals where justice records are requested, sold, or released to third parties. This may require that the public be informed when information is sold in bulk for commercial purposes.[35]

This principle is necessary for accountability and to implement the purpose specification principle.

Technology design principle. A justice information technology system is not transparent in its information. It does not easily allow individuals to verify how their information is collected, used, or disclosed, nor should the technology necessarily make its practices and policies open to the public. However, the information technology system must be designed to allow for some method of independent oversight, as the openness principle must be part of the technology for the purpose of accountability.

One way to accomplish the openness principle is through a proxy[36] who provides independent oversight. The system is designed to be transparent to the proxy and authorized system users, showing the types of transactions and linkages within the system, as well as the way in which personal information is collected, used, disclosed, and retained. When appropriate, the technology must be able to provide to the proxy a full description of all the circumstances where an organization discloses an individual's personal information to third parties, both inside and outside the justice system.

Information systems must be designed to allow all transactions (including who made changes, when, and for what purposes) made on an individual's file to be traced for accountability purposes (addressed in principle 8). A history of transactions must be retained for audit purposes and to respond to complaints.

7. Individual Participation Principle

The individual participation principle requires agencies to allow affected individuals to access their information.

---

[35] This type of notice continues to be a controversial issue that requires the balancing of the public's right to access the information with the individual's right to protect the secondary use of his information. See Chapter Five for further discussion on bulk data issues.

[36] A proxy function may be introduced in applying the privacy design principles to allow for the necessary accountability for an information technology system comprised of personal information, while taking into account that investigation and court proceedings could be compromised if individuals had access to their information. The nature of a proxy should be a point of discussion at the federal, state, local, and tribal levels. An option for a proxy is a point of systemwide accountability and advocacy, with audit functions, to ensure the privacy design principles are functioning as intended and personal information is not being misused. In small jurisdictions, the proxy function may be provided by the state or in a reciprocal arrangement with a neighboring jurisdiction. In any case, the proxy role needs to be developed by jurisdictions implementing automated justice systems. It should be noted that a proxy in this context is distinct from an agent who acts on behalf of an individual.

Given the unique environment of the justice system, an individual, or an agent for an individual or for victims and witnesses, should have the right, except as it would compromise an investigation, case, or court proceeding:

1. To obtain confirmation of whether or not the data collector has data relating to him;
2. To have communicated to him, data relating to him/her, 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/her;
3. To be given reasons if a request made under 1 and 2 is denied, and to be able to challenge such denial;
4. To challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed, or amended; and
5. To provide an annotation to data where an organization decides not to amend information as requested by an individual or an agent for an individual or for victims and witnesses.

Technology design principle. An information management system must be designed to provide an individual, or an agent for a requesting individual, copies of personal information without disrupting the ongoing operation of the justice system.[37] An example of this would be a system's ability to gather, collate, and disclose required pretrial information or to respond to the Freedom of Information Act requests efficiently.

The information management system must be designed to provide efficient access for authorized use and approved releases of information in a form that is readily understandable and at the lowest cost possible to the individual. For example, an integrated system may contemplate "one-stop shopping" for the public or a pointer system that directs the public to locations of information. This is discussed further in the following chapters.

An information management system must be able to amend or annotate personal information subject to disagreement over accuracy. The system must also have the capacity to notify third parties, in a timely manner (optimally in real time), who have either provided incorrect information or received incorrect information. Information systems must be designed so that all transactions (including who made changes, when, and for what purposes) made on an individual's record can be traced for accountability purposes (see principle 8).

8. Accountability Principle

The accountability principle requires agencies to have a means to oversee and enforce the other design principles.

Accountability should be established within each information system to assure the development and compliance with procedures that give effect to the principles stated above. The accountable party (information steward), whether an individual or a body, must preserve the meaning and integrity of the other design principles and

[37] Decisions on release or nonrelease of personal information must be established in a protocol that is in accord with the openness principle and the system's public access policy.

assess their effectiveness throughout the operation of the justice agency or integrated system. Roles and responsibilities of the information steward should be established by the system's key partners at the developmental stages of an agency system or an integrated justice information system.

The accountability principle is the "due process" mechanism of the eight design principles. An individual or his proxy should be able to challenge the system's compliance with any one of the privacy design principles through administrative procedures designed, implemented, and enforced by the information steward. The information steward should assure that procedures are in place that guarantee a timely, fair response to inquiries.

Technology design principle. To affect the integrity and meaning of all the design principles, there must be a mechanism to ensure accountability within the system. This may be accomplished through a high-level body or individual acting as an "information steward": a designate accountable for the privacy of personal information in the design and development of the justice information technology system.

Accountability practices for which the information steward would be responsible include:

1. Ensuring all the above privacy design principles have been incorporated in the technology design from the conceptual and contextual stages through implementation;
2. Ensuring information systems are capable of providing access to personal information on request and recording who has had access to the personal information and for what purpose;
3. Ensuring staff managing data are trained on privacy protection requirements as detailed;
4. Ensuring information systems are transparent and documented, so that individuals or a proxy can be informed about the collection, use, and disclosure of their personal information within the context of the principles outlined above;
5. Establishing regular security and privacy compliance audits commensurate with the risks to the data subject or other individuals with a relationship to the justice system. This would involve using internal auditors, public oversight agencies, and external independent auditors;
6. Ensuring that specific areas dealing with heightened privacy interests are addressed through policy, such as public access and juvenile justice information; and
7. Ensuring that the above privacy design principles and other privacy policies are providing the intended privacy protections through conducting regular privacy impact assessments. (See Chapter 7.)

Using the Privacy Design Principles

The privacy design principles are intended to provide a framework for state, local, and tribal governments to use when forming their justice systems' privacy policy

and identifying technology requirements. Recognizing and agreeing upon the privacy principles in this document is the first step to incorporating meaningful privacy protections into justice information systems. State, local, and tribal governments should also review and discuss any privacy law or regulation specifically applicable to their jurisdiction. Strategies for actual implementation of the design principles and privacy laws are discussed in Chapter Six.

State, local, and tribal governments need to begin by exploring how the privacy design principles can be incorporated into plans for new information systems and enterprise-wide architectures, and how they can be applied to existing justice information systems. In beginning these discussions, it may be helpful to consider privacy principles in the context of two audiences:

- Internal, meaning those agencies that make up the core of the justice system: law enforcement, prosecutors, defense counsel, pretrial services personnel, judges, court administration, correctional facilities, probation and parole bodies, victims services, and associated agencies; and
- External, meaning those players (e.g., charged or convicted offenders, plaintiffs, witnesses, victims, or public) that could have a relationship with the justice system but are not an operational part of the system.

Each audience requires an identification of issues that need to be addressed within the privacy design principles. It is important to note that the principles work under the assumption that any collection of personal information by members of the justice system is warranted, legal, and meets the test of reasonableness. For example, trawling[38] personal shopping information through loyalty cards for the purchase of large quantities of baggies is reasonable if searching for specific suspected drug traffickers. It is unreasonable if there are no suspects and the trawling is only based on the assumption that any significant purchase of baggies is suspicious, subjecting citizens who blanch large amounts of vegetables to unreasonable invasions of privacy. It is also important to note that when considering the "internal" justice system audience, there is tendency to assume a free flow of personal information relating to anyone with a "relationship" to the justice system, as long as the sharing is done pursuant to stated purposes.

Putting Together a Privacy Policy

The first step in drafting privacy policy is to develop the policy's broad objectives. The person(s) responsible for the privacy policy is the system's information steward. A privacy policy will balance the competing interests of public safety, privacy, and public access. Therefore, the information steward should involve the proponents of each of these interests in outlining the policy objectives.

Initial policy discussions should involve a cross section of interests, including justice agency practitioners from the drafting agency and any agencies[39] that will share information with it, legislators, individuals from the community, victims, media representatives, privacy advocates, commercial sector (information services),

[38] Trawling is used here to describe the process of casting a wide net in the waters of information with the broad intent to catch "something."

[39] Including indigent defense officials or other representatives of the legal interests of the individuals whose personal information will populate the justice information system.

academia, affiliated government agencies, and any other interested parties. An information steward convening such a group should not expect to receive specific direction for outlining the policy objectives but should use the group to identify the outer limits of each varying perspective.

Insights from the interaction of participants with competing viewpoints has two benefits: first, articulation of competing information interests informs the balancing of those interests, and second, competing interests are given the opportunity to participate early in the policy process, thus showing an environment of inclusion by the drafting agency. With so many interests involved in this discussion, the information steward might choose to obtain the assistance of a neutral facilitator. A neutral facilitator can record and discuss opposing viewpoints without the appearance of institutional bias.

The second step is to take the knowledge from the interest group and outline policy objectives according to the justice mandate of the drafting agency and in an effort to balance the competing information interests. The information steward may employ the talents of an individual or group of individuals within the agency to articulate these objectives in a few broadly worded phrases. The objectives will form the basis from which specific provisions of the privacy policy are drafted through the use of the policy drafting template in Chapter Six.

After articulating the policy objectives, the information steward, if not the top policy authority, should inform the top policy leaders (i.e., legislators, executive branch heads, and the judiciary) and seek buy-in on the objectives. The objectives may be modified as desired. After high-level buy-in is achieved, in the interest of inclusion, the agency may wish to inform the original interest group participants of the objectives upon which the agency will develop its privacy policy. Such disclosure gives possible opponents the opportunity to react to the broad objectives before detailed policy is developed. The drafting agency is not required to modify its objectives to satisfy every criticism. The careful articulation of the objectives, however, will allow the agency to explain and support its decision process.

When a set of objectives is in place, the information steward and policy drafters can begin the policy building process as described in Chapter Six. Many privacy policy questions can be solved by applying the privacy design principles relating to purpose, collection, use, and dissemination. Some underlying policy questions, such as the sensitivity of distinct information, and when and to whom it should be released, are more difficult to answer. The template in Chapter Six, in conjunction with the discussions in Chapters Four and Five, provides a framework for solving these difficult policy issues.

The final step in developing privacy policy is to subject the policy to a privacy impact assessment to determine whether the policy results in the anticipated privacy protections. Chapter Seven provides a privacy impact assessment for individual agency and integrated justice system policies. Ideally, an agency will be developing a privacy policy in conjunction with the planning stages of a new information system or an existing system modification. The privacy impact assessment can be used to test the policy at each stage of the new system or modification. If a privacy policy is being developed for an existing system, the privacy impact assessment is still useful to test its implementation.

Chapter Four:

Determining Rules for Interagency Information Exchange and Public Access

This chapter explores the privacy implications associated with collection, use, and sharing of personally and nonpersonally identifiable information within and without the justice system (public access) and how those implications shape information policies.

Purpose: to provide a theoretical basis for use in developing rules for interagency data exchange and public access to justice information

Determining Rules for Interagency Information Exchange

Current information systems in the justice sphere range from predominantly paper-driven to those that are highly automated and interactive. Increasingly, justice agencies are working together to plan, design, and implement integrated justice information sharing systems. These systems enhance the ability to collect, access, and use information, including personal information, and allow information to be entered once and used across and between many different agency systems.

Developing privacy policies that work throughout an integrated system requires cooperation of each component justice agency. Many public access, public safety, and privacy issues are unsettled and difficult to resolve. This burden becomes even more difficult where agencies with different functions and public mandates are sharing information.

In developing integrated justice system privacy policy, there are two levels of assessment. First, each agency must identify the categories of information sensitivity (Chapter Six) and determine when and where in the justice process this information is shared with other agencies or the public.

Second, the individual privacy and public access policies need to be reconciled, meaning, identifying any disclosure determinations that are contradictory and resolving timing or access problems. Often, this process is best done as part of a formal privacy impact assessment for an integrated justice system. The process for conducting this type of reconciliation is explained in detail in Chapter Seven.

Information exchange between justice agencies is taking place in every state, local, and tribal jurisdiction nationwide. The means of exchange vary from traditional paper transfer to real-time automated information systems. In all these systems, information that is exchanged is related to a justice purpose. Some of the information is administrative, and some is substantive case information. Additionally, some is personally identifiable information and some is not. Different interests are in play in deciding how, when, and with whom this information is shared.

Personally identifiable information exchange

The privacy design principles in Chapter Three provide the basis for developing justice information privacy policy. In developing its privacy policy, each justice agency must take into consideration its justice mandate, whether it receives or creates personally identifiable information, how it creates or receives this information, and how information is disseminated to other agencies within the justice system and beyond. From this overview, an agency can create a statement of privacy goals.

To take a privacy policy from a statement of desired goals to actual working principles requires mapping pieces of information as they flow through an agency or an integrated justice system. Mapping the information flows allows agencies to see what types of information are received or collected, in what context the information is used, whether it is personally identifiable, when, and to whom it is disseminated (see Chapter Seven). These questions are key to determining the privacy implications associated with information in any system. After determining the privacy implications of each piece of information, an agency or integrated system can make deliberate and well-reasoned decisions on whether, or in what context, the information will be shared. These decisions affect interagency exchange, as well as public access to the information.

Nonpersonally identifiable information exchange

Certain interests attach to the interagency exchange of non-personally identifiable information. The interests are not "privacy" interests but rather relate to an agency's public safety or operational mandate. There may be times when sharing general or administrative information within the justice system may compromise public safety. A determination as to sharing this information can be made by mapping the information flows as described above.

Often, the nondisclosure of this type of nonpersonal information is affected by the timing of its release. For example, highly sensitive intelligence information relating to terrorist activities may not be shared by law enforcement with other justice agencies until a critical time has passed; e.g., a suspect is arrested or a terrorist act is subverted. Or, administrative information, such as which law enforcement teams are on alert, may be kept within law enforcement until a threat has dissipated.

Generally, interagency sharing of information is encouraged to support public safety functions of justice agencies. Determinations not to share information should be made with care and should support public safety and the agency's justice mandate.

Determining Rules for Public Access

The American justice system is founded on principles of democracy, where the public's rights are protected by federal and state constitutions and laws and by the ability to participate in or monitor the justice process. Some justice processes allow for more public participation than others. For example, the court process is inherently more open than the law enforcement investigative process. Each justice component, however, has some "public access" method: a means by which the citizenry can avail themselves of the justice process, monitor the actions of the state, or obtain justice information for their own uses.

Public access has been a fundamental part of the American justice system throughout its history. Public access to justice information has always been available, changing in form as technologies allowed. For example, before current technologies, public access methods were limited to requesting information in person or in writing from the justice agency where the information was maintained. Over time, copying technologies allowed for actual documents to be reproduced from the files. Similarly, telephonic access allowed for more timely remote requests.

Information technology advances in the 1990s, however, changed the nature of public access. As the justice system's ability to electronically collect, use, and maintain information increased, so have individual and commercial desires to obtain information quickly and easily. Often termed the "Internet effect," individuals are demanding access to justice information with the same ease and efficiency as they access electronic commercial information.

In response to the public's expectations, justice agencies are employing new access technologies. For example, increased availability of the Internet is allowing individuals to receive justice information from remote locations rather than at the station house, prosecutor's office, courthouse, or jail. On-line information may include notices or process information, such as court dates, telephone numbers, and customer service information that direct people in "how to" access the justice system, as well as more substantive justice information, including crime data, arrests, warrants, and case and criminal history information.

In designing all privacy policies, however, it is important not to limit policies to currently available information technologies, such as the Internet. Today's technologies will give way to better, faster technologies that may change, again, the way we view information access. Developing privacy policy around the public, justice system, and individual interests in justice information will allow justice agencies to be proactive in applying policy to new technologies rather than reacting to their effects.

The importance of public access

The American justice system was created to serve the public. The justice system seeks to monitor other sectors of society, to investigate, and to levy justice. As a public service, it must conduct itself in the public view. The only means of "watching the watchers" is through the public's access to the processes and events within the justice system. This includes statutory rights to access records of day-to-day activity, as well as cases, reports, and decisions affecting individuals involved in the justice

process, and First Amendment and common law rights to access and publicize information about the justice system and individuals involved with it.[40]

Although it is important to maintain public access to as much justice information as possible, personal information or confidential public safety information may need protecting to varying degrees. Therefore, justice agencies must carefully weigh the responsibility for access to the justice process with protection of the personal privacy of those involved in the process. Justice agencies must also balance the need for public information against the need to keep information confidential in support of public safety functions.

There are no bright lines or easy rules to follow in developing policies to address these conflicting issues. The responsibility of justice leaders and practitioners today is to pave the way for the future of privacy and public access policies by upholding the presumption of public access while tempering it with reasoned and deliberate decisions that strive to protect individual privacy interests and enable the daily operation of the justice system.

What interests are present in public access to justice information?

Public access gives rise to specific interests for both the public and justice system agencies. The interests include those related to "access" and "release" of information generally, as well as risks to personal privacy associated with release of personally identifiable information. Constructing an effective privacy policy requires balancing the following, often competing, interests.

- First, the public's interest in monitoring the justice system processes through access to justice information.
- Second, justice agencies' interest associated with its public safety or civil justice functions; for example, "release" interests in releasing appropriate information on request and proactively releasing information when necessary for public safety. Release interests also include ensuring that confidential information necessary to law enforcement (e.g., ongoing investigations) or other justice mandates[41] is not released until it would not impair the agency's public safety or justice function.

---

[40] It is important to note that the First Amendment right to publicize information falls under the First Amendment right to free speech. The First Amendment right of access relates to the public's right to attend criminal trials. This is a "qualified right of access," where the court can deny access if it finds that the government has a compelling interest and the denial of access is narrowly tailored to serve that interest. See *Globe Newspaper Co. v. Superior Court for the County of Norfolk*, 457 U.S. 596, 606 (1982); *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555 (1980). Although the Supreme Court has not extended this qualified right of access to the right to review documents in criminal matters, circuit courts have applied the qualified right of access in this manner. See; e.g., *In re Search Warrant for Secretarial Area Outside Office of Tomas Gunn, McDonald Douglas Corp.,* 855 F.2d 569, 573 (8th Cir. 1988); *Seattle Times Co. v. U.S. Dist. Court,* 845 F.2d 1513, 1515-16 (9th Cir. 1988); *CBS, Inc. v. United States District Court,* 765 F.2d 823 (9th Cir. 1985). Therefore, the limited application of the First Amendment qualified right of access does not extend a constitutional right of public access to all justice information. This right of access to public records, although not absolute, is afforded by a common-law right of access. See *Nixon v. Warner Comm., Inc.*, 435 U.S. 589, 597 (1978). Further rights of public access to justice information at the federal, state, and tribal levels are provided by statute.

[41] In determining disclosure or nondisclosure in case law, this function is referred to as a "compelling government interest."

- Third, individuals' information privacy risks from the inappropriate release and use of personally identifiable justice information.

Who is the public? Simply stated from the justice system perspective, "the public" includes a broad group of people and organizations (individuals, profit and nonprofit entities, and the media) outside the traditional justice system agencies (law enforcement, prosecution, defense, courts, corrections, probation, parole, and victims services). Nontraditional justice agencies, such as social services, health, fire/EMS, and transportation may be public, depending upon the context in which traditional justice agencies are sharing information with them.

What is publicly accessible information? In terms of accessing justice information, there are different levels or classifications of information. Publicly accessible information is the most readily disclosed information in the justice system. There are balancing tests that must be applied by justice agencies and integrated systems in determining public accessibility. The first test relates to balancing the public's "need to know" with an individual's privacy interest in the information. The second test relates to balancing the public's need to know with the justice agency's public safety interest in the information. These interests will be affected by the context in which the information appears, whether it is personally identifiable information, and the time in the justice process at which the information is considered for public access.[42]

As described above, justice information includes administrative and substantive information. Some of this information contains personally identifiable information; some not.

"Nuts and Bolts" issues associated with publicly accessible information

Timing—When does justice information become public? When does it become "unpublic"? As information is collected or created by the justice system, timing becomes an important issue to its public accessibility. For example, arrests made by a police department are published for a certain time relative to the commission of the offense. After that period of time, information about a particular individual's arrest may not be publicly accessible from the police department without a specific request and authorized purpose. At some point in time, the arrest may become part of the official criminal history record and (depending upon jurisdiction) may not be publicly accessible at all. In this case, the same piece of information (name of the individual, description of the crime) has gone from "public" to "unpublic" through the passage of time and via traditional justice system rules.

The scenario applies in the reverse as well. For example, information collected during an investigation is not publicly accessible at that time. The same information, once introduced at trial, becomes part of the publicly accessible court record. If the

[42] For example, the content of a search warrant affidavit may contain personal information about the subject and witnesses, as well as information about investigative leads, law enforcement techniques, and presumptions. Consideration of type, context, and timing in releasing this information is imperative to protecting the privacy interests of the subject, witnesses, and the law enforcement purpose of the government investigation. What might not be appropriate for release precharge, might be appropriate for release after indictment or conviction.

case does not proceed to a resolution in the courts and the investigation is closed, information may then become publicly accessible from the law enforcement or other agency. Therefore, in some instances, timing is everything.

Timing restrictions, or protections, that worked to effectuate access policy in paper-records systems may not work as well in the electronic age. Once information is released in an electronic format, it can be duplicated and widely disseminated with much greater ease than paper records. In addition, it is nearly impossible to assure to whom it is disseminated once it leaves the original source. For example, arrest data that is publicly available over the Internet may be copied and electronically disseminated by an information purveyor. When the police department removes the arrest information notification, the information is still being disseminated to the public through the private source. A year later when the arrest becomes part of the official criminal history record, the purveyor may still disseminate that information—along with other related information the record has attached to it. These changes in how timing affects access to information should be considered in developing public-access policy.

Timing issues are extremely important in dealing with the movement of information within an integrated justice system. It is possible to have the same information be public at a certain agency while remaining nondiscloseable in another agency. For example, information in a nonpublicly accessible official criminal history record may be obtained in similar (if not the same) format from a court or corrections agency information system. In this way, an "unofficial criminal history compilation" is public where the official compilation may not be.

What is the life cycle of the information? In the paper age, justice agencies were required to develop policies for maintaining quantities of paper files. Physical storage limitations dictated that not all documents could be saved forever. In addition, utility of old documents was marginal, as stored documents were not easily retrievable, even with detailed indexing systems. Digital storage capability has changed the way we view volumes of information. Storage capability is practically unlimited, and access, retrieval, and analysis of stored documents is instantaneous. Therefore, document "life cycles" in the information age will be used as part of an access policy rather than implemented as a practical necessity.

Once released, public information is forever public. Downstream use of disseminated information is ultimately beyond control of the disseminating agency. This is true for both paper and electronic information, although the ease and broad dissemination capabilities of electronic information exacerbate this problem. An issue remains as to whether there is utility in the original source maintaining the information indefinitely. If maintained indefinitely, is the information indefinitely publicly accessible from the original source? If records are destroyed, is there a "record" that the deleted record existed? Is this publicly accessible? Agencies must answer these questions according to the goals of their public access policies.

In scenarios dealing with timing or life cycle, the goal is not to determine whether public access, especially electronic information access, is good or bad (it is a reality). As in developing privacy and public access policy itself, it is important that life-cycle statutes or regulations are not tied to currently available technology, as new technologies may change the way we store and access information. The challenge in developing life-cycle rules is to determine the true purpose of information

accessibility and information permanence and to design rules implementing this purpose. Much of this determination centers on the value of the information—to the individual, the justice system, and to the public.

What is the value of the information? Competing interests are at work in determining the "value" of information. Interests lie with the data subject (the individual), the justice system, and the public, including the media and commercial sector. "Value" is basically a personal judgment. However, government policy and technological capability increasingly make this judgment for the individual. It is crucial, therefore, that as justice agencies develop a privacy and public access policy, the value question is carefully considered from all perspectives.

In the justice system context, the value of nonpersonally identifiable information can be assessed by its usefulness in the day-to-day activity of the justice agency. Sensitivity and usefulness of the information in relation to the agency's operations will inform the agency's decision to keep the information, to share it within the justice system, or to release it to the public.

The decisions to share or disclose personally identifiable information adds an additional layer of analysis to the value question. At its most basic level, its value may be judged by answering some questions in a personal context. For example, if the information was about you or a family member, would you want it to be publicly accessible? If the same information was critical to providing safety to you or your family, would you want it publicly accessible?

Additional value judgments are made in the context of oversight and efficiency. For example, what information would you want to access to ensure the constitutional operation of the justice system? What information would you want others to access to ensure that you received due process in the justice system? What information would you disclose in return for your own "convenience" in working with the justice system?

Still other value judgments are made in a commercial context. For example, what is the consumer benefit of broad access to justice information? What is the market for justice information? How should access be treated in various contexts, such as for employment or housing background checks, by the insurance industry or just nosey neighbors?

The core of a privacy and public access policy is developed by reconciling the answers to value questions. Value questions like the ones above, although they may appear simplistic, are difficult to answer in a policy context. As information technology has eliminated some of the latent "paper inconvenience" protections, in some instances, the development of this more difficult policy has come to rest with the technology staff. The disclosure, timing, and life-cycle issues all rest on the basis of value judgments. It is clear that technology is the implementer of policy, not its creator. Therefore, a cooperative effort of legislators, justice leaders, practitioners, and technology staff is needed to address the "value question."

What type of access is available? Today, justice agencies must be prepared to provide public access through a variety of access methods. These include remote electronic access (Internet, dial-in, or satellite computer terminals), electronic access at the justice agency location, telephone access, written requests, and in-person requests. It is important to note that although this *Guideline* focuses on electronic

access to justice information, the privacy and public access issues discussed should be applied to all methods of access. In other words, privacy and public access policy *should not* be designed around limiting access by simply substituting another method of access for electronic access. Policy cannot be "paper" dependant, as justice and government systems are moving toward evermore electronic record keeping. For example, agencies should not develop policies that protect information by limiting its accessibility to only paper files. The privacy analysis must be done on the type of information and the context in which it is used. If it is deemed discloseable, or "publicly accessible," it should be accessible in all forms.

In the public access area, as justice agencies move toward more electronic records systems, there is concern that automation is actually limiting access to some, while granting greater access to others; i.e., those without computers no longer have access through traditional methods. The justice system must take care to maintain principles of openness and accessibility to all individuals. In the near future, this may require justice agencies to maintain paper and telephonic access, as well as to offer electronic access.

What are the fiscal issues associated with privacy and public access?

Justice practitioners agree that developing, implementing, and assessing privacy and public access policy in today's information society results in real costs to justice agencies. Therefore, agencies must combine fiscal support with internal operations that promote privacy policies.

As described above, the planning, design, and implementation of justice information systems is an expensive undertaking for state, local, and tribal governments. Retrofitting information system designs to account for privacy policy only adds to costs and delays operation. Therefore, privacy policies, including the delivery of public access, should be a part of any initial system design document.

Ideally, access to public information would be provided free of charge. Current reality dictates, however, that someone pay for the real costs associated with public access—whether paper, telephonic, or electronic. Jurisdictions cover costs in various ways, including state and local justice appropriations (from the tax base) and user access fees. Whichever method is used to cover costs should incorporate social policy promoting access to the justice system. For example, covering costs through state or local appropriations draws funding from the community at large. The public policy of these jurisdictions dictates that individuals, through their taxes, enable the justice system to provide access to public information to all members of the community.

Fees, on the other hand, pass the costs directly to those individuals or organizations that choose to, or must, access the justice system. Due to the importance of maintaining an open justice system, when setting fees, justice agencies must balance real costs with public policy. Fee structures created to offset costs must take care not to limit public access by becoming unreasonably high. In addition, fee waiver mechanisms must be in place to allow access to the indigent.

What fee (or tax) is too high? Too low? Just right? Fees or taxes should not be guess work. In determining a fiscally and socially sound fee or tax structure to support public access policy, a substantive cost analysis should be undertaken. This analysis may include a review of the following four considerations.

First is a review of actual costs. What are the actual expenses incurred in developing, implementing, upgrading, assessing, and maintaining privacy and public access for the electronic information system, telephonic, or paper access systems? For example, what are the actual staff hours required to operate the utilized system? What is the cost associated with doing a privacy impact assessment or other internal audit? What costs are associated with purchase, upgrade, and maintenance of technology, including computer systems, telephone systems, and duplication technologies (copiers, faxes)? What are the costs associated with equal accessibility, including Americans with Disability Act requirements?

Second is a review of resulting costs. What are the increases/decreases in labor and operating expenses resulting from implementation of electronic public access capabilities? For example, what is the public expectation for agency response to electronic requests? Can current staff meet these expectations?

Has the public demand for access outrun the access capabilities contemplated in the system design? Is the system able to handle access demands and internal operations? Will upgrades be necessary? What follow-up work is generated by electronic public access capabilities, including record clarifications, corrections, and requests for expungement? What extraneous interactions with the public are facilitated by electronic access; for example, technical "help" questions, questions about agency policies and procedures, and general inquiries about the justice system? Will additional staff be required to meet these requests?

What training costs are associated with implementing public access policies? Does training require legal expertise?

Third is a review of indigent access. What costs must be distributed to give effect to public policy guaranteeing access to all? How many requests for fee waivers are anticipated? What is the cost of these waivers to the agency or integrated system?

Finally is a review of profit motives. Is the agency or integrated justice information system seen as a revenue generator by the executive, legislative, or judicial branch? Is profit expected from the system? Is "public access for profit" legally or culturally forbidden in the jurisdiction?

From a public access policy perspective, the goal of the cost analysis is to support public access through determining what access fees are needed to cover actual and resulting costs and to build in a cushion allowing for fee waivers in appropriate instances. Whether profit is a part of this analysis or not is an individual agency or jurisdictional question.

Some justice information systems operate as profit centers for the executive or judicial branch. In some instances, funding for the information system may have been secured by promising future revenues to the state, local, or tribal government. In other instances, agencies and jurisdictions have intentionally declined to make a profit from public access to records. In still other jurisdictions, profits are checked by statutory revenue limits. Agencies need to consider their cultural or legal parameters, requirements, or prohibitions in this area. As with the other parts of a privacy policy, determining fee structures requires input of legislators, criminal justice policymakers, practitioners, and information technology managers.

Privacy impact of a public access to personally identifiable justice information

A public access policy considers implications for providing access to nonpersonally identifiable justice information, as well as personally identifiable information. The question of "privacy" (in addition to confidentiality) applies to personally identifiable information. A public access policy, therefore, must consider the additional privacy issues involved in allowing public access to personally identifiable information.

What is personally identifiable justice information? Simply stated, personally identifiable justice information is information within the justice system that is linked to an individual at the time of release or, through analysis, can be linked to an individual. To be effective, public access policy must consider the privacy implications of access to personally identifiable justice information. Therefore, personally identifiable justice information should undergo a second level of analysis from a public access perspective. It is important to note that publicly accessible personal information may vary according to specific jurisdictional law or policy.

Consider the following examples of publicly accessible, personally identifiable information that may be contained within the justice system:

- **Law enforcement:** police reports, arrests, warrants, personally identifiable or traceable neighborhood/city/county/state crime data and GIS data;[43]
- **Jail:** inmate information, pretrial information (scheduling, release);
- **Prosecution:** indictment/charging document;
- **Court:** pleadings, motions, hearing transcripts, trial exhibits, dispositions, judge/attorney/juror information, bond information, protection orders;
- **Corrections:** inmate information, classification information, gang affiliation;
- **Probation/parole:** term of probation/parole, sex offender status, violent offender status;
- **Victims services:** treatment providers, contact information;
- **Traditional criminal history record information:** some or all compiled information available pursuant to state law; and
- **Justice system employee:** policies, employee evaluations, employment histories, medical evaluations.

As the adage goes, "privacy for me, disclosure for everyone else." Justice leaders, however, must seek to apply privacy policy as fairly as possible.[44] To do so, leaders must be aware of the various types of interactions individuals have with the justice system and how personal information is collected and intended to be used in the justice process.

---

[43] Many law enforcement agencies use geospacial information systems to graphically organize and display crimes to aid crime prevention and officer response. Other justice agencies also use GIS technologies to "map" justice information to aid in information analysis.

[44] Not all players are similarly situated in the justice system. For example, convicted felons may forfeit some information privacy protections by virtue of their convictions. Witnesses and victims may be afforded more privacy protections in comparison.

Whose privacy interests may be affected by public access, and what information is involved? Individuals who may have personal privacy interests affected by justice information systems include victims, witnesses, jurors, law enforcement officers, justice staff, plaintiffs, respondents, attorneys, judges, defendants, offenders, families and associates of these persons, and anyone else who comes in contact with the justice process.[45] The information involved is information about the individuals collected or created in the justice process.

What are the privacy concerns associated with public access to personally identifiable justice information? Today, it is common to hear or read about individuals struggling to reconcile the benefits of information access with the privacy risks associated with participation in an information society. This conflict exists in the justice system as well. Many of the privacy concerns associated with electronic access to justice information parallel those being addressed in the e-commerce context; i.e., the fear that detailed, possibly erroneous, electronic profiles of individuals will be created, bought, and sold on the e-highway to the detriment of the individual. This tension is heightened for individuals' interactions with the criminal justice system for a number of reasons.

For example, in its public safety function, the criminal justice system has the ability to officially deny one's liberty as a result of the information it collects. Involvement with the criminal justice system is usually without notice to or consent from the individual involved.[46] Criminal justice records may contain an individual's most personal, tragic, and embarrassing information. Justice information can result in restraining individual liberties when properly released and accurate and can cause substantial injury to liberties if improperly released or inaccurate. And any involvement with the criminal justice system can bring with it a "stigma," unlike participation in the commercial or social sector.

In the civil justice system, many of the same embarrassing or highly personal information is collected and used in resolving life disputes, such as divorce and child custody, bankruptcy, employment grievances, and landlord/tenant disputes. Although not the same as the criminal justice stigma, improper release of sensitive personal information can have real detrimental effects on individuals' lives.

Therefore, the need to ensure public safety and protect individual privacy lean toward limited public access to personally identifiable information collected and maintained in the justice system. However, despite the high sensitivity of justice information and the uncertain social consequences of new information "access" technologies, the importance of maintaining a public justice system supports the presumption of public access.

---

[45] It is important to note that personal information of some public servants falls outside strictly personal privacy interests, such as public officials' reputations, personal information affecting the performance of public duties, or data interpretation by the public or media.

[46] See the Notice and Consent Principles discussed in the privacy design principles, Chapter Three, supra. The ideas of "notice and consent" that underpin many commercial privacy policies differ in the context of justice information, particularly criminal justice information.

How do the privacy design principles support public access to personally identifiable justice information?

As discussed in Chapter Three, the Organization for Economic Cooperation and Development's Fair Information Practices[47] set forth principles supporting privacy in the collection, use, and disclosure of personal information. Their goals are summarized as follows:

- Limiting the collection and use of personal information for the purposes intended;
- Ensuring information accuracy;
- Establishing security safeguards;
- Being open about the practices and policies regarding personal information;
- Allowing individuals access to their personal information and the ability to have it corrected; and
- Identifying persons accountable for adhering to these principles.

Each of these goals is important to consider in developing policies for public access to justice information and can be implemented through careful attention to recommendations of the eight privacy design principles (Chapter Three). A summary of the public access implications of the privacy design principles is included below. A review of the design principles in their entirety is recommended prior to (and during) the development of a privacy policy, described in Chapter Six.

1. **Purpose specification principle.** The purpose for which personal information is collected and used should be clearly articulated in writing prior to information collection. Part of this purpose statement should address disclosure of personal information to those outside the justice system; i.e., public access.

   For example, an agency's, or integrated system's, statement of purpose may state that personal information collected within its scope of operations may be subject to public disclosure in support of the presumption of public access to the justice system. Such public disclosure is governed by jurisdictional law, regulation, and public access policies of (the agency) or (various agencies).

2. **Collection limitation principle.** It is important for justice agencies to recognize that once information is collected, privacy and public access policy will affect how it is maintained, used, and disseminated within and without the justice system. It is critical that the presumption of public access be considered when determining what to collect at various points in the justice process. In other words, collecting information because "you can" or simply because it is available, without a clear understanding of why the agency requires the information, can result in difficult use and public access policy implementation. Once an agency has collected information, it is responsible for its appropriate downstream use and dissemination.

---

[47] See, http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM#3.

3. **Data quality principle.** As discussed in the data quality principle, information should be as accurate, complete, current, and verified as possible. These information qualities normally assume that an individual knows information has been collected and has some means of accessing the information to ensure its accuracy. Because an individual may not receive notice at the time information is collected by the justice system, agencies should make best efforts to inform the data subject of the release of his or her justice information upon public dissemination of personal information. Individual notification, however, may not be possible or practical for justice agencies, for example, in the release of bulk data records or when records have not been active and do not reflect current contact information.

   An alternative to individual notification may be a general public education and awareness campaign to inform the public at large of the agency's or integrated system's purpose statement—letting the public know personal information may be collected and eventually publicly released. Part of this campaign should inform the public of how to access their own justice information and provide processes for verification or correction.

   The relationship of data quality to privacy and public access is discussed in Chapter Five.

4. **Use limitation principle.** The foundation of the use limitation principle is that information should be used only in conformity with the purpose for which it was collected. As the design principle notes, use limitation is most applicable where information is disseminated to those outside the justice system; i.e., in a public access context. Subsequent use, referred to as "secondary use" or "third-party use," is an area of heated debate.

   Some legitimate secondary use of justice information not for "justice purposes" is inherent in public access to the justice system. The public does not seek information for the same reason justice agencies collected the information. The public (individuals, profit/non-profit entities, media) seeks information to monitor the operation of the justice system and to be informed about their fellow citizens. Both of these uses are legitimate—as in a review of jail inmate lists or court processes and decisions to be sure the justice system is upholding constitutional protections, or a review of a sexual predator database for safety of the community.[48]

   Justice leaders and individual citizens are troubled, however, about other kinds of secondary use, such as commercial use of justice information, especially bulk data sales to information vendors or commercial marketing firms. These issues are discussed in Chapter Five.

5. **Security safeguards principle.** Security safeguards are important to protect all justice information from loss or unauthorized access. When the information is personally identifiable, the risks for unauthorized disclosure are heightened for individuals, as well as the justice agency or integrated system. Increased use of electronic technologies enabling remote public

[48] In many jurisdictions, public policy, through legislation, has dictated that the privacy interests of sexual offenders is outweighed by the community's need to be aware of their criminal history of sexual offenses. In these jurisdictions, public access to this information to "be aware of who lives around you" is deemed a legitimate secondary use of the justice record.

access, such as the Internet, necessitates that justice agencies pay close attention to security. Security breaches can result in information being disseminated that is not intended to be publicly accessible information. Therefore, security is a key component to the implementation of any privacy and public access policy. These issues are discussed in Chapter Five.

6. **Openness principle.** The openness principle maintains that there should be a general policy of openness with respect to the *management* of personal information within the justice system; i.e., how it is collected, kept, and used. Access to management practices of justice agencies, however, may not be appropriate in some instances, such as during an investigation or prosecution. Access in these events would be appropriate following the conclusion of the particular case.

   Access to *substantive information* collected, used, and maintained in a justice agency or integrated system may be governed through the categorization of nondiscloseable, discloseable, and publicly accessible information explained in Chapter Six. The presumption of public access is the foundation upon which reasoned and deliberate decisions are made as to what information may not be public. The openness principle suggests that where information is deemed publicly accessible, the public should be placed on notice that the information exists and provided a "responsible party" contact within the justice agency or integrated system.

7. **Individual participation principle.** The goal of the individual participation principle as used in a public access policy is closely related to the concepts of "notice" and opportunity to review and verify information. As discussed above, notice of collection, use, and dissemination of personal justice information should be provided to the public, whether given individually or as a general statement of policy. This notice is instrumental to the public's opportunity to participate. As discussed below, mitigating risk to the public and risk (liability) to justice agencies calls for mechanisms through which to allow verification and correction of information inaccuracies. This topic is discussed further in Chapter Five.

8. **Accountability principle.** The accountability principle is the final principle that gives effect to all the others. This is true in developing the overall privacy policy or the public access component of a privacy policy. An information steward[49] should be appointed to oversee privacy and public access implications of the information system design. In the public access arena, however, an additional public advocate may be necessary.

   As discussed in the individual participation principle, the public must have a justice-agency or integrated-system contact person to whom requests, complaints, and questions can be directed. Although this public access contact may not be responsible for the implementation of the public access policy itself, he or she should be responsible for day-to-day interaction with the public on privacy issues. Such a contact (or department) is the privacy customer service center for the justice agency or integrated system.

[49] The concept of the "information steward" is discussed in detail in the privacy design principles (principle 8) and in the privacy impact assessment. See Chapters Three and Seven.

Chapter Five:

Public Access Implications of Data Quality, Bulk Data, and Risk

Purpose: to explore the impact of data quality on privacy and public access, to outline opposing views on whether bulk data should be treated differently from individual record data, and to suggest how to minimize risk to the public and justice agencies arising from public access and privacy issues

The preceding chapter highlights general public access concepts, as well as specific issues associated with protecting public safety functions and public access to personally identifiable information. As noted, public access, public safety, and information privacy interests inherent in the release of justice information are integral, yet competing, parts of the agency's or integrated system's public access policy.

Discussed in this chapter are general topics relating to public access policy that may have specific consequences when considered in relation to personally identifiable information.

Impact of Data Quality on Privacy and Public Access

Justice agencies at all levels of government are working to improve the quality of their information; i.e., improving the accuracy and completeness of data. In many cases, due to legacy systems and legacy data, improving data quality is an enormous and expensive undertaking. The justice system is recognizing, however, that fast access to imperfect data may be worse than no electronic access to data at all. The public needs to understand this concept as well. Providing electronic access to inaccurate justice information is not a public service; it is a public and personal injustice. In developing public access policy, it is important that public access desire not outrun an agency's capability to deal effectively with privacy and data quality issues.

Although data quality may not be a traditional privacy issue, it is specifically enumerated in the privacy design principles (principle 3). In practice, the accuracy, completeness, and currency of information connected to an individual raises as many concerns as the release of a type of information itself.

For example, if court dispositions are publicly accessible and searchable, once the record is located, it makes a big difference if "guilty" is listed as the disposition rather than "not guilty." Such an inaccuracy may be caused by releasing incorrectly

entered information, outdated information, or incomplete information. As discussed earlier, once information is released publicly in electronic form, it is not easily controlled or retrievable. Once leaving its source, it often cannot be easily corrected or updated.

There are procedures by which justice agencies can work to improve the quality of their data. A method of assessing and affecting data quality is available through the privacy impact assessment (Chapter Seven). Methods by which justice agencies can respond to individuals' requests for corrections to their information are also addressed in the privacy impact assessment. Paired with data quality, data volume is a public access issue. The pros and cons of releasing data in bulk is discussed under "bulk data" below.

In addition to the accuracy, currency, and completeness of the actual data, the quality of the information is affected by the public's ability to access *meaningful* pieces efficiently. Justice agencies should seek to implement "privacy friendly" information technologies; i.e., technologies that allow for electronic records storage, internal use, and filtering. Although "filtering" information has negative connotations from an openness perspective, filtering out non-pertinent data provides the public with access to desired information. Anyone who has used an Internet browser will appreciate the ability of the technology to filter, categorize, and rank information.

Additionally, from a justice agency or integrated system perspective, implementation of a functional public access policy may require advanced filtering capabilities. Not all justice information will be deemed publicly accessible. Filtering can provide information from records (including documents, data compilations, and multimedia files) that is appropriate under the policy, rather than denying electronic access to the whole record (document, compilation, or multimedia file) as a matter of course. When implementing these technologies, it is important to adhere to the two-dimensional concept of justice information; i.e., accessibility must be determined at a data-element level and within the context of the larger record (document, compilation, multimedia file).

Bulk Data and Public Access Policy

The term "bulk data" is used to describe large amounts of information disseminated at one time from an electronic information system. A colloquial term sometimes used to describe the way bulk data is provided is "data dump." Bulk data, as delivered, may be indexed and organized, sometimes not.

The bulk data discussion relates to release of nonpersonally identifiable justice information and to release of personally identifiable justice information. Generally, the bulk data debate concerning release (or sale) of nonpersonally identifiable information relates to whether the justice system should supply secondary users, specifically commercial users, with a commodity—large quantities of information that can be repackaged and resold. Although an interesting discussion, the issue is one of profit and cost rather than privacy or public safety.

For purpose of this discussion, the *Guideline* focuses on the more challenging debate regarding privacy issues associated with individually identifiable records provided by justice system agencies or integrated systems as bulk data. Also of concern is unidentifiable bulk data that, through analysis, renders individually identifiable information.

The privacy issues associated with bulk data are based in the privacy design principles of purpose specification and use limitation. These principles highlight the need to address possible secondary, or third-party, uses of information collected for a specified justice purpose. At the pinnacle of the bulk data debate is the sale or dissemination of personally identifiable bulk data for commercial purposes.

Differing views on bulk data

Should bulk data be treated differently than individual record data? Viewpoints on this topic vary. One view is that the nature of releasing large amounts of personally identifiable information raises privacy concerns due to the amount of data, the timing in which the data is released, the possibility for compounding inaccuracies, and possible inappropriate secondary use. For purposes of this discussion, this view is referred to as the "bulk data opponent" view.

The other view is that the release of bulk data, itself, has no bearing on privacy issues. Where information is public, the release of one personally identifiable piece of information is no different that the release of a large number of pieces of personally identifiable information. The secondary use of this information is not material, as it has been deemed public, and is, thus, available for use as the public sees fit. For purposes of this discussion, this view is referred to as the "bulk data proponent" view.

Because differing views are strongly held by each group, neither viewpoint is adopted by the authors of this *Guideline*. Both are articulated in the discussion below.

Bulk data opponents. Some groups or individuals have articulated concerns relating to the release of bulk data due to the amount of personal information, the timing in which it is released, and the analysis and secondary use capabilities not contemplated or intended at the time the information was collected. These theories are discussed below.

According to one theory, the release of large quantities of justice information at one time increases the downstream, secondary availability of inaccurate data. As discussed above, once data is electronically released from its source, it is not retrievable or easily corrected. It is common that bulk data released to the public, especially the commercial sector, on any given day remains "as is" for the life of that data in its use by the person or company. The larger problem is created when bulk data is compiled and sold by secondary users.

For example, on January 1, information reseller Company Q receives bulk data of court dispositions from Court R. Court R's records are continually updated, either in "real time" or on a daily basis. Company Q develops an Internet service to sell court dispositions relating to individuals for $19.95. By January 2, Company Q's data is no longer as accurate as when it left Court R. By May 2, Company Q's data may be doing more harm than good from a public-access perspective. Consider a situation where a person's name and identifier (social security number) was erroneously connected to another person's criminal record. This information was sold to Company Q on January 1. Company Q sold it to lots of other people and companies. On January 2, the mistake is corrected at Court R. Company Q and all

the other e-profilers may never know of it, and even if they do, may not be able to correct it. Possible? Yes, all too possible.[50]

One solution to the accuracy problem may be to allow Company Q to get a bulk data transfer on a daily basis, therefore guaranteeing the freshness of the data within 24 hours. However, this continual bulk data transfer concept raises other problems for justice agencies, specifically fiscal and operational issues. At the current time, even the most advanced justice information systems do not allow for continual bulk data transfers without impeding day-to-day system operation.

According to another theory, large quantities of records at one time increases analysis and unintended use possibilities. Data analysis is not detrimental to personal privacy, per se. It can be used beneficially to show, for example, crime trends, treatment effectiveness, and "at-risk" groups, and to support justice planning and budgets. Analysis can have more personal consequences, however, depending upon who is using the information and for what purpose.

For instance, the commercial sector can analyze court or corrections data to determine which heads of households have been incarcerated and use this data to market targeted services or products to the offenders' families, such as security systems, credit cards, and home equity loans. In another example, bulk data could be analyzed to isolate names of victims or family members and do targeted marketing on services or products. Picture a rape victim being inundated by junk mail for stress relievers, women's magazines, counseling, self-defense programs, athletic equipment, and even gun stores. Sound a bit unpalatable? Unfortunately, it is not far from reality.[51]

Inaccuracies from unanticipated manipulation and analysis of bulk information is also problematic. Secondary users are not always mindful of the original purpose for which the information was collected and the "metadata"[52] that supports the information. Such analysis can result in inaccurate conclusions regarding the persons identified in the bulk data.

Bulk data also feeds the development of "information profiles" that are being talked about in the context of e-commerce. Generally, the public is resisting the development of e-profiles on their living habits by commercial organizations. Bulk data available from the justice system can be used to supplement what was personal-choice information with criminal or related justice information.

For example, it may be quite easy for your employer or insurance company to obtain your profile from an electronic information service showing that you shop at a certain discount store, purchase ice cream and bacon every week, have three kids, pay child support for two more, like action movies (especially the violent Rambo kind), smoke, vacation at the lake, bought a fishing boat, and were arrested for possession

---

[50] *See Stolen Identity: Could It Happen to You?* (MSNBC television broadcast, April 18, 2000), http://www.msnbc.com/news/397082.asp, described in Chapter Two. In this case, a man's social security number was mistakenly attached to a convicted felon's record. He lost his job, family, and home before discovering the mistake and having it corrected at the local sheriff's office. The data, having been sold to a private information vendor, was not able to be corrected nationally. The damaging information could reappear at any time.

[51] To avoid this type of use, some states have statutes prohibiting the use of criminal justice records for the solicitation of business. See; e.g., Colorado's Criminal Justice Records Act, Section 22-72-305.5.

[52] Simply stated, metadata is information that describes the pieces of information—or "information about information."

of marijuana 10 years ago. Do you sound like someone who might be a health or employment risk? Does this profile provide an accurate picture about you? Who decides what that picture means in terms of employability or insurability? Even further, commercial information services are used by law enforcement agencies for investigations.[53] The addition of justice information to e-profiles and their use by law enforcement make the discussion even more important in relation to individual rights and liberties.

Bulk data opponents argue that the majority of bulk data use is driven by profit, not responsible use of justice information. Companies can request one piece of information at a time, but the value added by bulk data is in receiving large quantities of information in a single transaction. The sheer speed and ease in which large quantities of information can be released, manipulated, and re-released compounds the inherent dangers in potentially improper secondary uses of justice information.

Bulk data proponents. Bulk data proponents argue that the dangers (highlighted above) of commercial use, faulty analysis, and e-profiling remain a concern, regardless of the release of one justice record (or piece of information) or 10,000 justice records (or pieces of information). Bulk data proponents note that any concerns about bulk data should be focused on inaccuracies in the information, not the bulk release of accurate information. In addition, the accuracy issue is one that bears on the adequacy of the underlying agency or integrated system, not as a privacy issue linked to secondary use of the inaccurate information.

According to one theory, the release of one piece of information is no different from releasing 10,000 pieces of information. In a justice context, where personally identifiable information is deemed publicly accessible, all of it is available to everyone. It makes little difference whether the information is accessed one piece at a time or in large quantities. The effect on an individual's privacy interest from possible inappropriate secondary use is the same. Therefore, the response to the secondary use concern should be to encourage legitimate secondary uses of bulk data, while discouraging illegitimate uses through civil and criminal penalties.

According to another theory, bulk data concerns should be focused on the release of inaccurate data, not on the bulk release of accurate data. The danger in releasing inaccurate data is essentially the same in releasing one piece of faulty data or 10,000 pieces of information, some of which may be inaccurate. The releasing justice agency or integrated system is responsible for correcting and assuring the accuracy of all of its information. Additionally, "staleness" is not a bulk data concern but an accuracy issue that is the responsibility of the justice agency.

The moderates v. the purists. There are various strata of views by bulk data opponents and proponents. Those who have moderate views in each camp suggest that justice agencies should require an explanation of why the bulk data is requested and how it will be used. This requesting process is not intended to limit bulk data releases for purposes consistent with how and why the information was collected

[53] The FBI routinely consults on-line databases to obtain public source information regarding individuals, businesses, and organizations that are subjects of investigations. See, Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation before the Senate Commission on Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, March 24, 1999.

by the justice system, or in a public review purpose. The requesting process is to prevent, to the extent possible, unintended effects from improper commercial, academic, media, or private individual uses of the personally identifiable information.

Bulk data "purists" in each camp, however, find this middle ground completely unworkable. The basis for the disagreement with the middle ground is that the release decision will become a subjective decision left to the whims of the justice agency. Pure bulk data proponents view the requesting process as a mechanism to refuse legitimate requests for bulk data. This is based on the belief that publicly accessible information should be available for any purpose, not to be limited by the releasing agency or integrated system.

Pure bulk data opponents disagree with the requesting procedures for similar reasons, noting that the possibility for misuse remains where applicants are not forthcoming in revealing the true secondary uses for the information. In other words, the proponents say they will be "required to lie" to get bulk data, and the opponents presume that the requesters are lying to get it. Furthermore, neither group trusts the judgment of the justice agency making the bulk data release decision.

Where do we go from here? Currently, many justice agencies and integrated systems leaders are struggling to develop workable bulk data policies. As can be seen from the differing views, the bulk data issue will be difficult to resolve. As a first step, justice agencies should refer to jurisdictional law, regulation, and existing access policies for guidance on this issue. If no specific guidance is available, individual justice policymakers will need to assess the varying bulk data concerns in light of their responsibilities as public servants and the objectives of their privacy policies.

Minimizing Risks to the Public and Justice System

Public access and privacy issues give rise to risks for both the public and justice system agencies. The public's risks are injury from the release of inappropriate justice information, or the inability to access appropriate justice information. From justice agencies' points of view, the risks include inappropriately releasing information, not releasing information on request, or not proactively releasing information necessary for public safety. Any of these situations could result in time-consuming and costly law suits against the justice agency, as the public's remedies are limited in many instances to those available through civil litigation.

Mitigating risks through privacy policy

The best way to minimize agency risk is to implement privacy policy that embodies deliberate and well-reasoned decisions of the justice agency or integrated system. Ideally, such policy will prevent inappropriate access to information and subsequent injury to individuals. It is inevitable, however, that any policy will have its flaws. An agency can take several steps to mitigate its liability when such events take place.

First, it is imperative that any agency with an information system know the meaning of its own data. In other words, an agency must be knowledgeable about the information it collects, uses, shares, and maintains in its systems. It must recognize the level of data accuracy and what may be revealed from analysis of the data. It must be prepared to address whether analysis reflects the true nature of the data. An agency must avoid being surprised by its own information.

Second, agencies must support privacy policy internally through fiscal resources and education and training. Agencies should engage in regular independent reviews through privacy impact assessments and information audits. All agency employees should be trained on how privacy policies work and why they are crucial to agency operation.

Third, agencies can be proactive in dealing with the public. Agencies may want to offer a "help" line where individuals can obtain assistance in accessing their information, find out what the information really means, how to file complaints, and what remedies may be available to them. Agencies may also want to take a proactive position in dealing with the public in the form of "inquiry notification." This concept is similar to that followed by credit-reporting agencies where after a number of requests for an individual's information (record) have been received over a set period of time, the individual receives notice that his or her information has been accessed. This notice would prompt concerned individuals to verify the accuracy of their information and assist the agency in improving the quality of its information.

Finally, agencies can research existing remedies that are alternatives to civil litigation—for example, whether state Freedom of Information policy covers a complaint, or whether the Attorney General's Office has mechanisms to address the complaint. Agencies may want to institute their own administrative procedures for addressing public complaints. For example, individuals with complaints about accuracy of their information (record) may simply wish to have a forum in which their complaint can be heard, a determination on a correction rendered, and some nominal restitution made. In these forums, individuals and the agencies get timely results at much reduced cost to both parties.

Minimizing risks through privacy- and security-enhancing technologies

Privacy is often associated with security. While these terms are interrelated, it is very important to remember that these are separate concepts.[54] An information security policy is not a substitute for a privacy policy; it is an important component of the overall privacy plan.

Security policy can mitigate the risks that sensitive data will be accessed by unauthorized individuals and assure that valuable information systems are protected. Information security has become of growing public concern as more and more information about individuals is available electronically. Although personal information may be properly accessible electronically, its wide availability may invite attacks to gain access to nondiscloseable data held in these systems. For example, there has always been a lingering fear that hackers might enter protected government systems and download confidential information, such as criminal intelligence data. In addition, a growing phenomenon has emerged where identity thieves use the Internet to steal information about private citizens from financial institutions, online stores, and even from the home computers of the victims themselves in order to commit crimes.

Various types of security devices are required to promote authorized access and to prevent unwarranted access in paper and electronic information systems. There

[54] See Chapter Two for a discussion of privacy, confidentiality, and security.

are human-driven security devices, such as biometric devices,[55] IDs, or passwords that log or facilitate access to sensitive data or to physical facilities, and there are system-driven security components, such as computer hardware and software. Obviously, justice agencies maintaining paper-records systems will focus on human-driven security and security of physical space. As justice agencies move to predominantly electronic systems, however, effective security policies must take into consideration system-driven as well as human security components. For purposes of this discussion, the *Guideline* focuses on system-driven security components intended to protect electronic justice information.

From a computer hardware perspective, security components such as routers, hardware firewalls and secure network channel technology are all very common ways to monitor who has access to systems and data, as well to create a secure shell around the host system. Routers act as selective access points for packet data,[56] using certain protocols, to enter the system. Hardware firewalls,[57] act as barriers to the world outside the system. Hardware firewalls are normally programmable and are useful in screening user-access at point of entry from a network/Internet connection.

Secure network channel technology is now beginning to take hold in both the military and justice communities. This technology involves adding a platform[58] or platforms at the entrance point(s) between secure and nonsecure networks. The intermediate platform acts a screening mechanism, or sentry, for accessing the secure network, by encoding data transmitted through it. The sentry also eliminates the ability for a hostile user to log directly into the server on the secure side of the channel from the nonsecure side. All transactions must go through the network channel sentry. The successful use of this technology facilitates the movement of data between such networks where, in the past, they would have had to physically swap tapes or data drives.

From a software perspective, there are many more means for making data secure and maintaining privacy. At the heart of these software protections is the notion that encryption technology is a very good way to protect data and should be used actively. Examples of such software solutions are:

---

[55] These devices usually scan voice-print, fingerprint, or retina patterns to allow physical access. New advances in this technology, such as the use of face-scanning technology and infrared temperature imaging technologies are all in their relative infancy but may become quite commonplace in the near future.

[56] Packet data means: Data (whatever it might be) is translated so that it can be sent in evenly-sized hunks (packets) by FTP (File Transfer Protocol), from machine-to-machine or network-to-network.

[57] A hardware firewall is an external unit that the network connection passes through. The purpose of adding this hardware is to intercept hostile traffic from hostile places before such things get too far into the network. It acts as a sentry, much like a router does, and tries to determine if an unknown person is trying to enter the network from an unauthorized location or user-ID. Routers usually search for strange traffic coming from unauthorized machines outside the network, whereas a firewall is a little more complex and is actually trying to look at what data is arriving and from whom it is coming. The difference between a hardware firewall and a software firewall is that the hardware version intercepts bad traffic from bad places before it gets to the server and the rest of the network. A software firewall intercepts bad traffic once it reaches the server or individual machines. Software firewalls are primarily used by home office users and smaller companies who cannot, or choose not to, afford the hardware firewall.

[58] "Platform" is another way of saying computer. A platform can be a PC, server, or a mainframe, or anything in between. The terms computer, platform, or machine can be used interchangeably to describe the same thing.

- **Software firewalls.** Protects a system or individual computer from being attacked by an outside source through limiting the access to identified sources.
- **Anonymous browsers.** Internet entry point designed to mask the identity of the user from the Web sites visited. Prevents information gathering by refusing to accept or send "cookies" from such sites. "Cookies" contain information about individual computers which could hold identifying information about the user.
- **Secure socket layer technology.** Encrypts communication and authenticates connectivity between two devices.
- **E-mail shredding products.** Permanently dispose of retrieved e-mail.
- **HTML filters.** Block advertisements from being displayed and stop unwanted cookies from being placed or retrieved on a computer.
- **Web encryption.** Works similarly to secure socket-layer technology, encrypting data passed between platforms.
- **Disk encryption.** Encrypts the contents of a hard drive, preventing the contents from being accessed and read.
- **Disk file erasing programs.** Clean up hard drive space, leaving no trail of the previous contents.
- **Private key infrastructure.** A conglomeration of encryption, authentication, certificate authorities, and policy tools designed to secure a specific set of linked platforms.

The evolution of security technology has no doubt enhanced the ability to protect data from unauthorized access or public disclosure. This technology, although its purpose seems to be to keep data "in," has allowed greater levels of appropriate public access than ever before. For example, early in this information age, many pieces of justice information that were normally accessible by going to a physical location, such as a courthouse, became obtainable via the Internet without any thought to privacy or security implications.

Only recently have security access controls[59] been placed on some information to afford desired privacy protections. Security access controls are critical to the implementation of a successful privacy policy. Security is addressed in the privacy design principles (principle 5) in Chapter Three and as a critical component of the privacy impact assessment in Chapter Seven.

[59] These security access controls include requiring users to create access accounts identifying themselves to the host computer and forcing user information requests to come through router/firewall access points.

Section III

Drafting Privacy Policy

Chapter Six:

Privacy Policy Drafting Template

Purpose: to provide analysis tools for agency and integrated justice systems, including templates for mapping data flows, determining data sensitivity, and developing a privacy and public access policy

Drafting privacy policy is a two-stage process, which presumes that each of the privacy design principles (Chapter Three) has been carefully considered. Stage 1 involves analyzing each data element (such as a person's name, address, or income). This stage consists of three major components, as noted immediately below. Stage 2 is use of a drafting template, designed to assist agencies in developing privacy policies applicable both to interagency information sharing and to public access to justice data.

Data Element Analysis

The first stage in drafting privacy policy is analysis of data elements (i.e., pieces of information). Such an analysis, in turn, involves mapping information flow, determining attributes of data elements (e.g., their disclosure-related sensitivity), and establishing a privacy baseline or presumption.

Mapping the information flow

Mapping the information flow is a way to identify decision points relating to information collection, use, and dissemination within an agency or an integrated justice system. In many cases, this type of information flow-mapping has already been completed by system developers, albeit not from a privacy perspective. To assess privacy implications, the only addition to this previous mapping process is analyzing what is done regarding information privacy at each of the information exchange points; i.e., the collection, access, use, and disclosure of personal information.

The information flow map is a tool to go beyond the privacy design principles and "drill down" into the information flow in an agency or integrated justice system. This type of analysis is necessary to completing this chapter's privacy policy template and Chapter Seven's privacy impact assessment.

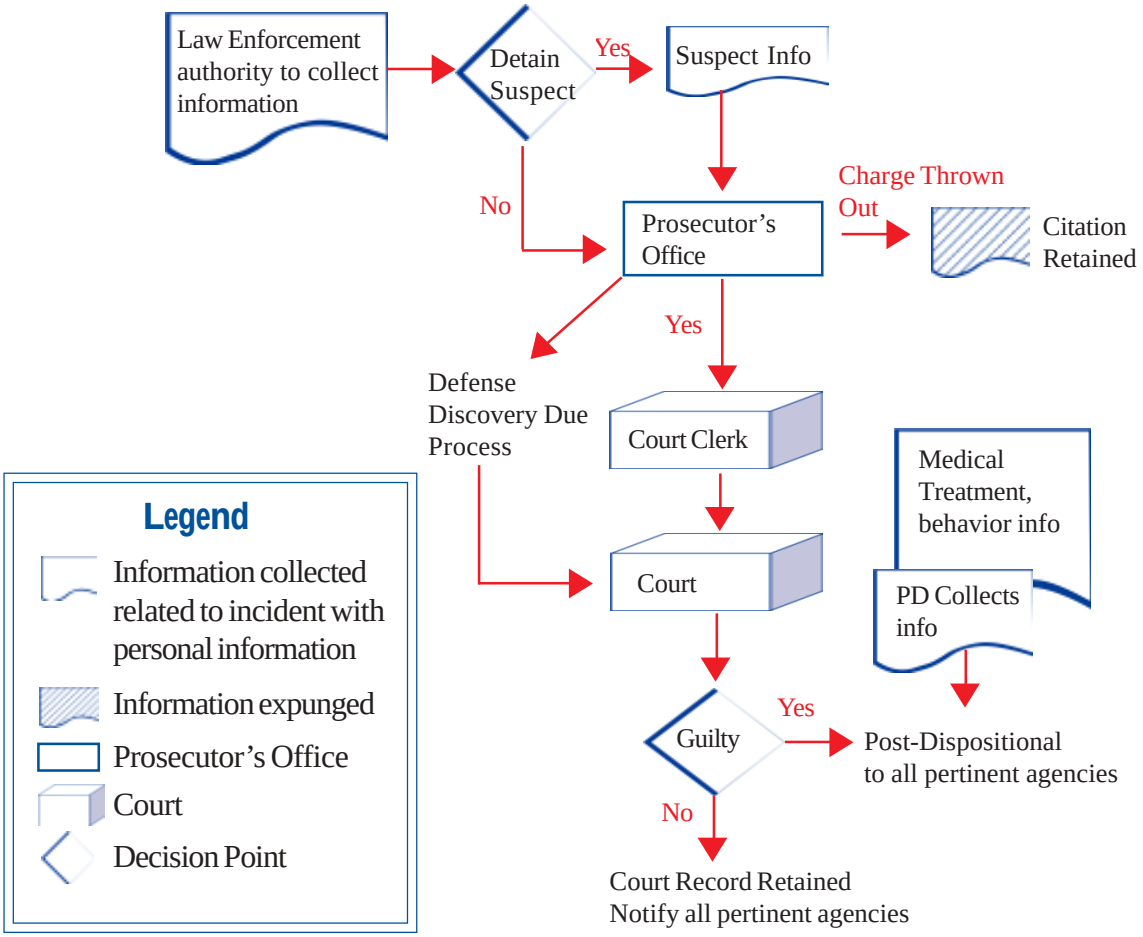
The accompanying example data flow diagram (Figure 1) indicates the first step in mapping the collection, use, and disclosure decision points of information flows in a traditional criminal justice system context. Please note that this is only one example of a data flow model. Agencies and the flow of information may differ from

jurisdiction to jurisdiction. Information flows of alternative justice processes, including prevention and diversion programs, should be mapped in a similar fashion.

Mapping the information flow will also highlight the decision points where the original information entered might change in the justice process. For example, an initial charge might be made by law enforcement, then changed by the prosecutor, and finally disposed of in court by a plea to another offense. Ensuring integrity (accuracy) of the information within the various agency databases of an integrated justice system provides the foundation for responsibly using and disclosing personal information.

Once an information flow model is created for an agency system or an interagency information exchange, the model can be reused. For example, an information flow model for the criminal justice system may need only a few changes to be applicable to the same players in a juvenile justice system. The introduction of social services interacting with the court or the prosecutor's office and the particulars of the post-disposition organizations would be the key changes. The rest of the model could be kept. However, the *attributes of the pieces of information* regarding the conditions of use and disclosure of personal information *would differ significantly*. Therefore, close attention must be paid to determining the attributes of the information in different justice system contexts.

Figure 1



Determining the attributes—red, yellow, and green information

At each mapped decision point, "attributes" of each "piece of information" (i.e., data element, such as a person's income) must be determined. The attributes refer to the nature or sensitivity of the information that is being disclosed and the conditions placed on the information regarding its collection, use, dissemination, retention, and expungement. Where attributes have not already been defined, policy decision makers in each justice agency or integrated system should determine the attributes for each data element as to its use and disclosure; i.e., who can access the information, as well as when it can be accessed.

For example, a witness statement contains certain header information (the physical characteristics that surround the witness statement, witness name, address). At an appropriate time in the justice process, the header information and content can be disclosed to the accused. The disclosure of this information, however, is dependent on timing in the justice process. Such information would not be disclosed precharge. It might be disclosed during pretrial discovery. It would be disclosed at the time of trial. Some or all of the information may be publicly accessible after trial.

To help determine how and when information is used, and with whom the information may be disclosed, it may be useful to group "similarly sensitive" information in various categories. For illustrative purposes, we will use a traffic light metaphor:

- **Red-light information:** not disclosed or only disclosed under extreme circumstances.
- **Yellow-light information:** disclosed, but with caution and after full consideration of the consequences.
- **Green-light information:** routinely disclosed.

Nondiscloseable (red) information is generally not disseminated outside the holding agency or is disseminated within the justice system under strict conditions or in very limited circumstances. Examples of nondiscloseable information may be court-sealed records, criminal intelligence information, and information in ongoing investigations.

Discloseable (yellow) information is not always available to other agencies or the public but may be released upon a balancing of justice agency interests or on agency review of a specific request for an authorized purpose, such as an individual's request to see his or her own information or a nonjustice organization's or individual's request for an authorized purpose. Examples include personally identifiable justice record information between agencies or public requests for criminal records checks for noncriminal justice purposes (i.e., employment background checks), juvenile records requests, and criminal history information (where permitted by state law).

Publicly accessible (green) information is by law or tradition available to justice agencies or people or organizations upon general request. Some publicly available information is related to the justice process. For example, crime statistics, agency operational data, or public service announcements. Other publicly accessible information is "substantive," relating to people, cases, and events, such as the "justice record." Even though green information is the most freely accessible justice

information, its disclosure should still be weighed against individual privacy interests and public safety interests.[60]

These classifications should be applied to each piece of information as it is collected, used by agencies, and disclosed throughout the justice system, as well as when information is considered for disclosure *outside* the justice system; e.g., between law enforcement and educational agencies, or the courts and the public.

For example, consider a data element such as the income of an arrestee. The information flow map(s) would help identify to whom that information would be disclosed within the justice system, and if, where, and when it could be disclosed to the public. The following series of questions are designed to assess the data element attribute (sensitivity). In answering each of the queries, it is important to consider the type of information (what is it), its context, and when it will be shared (when, or at what point, in the justice process might the holder of the information contemplate its release to another agency or the public).

1. Is the data element personally identifiable information? If no, go to #5. If yes, go to #2.
2. Do the interests of public disclosure outweigh the agency's interest in nondisclosure? If yes, the information is discloseable within the justice system (yellow). To determine public access, go to #4. If no, go to #3.
3. Do the interests of the receiving agency outweigh the giving agency's interest in nondisclosure? If yes, the information is discloseable within the justice system (yellow). To determine public access, go to #4. If no, the information is not disclosed (red).
4. Do the privacy interests of the individual outweigh the public's interest in disclosure? If yes, then the information is not publicly disclosed. If no, then go to #6.
5. Does the interest of public safety outweigh a justice agency's interest in interagency disclosure? If yes, the information is not disclosed (red). If no, go to #6.
6. Does the interest of public safety or an agency's justice mandate outweigh the public's interest in disclosure? If yes, the information is not publicly disclosed. If no, the information is publicly disclosed (green).

In the above example, presume that the analysis finds that the arrestee's income is discloseable within the justice system but not publicly accessible. In determining exactly how the income of the arrestee is disclosed within the justice system, policymakers must also determine who should have access to this piece of information within the receiving agency. For example, a disclosure rule could be that personal financial information is restricted to access by pretrial personnel and judges to determine applicability for indigent defense services, but not accessible by other court staff. In this case, after assessing the "receiving agency's interest" and determining that disclosure is appropriate to the court, additional conditions are attached to the data element, limiting disclosure within that agency. Before the court passes on the information, it would do the same analysis, determining type,

[60] See Chapters Four and Five for a full discussion of balancing these interests.

context, and timing as it relates to the income of the arrestee (who is now possibly a defendant) before it is shared.

Very careful data analysis must be done with regard to public disclosure of information. For example, another piece of "yellow" information may be the name, birth date, sex, and race of the individual. Within the justice system, these pieces of information are ordinarily standard identifiers and probably would be shared agency to agency. However, in determining public access, they must be considered in the context in which they appear. After the balancing test in inquiry number 2 above, it may be determined that these identifiers are not routinely released to the public in their context.[61] Therefore, although they might be routinely shared within the justice system, they are not always shared with the public.

Even when an agency determines that such information can be released to the public, one final test must be applied: Will the release impede a public safety or other justice function? The balancing of public, justice, and individual interests is discussed in detail in Chapters Four and Five.

Establishing a baseline

Often, a preferred default policy of privacy practitioners is the presumption of nondisclosure for all information unless certain conditions are met. This applies the most protective privacy policy, the "red light" attribute, to all information, allowing certain pieces to be released only if disclosure conditions are met.

In many jurisdictions, the presumption baseline is for public access. This approach allows disclosure of all data, unless tagged to indicate that release requires a higher dissemination threshold. This applies the "green light" attribute to all information, allowing nondisclosure of certain identified pieces or types of information.

Pursuant to the First Amendment, the preferred presumption is public access. Various state statutes and regulations may contravene this position relating to justice information. Therefore, jurisdictions and agencies must determine for themselves which approach provides workable, appropriate privacy protection, while allowing for system functionality.

Drafting a Privacy Policy Through Use of the Template

As noted previously, a justice information privacy policy should consider information exchanges between traditional justice system agencies, as well as with the public (including nontraditional justice agencies, individuals, and the media).

When an agency or integrated system is ready to begin using the privacy policy template, it should have a general idea of its overall privacy policy objectives. Therefore, at this time, the policy drafters have considered each of the privacy design principles (Chapter Three). They have determined what information is collected, maintained, and they have mapped the data flow within their agency or within an integrated justice system. They recognize that some of the information

[61] See the template in Chapter Six for assistance on developing public access policy for these types of disclosures.

will not be nondiscloseable (red), some will be subject to limited disclosure (yellow), and some will be publicly accessible (green).

The discussions above focus on issues and factors that should be considered when answering template questions. The purpose of the template is to assist in developing a complete privacy policy that accounts for interagency information sharing, as well as public access to justice information. The template questions develop the general scope and goal of the policy, identify classifications of information for interagency sharing, and determine public access to justice information generally, with specific questions relating to public access to personally identifiable information.

The template is intended for general use by a variety of justice agencies. Theoretical policy examples are given from various justice agency viewpoints, and some actual policies are quoted, but each section does not address every justice viewpoint. *(Similar issues relate to public access to proprietary commercial or association information. It is the position of the drafters of the Guideline that commercial interests have sufficient remedies to protect trade secrets, such as requesting that certain court information be sealed, or filing suit for damages. Therefore, a detailed discussion of these issues does not appear in the template.)*

The theoretical and actual examples are not intended to be "recommended" language for users of this *Guideline*. Practitioners are urged to use these examples to guide the development of their own privacy policies and to carefully consider limitations or opportunities for interagency information sharing or public access depending upon the nature of their justice mandate. Practitioners are encouraged to start with a "presumption of disclosure" and consider specific conditions and consequences that may limit interagency sharing or public access to their system information.

The policy design template below, consisting of Parts A – F, is intended to help justice leaders and managers to articulate the goals of an agency's or integrated system's privacy policy; identify with whom they share information, including their "public"; determine what information is nondiscloseable, discloseable, and publicly accessible; and decide the way in which information will be delivered to other justice agencies and the public.

Template Part A: Developing a purpose statement

The purpose statement is a broad statement of principles describing the balance of the justice agency mandate, the need for information sharing, the privacy interests the agency seeks to protect, and the need for public access.

1. What is the purpose of your information system?
2. Do your information collection practices mirror your system's purpose?
3. What are you trying to achieve through interagency information sharing?
4. What are you trying to achieve through public access?
5. Are there limits to interagency sharing or public access provided by jurisdictional laws or guidelines?
6. Is interagency sharing or public access to certain information required by jurisdictional laws or guidelines?
7. How does this privacy policy serve to reconcile any competing interests?

The following is a hypothetical example of a court-related goals statement:

(a) Statement of Interagency Information Sharing Policy. [Example Court A] receives, collects, uses, maintains, and disseminates information relating to criminal and civil actions within its jurisdiction. This information may be personally identifiable. The information is received, collected, used, maintained, and disseminated by [Example Court A] for the purpose of processing judicial actions. [Example Court A] may not disseminate information to another justice system agency for a purpose other than a legitimate justice system function. Certain information is provided to the public, pursuant to the public access policy in (b) below.

The following example goals statement is actual policy as expressed in Idaho Court Administrative Rules, Rule 32:[62]

(b) Statement of Public Access Policy. The public has a right to examine, inspect and copy the judicial department's declaration of law and public policy and to examine, inspect and copy the records of all proceedings open to the public. However, certain kinds of detailed factual inquiries (particularly those involving children, or whose disclosure might endanger or lead to the harassment, embarrassment or humiliation of innocents) have traditionally been exempt from disclosure to the public and will continue to be. This rule reconciles these competing policies by providing for the public's access to the former records while categorically preserving the confidentiality of certain kinds of proceedings; it further recognizes that in cases ordinarily open to the public there may nevertheless be instances in which the disclosure of certain records would endanger innocents, invade privacy, defame, humiliate or ridicule innocent individuals, disclose proprietary business records or trade secrets, or otherwise inappropriately make public certain private facts. This rule provides for exemption from disclosures in certain categories of cases and preserves the court's flexibility to make appropriate exceptions from disclosure in other circumstances.

Template Part B: Determining the scope of your policy

The scope of the privacy policy sets out the framework of interests to be protected under the goals statement and how the policy will be enforced.

1. Who, what, where, when? Who is requesting? What is the type of information being requested? Where is the request coming from—another justice agency? The public? Is it electronic, written, in person? When in the justice process is the request made? Does the timing of the request change the classification of the information (red, yellow, green)?

2. Who is responsible for the policy? Which individual or group of individuals is responsible for drafting the policy? Which individual or group of individuals oversees the administration of the privacy policy? Is there an individual or group of individuals assigned to administer the public access portion of the policy?

[62] This example is drawn from Lawrence P. Webster, "Caught in Converging Technologies: The Modern Court Administrator and the Privacy/Access/Security Conundrum," faculty article, Sixth National Court Technology Conference (CTC6), Sept. 1999.

3. What is the process for modifying/enforcing policy? What is the method to protest operation of the policy (complaint mechanism) for other justice agencies? For the public?

The following is a hypothetical example of a scope-of-policy statement for a law enforcement agency:

This policy applies to all requests for information maintained by the [Example Police Department], including statistical data derived therefrom. This policy also applies to the design and operation of any interagency information sharing system. This policy applies to case information, as well as administrative and internal business process information of the [Example Police Department].

This policy contains provisions for public access. These provisions apply to all personal, written, or electronic requests to access or obtain copies of any paper documents, audiotape, videotape, microfilm, computer or electronic-based record maintained by the [Example Police Department], except for requests initiated by authorized justice agency personnel.[63]

This policy is administered by the [Information Steward] for [Example Police Department]. Public access policies are administered by the Privacy Ombudsman located in the Office of the Information Steward. Any questions or concerns regarding requests for information should be directed to this office.

The scope-of-policy statement of the Washington State Courts follows:[64]

I. Authority and Scope

A. These policies govern the release of information in the Judicial Information System (JIS) and are promulgated by the JIS Committee, pursuant to JISCR 12 and 15(d). They apply to all requests for computer-based court information subject to JISCR 15.

1. These policies are to be administered in the context of the requirement of Article I, §10 of the Constitution of the State of Washington that "Justice in all cases shall be administered openly and without unnecessary delay," as well as the privacy protections of Article I, §7.

2. These policies do not apply to requests initiated by or with the consent of the Administrator for the Courts for the purpose of answering a request vital to the internal business of the courts. See JISCR 15(a).

Template Part C: Determining how information is verified, maintained, and corrected

The verification and correction statement describes how the agency or integrated system ensures data quality. Data quality is an important aspect of privacy and public access policy. As described in the privacy design principles, privacy protections include allowing for verification and correction of individuals' information. This may

[63] Authorized justice agency personnel includes law enforcement officers, prosecutors, defense counsel, court personnel, and pretrial, probation, and parole officers operating as in their daily justice system capacities, and other organizations specifically designated by [Example Police Department].

[64] See the entire Washington State Courts data dissemination policy in Appendix D or at www.courts.wa.gov/datadis/policy.cfm.

be done through internal cross-referencing or through individual or proxy access to the information. Data quality is integral to public access policy by ensuring that information released to the public is accurate, complete, and up-to-date.

1. What methods are in place to assure data quality?
2. Does the system perform internal verification of data?
3. Does the system allow an individual to access his/her personal information?
4. Does the system provide a correction process? What is the standard for determining accuracy of data? What is the standard for allowing data modification?
5. Does the system require other information sources (agencies) to guarantee the quality of their data?
6. In an integrated system, who is ultimately responsible for data quality? The collecting agency? The receiving agency? The distributing agency?

The following is a hypothetical example of a data quality statement for a probation department:

[Example Probation Department] receives information from a variety of sources, including [clients, X court, prosecutor's office, defense counsel, law enforcement agency]. [Example Probation Department] strives to provide accurate, current, and verified information to other justice agencies and the public.

Information received by [Example Probation Department] from individuals and other government agencies is cross-referenced and verified to the best possible extent by [Example Probation Department] staff. Access to individual information may be provided pursuant to the access statement below. Data errors or inaccuracies are flagged in the system, and an information correction evaluation is conducted within 24 hours of detection. The correction evaluation is performed by the Office of the Information Steward (data management section) according to stated procedures. No information flagged as possibly erroneous is disseminated by [Example Probation Department] until the error is resolved.

Template Part D: Deciding who gets access

The access statement identifies the classification of information and which justice agencies have access to the information. The access statement also identifies who may gain access to information under the "publicly accessible" category. A number of privacy design principles should be considered in constructing this section of the policy. For example, the use limitation principle, the security principle, the openness principle, and the individual participation principle.

1. Who are your justice partners? From whom do you receive information? To whom do you give information?
2. Who is your public—individuals, private industry, media, scientific and academic organizations, and other government agencies?

The following is a hypothetical example of an access statement for an integrated justice system:

This policy governs dissemination of information to justice system agencies in [jurisdiction Y] [agencies x,y,z,...]. This policy also governs individual, for-profit and nonprofit corporate, media, scientific and academic, and nonjustice government agency requests for information. Information maintained by [Example Corrections Agency] is provided to [Example Court A] pursuant to state law. Information maintained by [Example Corrections Agency] is accessible to the public by request, subject to the limitations set forth below.

Template Part E: Deciding what information can be accessed by whom

The information access statement describes types of information, if and when it is disseminated within the justice system, and if and when it becomes publicly accessible. An access statement balances justice, individual, and public interests. The balancing of interest requires a detailed look at the "who, what, where, and when," described in Template Part B above.

Different levels of access must be addressed for information sharing within the justice system and with the public. For example, when an agency determines that it will release information to another justice agency, some of the information may be personally identifiable, some may not. In a privacy context, the personally identifiable information requires additional analysis to determine whether access should be restricted at the receiving agency. If so, the receiving agency should establish access protocols limiting access to personally identifiable information as appropriate. For example, a jail record may contain a defendant's HIV status. When the jail shares the custody record with pretrial services (part of the court system), the court's system may limit access to only the pretrial services officer and close that data as to general access by the clerk's office.

Similarly, a public access policy balances the public's need to know with the justice system's public safety interest. In a privacy context, additional analysis should be done with respect to personally identifiable information: for example, a public access policy may release all court proceedings. Within the court proceeding information, however, specific pieces of personally identifiable information may be redacted under the policy, such as victims' names and addresses.

1. What information does your agency have, in broad, general terms (i.e., administrative, justice record)? In what form is information available (electronic, paper, or both)? Does this information contain personally identifiable information?

2. Are there jurisdictionally specific laws, regulations, or existing policies that set out limits or requirements for interagency sharing of the information? If so, what are they? Are there jurisdictionally specific laws, regulations, or existing policies that set out limits or requirements for public access to justice information? If so, what are they?

3. What information has been shared with other justice agencies traditionally? Does this include personally identifiable information? What information are you

currently releasing to other justice agencies that is in paper format? In electronic format? Does this information contain personally identifiable information?

4. What information has been released to the public traditionally? Does this include personally identifiable information? What information are you currently releasing to the public that is in paper format? In electronic format? Does this information contain personally identifiable information?

5. Are you releasing information in bulk to the public? Does this information contain personally identifiable information?

The following questions pertain to interagency information sharing.

6. Applying jurisdictional law, regulation, and the presumption of disclosure, is there information that your agency does not share with other justice system agencies? Why?

    - Is there potential for significantly impeding a justice or public safety function of your agency if other agencies have access to this justice information? If there is potential for significantly impeding a function, is the information discloseable (limited access) or nondiscloseable? Is timing of the release determinative of the accessibility of this information (e.g., investigative information, search warrants, court records)?[65]

    - Does your system contain personally identifiable information about victims, witnesses, jurors, juveniles, domestic relations matters, medical records, tax or financial records, subject's relatives or associates, or justice system employees?

    - Have you considered whether any of the foregoing types of personally identifiable information in the context in which it appears may or may not be shared with other justice agencies? Is there a potential for individual harm in sharing the personally identifiable information? Is the use of the information in other justice agencies consistent with the purpose for which your agency received or collected the information?

7. If there is potential for individual harm, is there a way to mitigate potential harm through use and subsequent dissemination limitations? If there is potential for individual harm, are portions of records (documents, multimedia files) discloseable after performing redaction/extraction or filtering?

8. Does your agency actually do redaction/extraction or filtering? If so, how? Are redaction/extraction or filtering processes built into your information system (whether manual or electronic)?

9. Are there real costs in implementing privacy protection considerations for interagency sharing? Are the data protections requested in existence, or will they need to be designed and implemented? Is there potential for substantially disrupting internal agency processes in providing the privacy protections? Can this be mitigated? Can your agency make interagency sharing technically and culturally compliant with privacy laws, rules, and policy? How?

---

[65] For example, information in an ongoing investigative file may not be shared by non-law enforcement agencies if requested during the investigation. Upon completion of the investigation; i.e., when access will not impede a significant law enforcement purpose, the information may become accessible by other justice agencies.

The following queries pertain to public access.

10. Applying jurisdictional law, regulation, and the presumption of public access, is part of your justice information not publicly accessible?

    - Is there potential for significantly impeding a justice or public safety function of your agency by public access to this justice information? If there is potential for significantly impeding a function, is the information discloseable (limited access) or nondiscloseable? Is timing of the request determinative of the accessibility of the information (e.g., investigative information, search warrants, court records)? For example, information about an ongoing investigative file may not be publicly accessible if requested at that time. Upon completion of the investigation; i.e., when access will not impede a significant law enforcement purpose, the information may become publicly accessible.
    - Does your system contain personally identifiable information about victims, witnesses, jurors, juveniles, domestic relations matters, medical records, tax or financial records, subject's relatives or associates, or justice system employees?
    - Have you considered whether any of the foregoing types of personally identifiable information in the context in which it appears may or may not be publicly accessible? Is there a potential for individual harm in publicly releasing the personally identifiable information? If there is potential individual harm, does the need to support public access to the justice system outweigh the potential harm? If there is a need for public access, is there potential to significantly impede an agency's public safety function by releasing the information? If personally identifiable information is not publicly accessible, is it discloseable (limited access) or nondiscloseable?

11. Are portions of records (documents, multimedia files) publicly accessible by performing redaction/extraction or filtering?

12. Does your agency actually do redaction/extraction or filtering for public access? If so, how? Are redaction/extraction or filtering processes built into your information system (whether manual or electronic)?

13. Are there real costs in providing the publicly accessible information? Is the data format requested in existence, or will it need to be prepared? Is this a recurring request—similar to others submitted in the past? Is the request an intention to harass or interfere with agency operations? Is there potential for substantially disrupting internal agency processes in providing the information? If your agency encounters difficulty in providing public access, can your agency make accessibility technically and culturally compliant with public access laws, rules, and policy? How?

Below is a hypothetical example of an information access statement for a corrections agency:

[Example Corrections Agency] maintains information relating to the operation of the agency and inmates and cases under its jurisdiction. Inmate and case information maintained by this agency is shared with [specific justice agencies]

pursuant to an agreed purpose for collection and consistent use of the information.

Information is publicly available upon request, subject to the following exclusions: information that would endanger innocents–defame, humiliate or ridicule innocent individuals, disclose proprietary business records or trade secrets, or otherwise inappropriately make public certain private facts; medical or psychological records of inmates; information regarding personal affairs or medical records of [Correction Agency] employees; information protected as nondiscloseable by law or regulation, or as directed by a court; information that may impede a public safety function of this agency if released, either due to content or timing of release.

Information requested by a member of the public in bulk is subject to bulk data disclosure policies of this [Agency] [jurisdiction]. According to these policies, this [Agency][jurisdiction] requires that an individual or organization making a bulk data request submit the purpose for which the information is requested; a statement describing the intended secondary use of the information (if no secondary use is contemplated, so state); and a statement of indemnity (a form provided) releasing the [Agency] from liability for secondary use disclosures or inaccuracies.

See Appendix D for the access statement of Washington State Courts.

Template Part F: Deciding the method of access

The method-of-access statement describes the ways in which other agencies or the public can request and receive justice information. The development of this statement should be carefully tailored to account for existing agency access capabilities and resources. The method-of-access statement should not be used to "implement" privacy policy—i.e., by providing *de facto* protections in offering only paper-records access where electronic access is available. Rather, the statement should reflect the agency's best attempt to deliver "yellow or green" information to other justice agencies and the public. Careful consideration should be given to providing equal access according to the public's ability to use electronic or other means of access, including access for the disabled under the Americans with Disabilities Act (ADA).

1. What technologies do you have (paper, telephonic, electronic)?
2. Where is your information located predominantly?
3. What are your information storage and management goals? (Are you moving toward a paperless system?)
4. What methods of access are available? Are justice agency requesters being treated uniformly? Are public requests treated uniformly? Are varying methods of access to the same information available, including paper, telephone, and electronic? Do your methods of access account for varying levels of justice agencies' electronic capabilities? The public's electronic capability? Have you considered appropriate means of access under the ADA? Are alternative access methods available by request?

5. What are your operational and cost limitations? Are there processing/fiscal limits on the amount of justice agency or public access afforded by your system (electronic or manual)?

6. What information quality/accuracy can be assured from the various methods of access?

7. Do you charge access fees? If so, what is your fee structure? Does this structure reflect a thoughtful cost analysis, balancing the need for interagency sharing or public access with real costs? Do you intend to make a profit on interagency sharing? If so, are you? If not, are you? Do you intend to make a profit on public access? If so, are you? If not, are you?

Below is a hypothetical example of a method-of-access statement for a court:

[Example Court]'s goal is to provide justice agencies in [jurisdiction or jurisdictions] with efficient and timely access to information necessary to the day-to-day operation of their agencies. Electronic, telephonic, and paper access will be determined through interagency agreements. [Example Court] is striving to move toward a fully automated information records system. Therefore, sharing agreements will focus on utilizing the most advanced information sharing capabilities of the agencies involved.

[Example Court] also strives to provide the public with efficient and timely access to public record information. We offer paper copy and/or electronic information system access to public records, depending upon the method by which our agency currently maintains the information.

Electronic information systems access is available for all information requests for records dating from 1995 to the present. For information requests prior to 1995, electronic access may not yet be available. In these instances, [Example Court] will seek to process your information requests as quickly as possible, pursuant to our paper records access policy.[66]

Electronic access to public records is available through our Web site at www.courtrecordsaccess.org, or at computer terminals located in the clerk's office. If you are unable to access our electronic records through the Internet or an access terminal, these records are available by written request, pursuant to our paper records access policy.

Records access fees are charged for both electronic and paper access.

[66] Denoting a "paper records access policy" is simply an attempt to highlight that there may be differing response times and fees for actual paper copy requests. This is not a determination that information will be treated differently in a paper request.

Section IV

Privacy Policy Assessment, Education, and Training

Chapter Seven:

Privacy Impact Assessment for Justice Information Systems

Purpose: to explain the importance and process of undertaking a privacy impact assessment (PIA) for single agency and integrated justice information systems, and to provide templates for doing single agency and integrated justice system impact assessments

A Privacy Impact Assessment (PIA) is a process used to evaluate privacy implications of information systems. An agency or integrated system may use a PIA to implement and assess the effect of its privacy policy.

Getting Started on a PIA

Discussed here are the benefits, components, and goals of a PIA. The importance of assessing privacy risks is also stressed.

What are the benefits and components of a PIA?

PIAs provide a number of benefits to justice agencies that include enhancing policy decision-making and system design, anticipating the public's possible privacy concerns, and generating confidence that privacy policies are being considered in the development and implementation of single agency or integrated justice information systems.

The PIA process described in this chapter is designed to guide state, local, and tribal justice agencies in assessing privacy throughout the early stages of justice system development, as well as assessing privacy risks of their existing operational systems. The process consists of using an information flow map, applying a set of privacy questions to the information flow, identifying risks, and developing a solution to these privacy risks.

A PIA has three components:

1. A map of the information flows associated with the justice agency's, or the integrated system's, business activity to determine information decision points and privacy vulnerabilities.[67]
2. A privacy analysis of the information flow that examines whether agreed-upon privacy policies are adhered to, whether there is technical compliance

[67] This is essentially the same information flow map as discussed in Chapter Six.

with a jurisdiction's statutory or regulatory privacy requirements, and whether these policies and laws are affording the desired privacy protection.

3. An analysis of privacy issues raised by the system review, including a risk assessment and a discussion of the options available for mitigating any identified risks.

What are the objectives and goals of a justice system PIA?

The objective of the PIA is to help justice practitioners identify and address information privacy when planning, developing, implementing, and operating individual agency and integrated justice information systems. PIA goals include:

- Providing senior justice leaders with the tools necessary to make fully-informed policy and system design or procurement decisions based on an understanding of privacy risk and of the options available for mitigating that risk.
- Ensuring accountability for privacy issues is clearly incorporated into the role of the justice system project managers and sponsors.
- Ensuring that there is a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy law and regulation, as well as accepted privacy policy.
- Providing basic documentation on the flow of personal information within the justice systems for use and review by policy and program staff, systems analysts, and security analysts, and as the basis for the following: public response and comment; adequate notice and consent statements (where applicable) for the accused, victims, witnesses, jurors, and their families; structuring legislative amendments, contract specifications and penalties, partnership agreements, and monitoring and enforcement mechanisms; post-implementation verification and periodic reviews and audits.
- Providing a methodology that ensures the best possible implementation of privacy protections at the start-up of justice information systems.
- Identifying remedial steps necessary to improve privacy protection in existing operational justice information systems.

When is a PIA needed?

Relevance. A PIA is relevant when justice agencies are developing or currently operating information management systems or integrated information systems that involve the collection, access, use, or dissemination of personal information.

Examples of information systems' initiatives that may require a PIA include:

- Creation, modification, or annual review of databases containing personal information, particularly where the information is sensitive or the database includes information about a significant number of people.

- Development of identification and authentication tools, especially those for multipurpose identifiers (e.g., state identification numbers "SIDs") or biometrics.
- Development and implementation of system integration policy and technologies that promote interagency justice information access or sharing between law enforcement, prosecution, defense, courts, corrections, probation, and parole.
- Development and implementation of system integration policy and technologies that promote interagency justice information access or sharing, including juvenile justice, family courts, probate courts, general civil courts, and affiliated agencies, such as health, social services, education, and transportation.
- Development and implementation of electronic public access policy and technologies.

Timing. Ideally, a PIA should be initiated at the early stages of system development and integration planning. Privacy must be considered in the concept and system definition stages and continue through analyzing the system requirements and making decisions about data usage and system design.

The PIA is best approached as an evolving document, moving from general application of privacy policy at the concept stage to detailed assessment of these policies at the system development and acquisition stages. It is imperative to recognize that a PIA is not a "one-time" procedure for justice agencies or integrated systems. PIAs should be done at various times from planning through implementation and should become part of ongoing system upgrades and maintenance schedules.

Although it is best to begin a PIA at the early stages of system concept and design, given the importance of personal information privacy, PIAs of existing justice systems are also necessary to assess and address ongoing information system privacy issues. PIAs of existing systems may be planned to coincide with system upgrades or maintenance.

Who completes the integrated justice system PIA?

Privacy policy development is largely the responsibility of high-level policy executive(s) within the justice system. Ensuring compliance and effectiveness of privacy policy is also the duty of those responsible agents, whether in a single-agency system or an integrated justice system. This person or group of persons is sometimes referred to as the "information steward"[68] for the justice agency or integrated system. The information steward will be guided by jurisdictionally applicable law or regulation and may look to sources of policy guidance, such as the privacy design principles.

The information steward should be a part of a team that is integral to the development and operation of the overall information system policy. The duties of the information steward in conducting a PIA differ from those of a "privacy auditor," which infers policy review at arm's length rather than from the inside out.

[68] See Chapter Three, "Privacy Design Principles for Justice Information Systems," and design principle 8 for a full explanation of the accountability principle.

For purposes of this document, the function of the information steward is discussed in the context of an integrated justice information system.

In an integrated justice system, the information steward, whether an individual or group, must ensure that privacy law and policy is implemented appropriately and that law and policy are actually affording the anticipated privacy protections.

To accomplish this mandate, the information steward may choose to appoint a privacy project manager (PPM)[69] to monitor privacy concerns during development, implementation, and operation of the integrated system.[70]

For example, at the outset of the integrated system design, the PPM[71] would undertake the following:

1. **Component system review.** Work with representatives from each component agency to oversee the completion of a PIA for each component agency's system, involve the system "owners" and the system "developers" in completing each component's PIA,[72] and develop an agreement of a "baseline standard"[73] of privacy protection.

2. **Integrated system review.** Conduct a PIA of the integrated system itself by comparing the project design decisions against the criteria of the privacy design principles and jurisdictional law and regulation, assessing the impact of the agency systems on the privacy objectives of the overall system, giving special attention to unintended affects on privacy created by interagency information sharing, and providing results from all the PIAs (agency and integrated system) to the justice system information steward.

In this context, the information steward bears ultimate responsibility for ensuring the implementation of privacy policy. This responsibility is carried out through the PPM overseeing the PIA process for each agency and for the integrated system. Any adjustments or changes in policy as a result of the PIAs must be addressed by the information steward. Resolution of the privacy issues is discussed further in step six of PIA preparation, later in this chapter.

---

[69] The PPM should have a range of skills including policy development, operational program and business design, technology and systems expertise, risk and compliance analysis, and procedural and legal knowledge.

[70] If the PIA is being undertaken by a single agency, the roles of the information steward and the PPM still apply. In some smaller agencies or jurisdictions, however, these roles may be combined. The information steward would oversee the completion of the impact assessment and work to address any resulting privacy concerns.

[71] It is recognized that privacy impact assessments require broad knowledge of both policy and technology issues. The PPM may need to develop a team approach to completing the PIAs of each agency and the integrated system. In this collaborative effort, however, it is important that a single individual ultimately be responsible for ensuring completion of the privacy impact assessment.

[72] The system "owners" are the individual justice agencies responsible for outlining their systems' purposes and requirements. The system "developers" are the entities, either private sector or government, that will address technical aspects associated with implementing the owners' requirements.

[73] The baseline privacy standard is that level of privacy protection toward which each component system will work to achieve. Privacy issues should be addressed component by component until each agency system achieves the agreed-upon baseline of "privacy protection."

Assessing privacy risk

What is risk? The PIA assesses "privacy risks" associated with operating justice information systems that collect, access, use, or disseminate personal information. The term "privacy risk" takes on two meanings in this context.

The first pertains to the risk to citizens stemming from their personal information, how it is used, and the propensity for individual harm from inappropriate use. As discussed in earlier chapters,[74] the collection of personal information in the justice system differs from private sector information gathering and even from other governmental information gathering. The difference is apparent in the areas of notice, consent, and voluntary participation. Most individuals who are in contact with the justice system are not voluntary participants; e.g., the accused, victim, witnesses, and even jurors, and personal information about these individuals is obtained and used regardless of their consent. Therefore, the nature of personal information collection, use, and dissemination in the justice system requires an elevated standard of agency accountability to ameliorate the risk of harm to individuals from misuse of personal information within the justice enterprise or release to the public.

The second is the risk to the success of justice information sharing systems themselves. The greater the perceived individual risk to the public, the greater the actual risk to justice system agencies that information sharing will endure harsh criticism. Ultimately, this climate will impede the ability to share information electronically and reduce the justice system's efficiency and effectiveness.

For example, risks to an integrated justice system in considering privacy implications may include:

- Stimulating public outcry as a result of a perceived (or actual) loss of privacy or a failure to meet expectations with regard to the protection of personal information;
- Losing credibility or public confidence (and ultimately legislative funding) where the public feels that a proposed program or project has not adequately considered or addressed privacy concerns;
- Incurring possible liability at the personal or agency level; and
- Underestimating privacy requirements such that systems need to be redesigned or retrofitted late in the developmental stage at considerable expense.

Technical points of risk. Fundamentally, many people within the justice community associate privacy with security. Although the two terms are not synonymous, they are interrelated. For instance, when an organization establishes privacy policies, they normally define the mechanisms and procedures for enforcing these policies. Security, then, is best viewed as a category of tools and techniques for implementing organizational policies (including those related to privacy). Security practitioners normally divide the security domain into six basic functions:

1. **Authentication.** Definitively identifies individuals before they are allowed to request information resources.

[74] See Chapters Two, Four, and Five.

2. **Access control.** Permits individuals to access only those information resources they explicitly have been given permission to use.
3. **Confidentiality.** Protects data from disclosure to unauthorized individuals.
4. **Nonrepudiation.** Verifies that transactions occurred, and prevents one party from refuting the transaction to a second party.
5. **Integrity.** Protects data from unauthorized modification or destruction.
6. **Availability.** Minimizes business process disruption caused by information availability issues.

The first three of these security functions (i.e., authentication, access control, and confidentiality) are essential for the effective implementation of any privacy policy. Aside from policy considerations of what information should be shared versus what information should remain private, there are a variety of technical issues that must be resolved in order to provide assurances that privacy policies can and will be enforced. Data owners should evaluate their privacy risks and design effective security infrastructures to mitigate applicable technical risks. Examples of technical risk mitigation issues are included in Appendix C.

These areas scratch the surface of what technologists must be concerned about when considering privacy and security issues. Although we recognize that "privacy" is not the same as "security," the terms are inextricably related when considering how privacy affects the information technology applied in the justice environment.

Managing risk. The risks identified above can be managed with careful attention to privacy policy and applicable law. Risk in integrated justice systems can be managed with the use of strategies and tools such as the privacy design principles, privacy-enhancing technologies,[75] privacy impact assessments, standards, and public education.

Steps in the PIA Process for Justice Information Systems

The PIA for justice information systems is designed to assess privacy risk through evaluating an information system's implementation of the privacy design principles through its privacy policy, as well as its adherence to jurisdiction-specific privacy law or regulation. Full text and explanation of the privacy design principles is set out in Chapter Three. Developing and drafting a privacy policy is set out in Chapters Four, Five, and Six. Agencies using the PIA should also consult the specific privacy law and regulation of their jurisdictions. A compilation of existing state privacy law is available from *Privacy Journal.*[76]

---

[75] Examples of privacy-enhancing technologies include encryption, digital signatures, anonymous electronic cash, and service delivery systems.

[76] Robert Ellis Smith, "Compilation of State and Federal Privacy Laws," 1997 ed. (Supp. 1999). *Privacy Journal* is an independent newsletter, focusing on privacy in a Computer Age, that has been published monthly since it was founded in November 1974. *Privacy Journal* maintains an extensive research collection of materials about privacy, including a compilation of state and federal privacy laws. Resources can be obtained through *Privacy Journal*, Post Office Box 28577, Providence, RI 02908, (401) 274-7861, privacyjournal@prodigy.net.

Review of the overall PIA process

As noted earlier, a general PIA has three components: a map of the information flows, a privacy analysis of the system information flow, and an analysis of privacy issues raised and options available for mitigating identified risks. Justice agencies assessing their information management systems should complete each of those components through the six-step process described below.

In an integrated system PIA, there are two levels of assessment. First, a PIA needs to be completed for each justice component agency's system, and second, a PIA needs to be completed for the information exchanges of the integrated information sharing system itself. The objective of undertaking the two levels of assessment is to identify privacy issues of each component system, assuring that they are properly addressed, and to evaluate the privacy impact of all the component systems working together in an integrated capacity.

In doing an integrated system PIA, the information steward is responsible for assessing and resolving information privacy issues. The information steward may appoint a privacy project manager (PPM), who has the responsibility of working with the component agencies to ensure that each completes a system PIA. These component PIAs can be completed within each agency and then communicated to the PPM, or the PPM and his or her team can undertake the agency PIAs as part of the overall integrated system assessment.

When privacy risks are identified, the PPM should raise the privacy concerns to the system's information steward for policy and technology direction. This should be done at the earliest possible phase of system design and development and continue throughout implementation and system maintenance. The ability to accurately address an integrated system's privacy impact through a PIA depends on each agency's dedication to identifying potential (or actual) privacy risks at each stage of justice information system development and implementation.

While a complete six-step PIA includes all three stages (information flow map, privacy analysis, and risk analysis), each stage alone may be useful to information stewards and system designers as they go through the design and decision-making processes. For example:

- A "general privacy issue identification" for each component system is useful to gage what privacy issues are germane to the purpose of the overall system at the concept and planning stages.
- In an integrated system, each component agency can complete the issue identification piece while the more complex information flow map is under development.
- Where the PIA involves assessing an existing system, a general analysis of privacy issues may help to suggest immediate policy adjustments while system design changes are contemplated.

PIA step one: Mapping the information flow

Mapping the information flow requires developing a decision tree to understand the decision points relating to information collection, use, and dissemination within an agency system or an integrated justice system. Mapping information flows in a

privacy context is discussed at length in Chapter Six. The information flow maps discussed there to draft privacy policy are the same as those needed to complete PIA step one.

PIA step two: Component agency privacy analysis questions and answers

If a single agency desires to assess the privacy impact of its information management system(s), the agency should complete the questions and answers (Q&A) in this section. After completing the Q&A, an agency should complete the privacy analysis in step three and move to resolving privacy issues in step six.

If an agency is completing the impact assessment as part of an integrated information system, the agency should provide the completed assessment to the integrated system PPM.

Understanding your agency's environment. Before proceeding to the Q&A based on the privacy design principles, it is essential that you determine if your information system is part of a unique "environment" of systems that may be subject to special law, regulation, or policy. This determination may affect how you answer the privacy design principle assessment questions. Please consider the following:

- Is the information in the system being compiled for the purposes of identifying individual criminal offenders and alleged offenders? Does it consist only of identifying information and notations of arrest, the nature and disposition of criminal charges, sentencing, confinement, release, and probation or parole status (criminal history record information)? Is this compilation considered the "official criminal history record" for state reporting purposes? Is the system collecting this information funded in whole or in part with federal government funds? If so, does the system comply with the requirements of 28 CFR Part 20?
- Is information in the system being compiled for the purpose of criminal intelligence investigation of individuals, including reports of informants and investigators? Is there relevant state, local, or tribal law, regulation, or policy that governs your system's collection, access, use, or dissemination of this type of information? Is the system collecting this information funded in whole or in part with federal government funds? If so, does the system comply with the requirements of 28 CFR Part 23?
- Does information in the system include information on juvenile offenders or suspected offenders, or their families? Is there relevant state, local, or tribal law, regulation, or policy that governs your system's collection, access, use, or dissemination of this type of information?
- Does the information in the system include information required by statute to be maintained and used for research or statistical purposes? Is there relevant state, local, or tribal law, regulation, or policy that governs your system's collection, access, use, or dissemination of this type of information? Is the system collecting this information funded in whole or in part with federal government funds? If so, does the system comply with the requirements of 28 CFR Part 22?

- Is there relevant state, local, or tribal law or regulation that governs your system's collection, access, use, or dissemination of personal information in general?
- Has your agency undertaken a specific effort to identify any relevant law, regulation, or policy relating to the information mentioned above?
- Has your agency undertaken a specific effort to implement identified legal and policy requirements where necessary?

These questions are intended to flag privacy issues specifically associated with criminal history information, criminal intelligence information, juvenile justice information, and information used for research or statistical purposes, as well as to highlight the necessity to become aware of and to implement requirements of jurisdictionally specific law, regulation, and policy.

A careful analysis of agency systems collecting, accessing, using, or disseminating personal information should be done, taking into account specific jurisdictional law, regulation, or policy in these contexts. Agencies completing their PIAs should seek legal counsel within their jurisdictions to ensure these requirements are implemented appropriately.

Privacy design principle Q&A. The questions that follow are based on the eight privacy design principles discussed in Chapter Three.

1. Are you following the purpose specification principle?
   - Is there a written purpose statement for the system collecting personal information? Set out the purpose statement(s).
   - Is the written statement(s) publicly available prior to the time of information collection?
   - If available publicly, is the written statement(s) set out in the organization's collection form(s) in a comprehensive and prominent manner?
   - Is the written purpose statement periodically reviewed and updated?
   - Has a clear relationship been established between the personal information being collected and the system's functional purpose and operational requirements?
   - Is the personal information collected pertinent to the stated purposes for which the information is to be used?
   - Are there limits on subsequent (secondary) use of the information?
   - Are there limits on third-party or private-sector partnerships or relationships where personal information is or will be disclosed?
   - If not, do these secondary use(s) conform to the stated purpose?
   - Does the system have mechanisms to inform data subjects of third party, secondary use disclosure?
2. Are you following the collection limitation principle?
   - Are you limiting the collection of personal information to the system's identifiable purpose?

- Is personal information obtained by lawful and fair means?
- Where appropriate, is personal information obtained with the knowledge or consent of the data subject?
- Is relevance considered when collecting personal information on individuals without their knowledge or consent, or when the individual is not charged with a crime (i.e., under investigation, or when an investigative body is "information gathering")?

3. Are you following the data quality principle?
   - Is the personal information collected for stated purposes accurate, complete, current, and verified?
   - Is the system collecting "original" or "new" information?
   - Is the personal information collected directly from the data subject?
   - Do you have a procedure for tracking requests to modify information, determinations of the requests to modify, modifications made based on the requests, the source of the information that is used to modify the information, and when the last modification occurred?
   - Is there a procedure to provide notice of correction (modification) to subsequent justice system users and third parties (secondary users)?
   - Where appropriate, does the data subject have some means of accessing the information to ensure it is accurate and up to date?
   - Where personal access by the data subject is not appropriate, are there other methods to ensure that the information held is accurate and up to date?
   - When a person challenges the accuracy of a record, is he/she provided with information about the agency personnel responsible for the record and administrative procedures governing inquiries?
   - Do you have procedures for addressing data management issues and record retention issues?
4. Are you following the use limitation principle?
   - Is the use of the information relevant to the purpose for which the system is being designed (operated)?
   - Does the system limit the use or disclosure of personal information to the articulated purpose(s) in accordance with principle one?
   - Are any secondary uses limited to those with the consent of the data subject, by the authority of law, for the safety of the community (including victims and witnesses), or pursuant to a public access policy?
   - If personal identifiers are used for purposes of linking across multiple databases, do these multiple databases have consistent purposes?
   - Do you have procedures to ensure a "record of use" is maintained? Is it attached to each piece of personal information?

- Will the system prevent the derivation of new information or creation of previously unavailable information about an individual through aggregation from the information collected? Is an agency or the system itself prevented from making determinations about individuals that would not be possible without this new information? Do you have procedures in place to verify the new information for relevancy and accuracy?
- Do you prohibit personal information from being sold or released under public access policy to private information gatherers (resellers)? If not, is the released information "publicly accessible"[77] pursuant to your public access policy? If sold to private information gatherers (resellers), are there any contractual agreements between you that would prevent the unintended use, or misuse, of the personal information provided by your system?
- Does the system have mechanisms to inform data subjects of third-party (public), secondary use disclosure?

5. Are you following the security safeguards principle?
   - Does the system have security safeguards?
   - Have you documented the system's security safeguards that protect personal information against loss, unauthorized access, destruction, use, modification, and disclosure?
   - Are security safeguards provided according to sensitivity of the information and risks to all involved parties?
   - Has there been an expert security review?
   - Have staff been trained in requirements and ethics for protecting personal information?
   - Is staff aware of policies and consequences regarding breeches of security?
   - Are there controls in place over the processes that grant authorization to modify (add or delete) personal information?
   - Does the system allow user access and changes to personal information to be audited by date and user identification?
   - Are user accounts, access rights, and security authorizations controlled and recorded by accountable systems or records management processes?
   - Are access rights provided only to users who actually require access for the system's stated purposes?
   - Are there contingency plans and mechanisms in place to identify security breaches and disclosures of personal information in error?
   - Are there mechanisms in place to communicate violations or errors to subsequent users to mitigate collateral risks?
   - Are there adequate, ongoing resources budgeted in maintenance plans for security upgrades with measurable performance indicators?

[77] "Publicly accessible," meaning, that which by law or tradition is readily available to nonjustice organizations or individuals without the need to state an authorized purpose.

- Are the system's security safeguards comprehensive enough to include all system back-up mechanisms?

6. Are you following the openness principle?
   - Does the system have a general policy of openness about developments, practices, and policies with respect to the *management* of personal information (apart from the actual information)?
   - Does openness include public access to the management practices of the information?
   - Does openness require clear communication to affected individuals where justice records are requested, sold, or released to third parties?
   - Does openness require clear communication to affected individuals where justice records are requested, sold, or released under the system's public access policy?
7. Are you following the individual participation principle?
   - Does the system allow an individual, or an agent for an individual, to obtain confirmation of whether or not the data collector has information relating to him or her?
   - Does the system allow an individual to receive information relating to him or her 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/her?
   - Does the system provide for an explanation if a request is denied? Is an individual able to challenge a denial?
   - Is the system designed to afford the above access rights with minimal disruption to day-to-day operations?
8. Are you following the accountability principle?
   - That is, is there an individual or agency body who is accountable for complying with measures that give effect to the privacy design principles, the public access policy, and applicable law or regulation?

PIA step three: Assessing the component agency answers

The answers to the foregoing eight questions should be compared to the objectives of each corresponding privacy design principle contained in Chapter Three.

Questions 1-8 above are phrased to help identify possible areas of information privacy vulnerabilities within an agency system. Where a question is answered in the negative ("No"), agency representatives should document the following items for each such answer:

1. What is the reason(s) that you answered "No"?
2. Is there a law, regulation, or articulated policy that would except the system from compliance with a particular policy suggested by the privacy design principle connected to this question?

3. Is there a logical exception related to the purpose of the agency system (e.g., law enforcement investigation or intelligence gathering)?
4. What can be done to the system to make the answer to this question "Yes"?
5. If you must retain the identified privacy risk, what plans or procedures are in place to mitigate possible effects of the identified risk?

Agency representatives should keep in mind that although there may be a legal, regulatory, or traditional policy exception for their information system, implementation of additional privacy protections may be appropriate. This is especially relevant given the public's interest in and growing concern about information privacy. The documentation as to why the system has not answered affirmatively ("Yes") to any one of the questions in the PIA should be retained and become a formal part of the impact assessment.

Additionally, where an agency is part of an integrated information sharing system, the agency, in cooperation with the PPM, should weigh its responses to the questionnaire against the agreed-upon "privacy baseline" of the integrated system agencies. Where the agency's system falls short of meeting the privacy objectives, these areas should be brought to the attention of the integrated system PPM and receive additional consideration.

PIA step four: Integrated system privacy analysis questions and answers

The integrated system PPM should answer the following questions, taking into consideration the results of the component agency PIAs. The questions are based on the eight privacy design principles discussed in Chapter Three.

1. Does the integrated justice system follow the purpose specification principle?
   - Are the purpose statements of the component agencies' systems compatible?
   - Have all of the component agencies agreed to the purpose for which information is collected in those agencies that are passing them information or to which they pass information?
2. Does the integrated justice system follow the collection principle?
   - Are the collection policies of the component agencies' systems compatible?
   - Have you determined which agency bears responsibility for protecting the privacy rights of individuals affected by the collection of information when it is shared among other justice agencies?
   - Have you determined which agency is responsible for data quality of the collected information (see below)?
   - Do you have a process in place to evaluate the possible cumulative effects on individual privacy due to sharing information collected by different component systems?
3. Does the integrated justice system follow the data quality principle?
   - Are the data quality assessments of the component agencies compatible?

- If they are not compatible, can you identify the weakest "link(s) in the chain"?
- Do you have a procedure in place to address (improve) data quality at this weakest point(s)?

4. Does the integrated justice system follow the use limitation principle?
   - Are the use limitation policies of the component agencies compatible?
   - Are the public access policies of the component agencies compatible?
   - Is information "publicly accessible" under one component's public access policy also "publicly accessible" under all the other's public access policies?
   - Does the integrated system have mechanisms to inform data subjects of third-party (public), secondary use disclosure?
   - Does the use of information throughout the integrated system derive *new* information (such as a compilation)?
   - Are the component agencies only using this information according to the agreed purpose of the integrated system?
   - Are component agencies aware that their decision-making may be based on "new" (aggregated) information?
   - Do the component agencies have safeguards, or review procedures, at these decision-making points?
   - Does the integrated system limit the release of this new information to secondary sources such as scientific, educational, or other government organizations; private industry; the media; information resellers; and private individuals?
5. Does the integrated justice system follow the security principle?
   - Are security levels of the component agencies' systems compatible?
   - Can you identify the weakest "link(s) in the security chain" in the integrated system?
   - Do you have a procedure in place to address (improve) security at this weakest point(s)?
   - Do you have procedures in place that allow you to improve (upgrade) security while still maintaining the interagency flow of information in the integrated system?
6. Does the integrated justice system follow the openness principle?
   - Are the openness standards of the component agencies compatible?
   - Are there openness standards for the integrated system itself?
   - Does the integrated system have a general policy of openness about developments, practices, and policies with respect to the *management* of personal information (apart from the actual information)?

- Does openness include public access to the management practices for the information?
- Does openness require clear communication to affected individuals if agencies within the integrated system sell or release personal information to third parties?
- Does openness require clear communication to affected individuals if agencies within the integrated system sell or release personal information pursuant to public access policies?

7. Does the integrated justice system follow the individual participation principle?
   - Are the individual access policies of the component agencies compatible?
   - Are the individual challenge procedures of the component agencies comparable?
   - Do the component agencies' access policies and challenge procedures have no measurable negative impact on the day-to-day operation of the integrated system?
8. Does the integrated justice system follow the accountability principle?
   - Is there an information steward for the system who is accountable for complying with measures that give effect to the privacy design principles, public access policy, and any applicable law or regulation?
   - Is the information steward accountable for (1) ensuring all the above privacy design principles have been incorporated in the technology design from the conceptual and contextual phase through implementation; (2) ensuring information systems are capable of providing access to personal information on request and recording who has had access to the personal information and for what purpose; (3) ensuring staff managing information are trained on privacy protection requirements as detailed; (4) ensuring information systems are transparent and documented so that individuals or a proxy can be informed about the collection, access, use, and disclosure of their personal information within the context of the principles outlined above; and (5) establishing regular security and privacy compliance audits commensurate with the risks to the data subject or other individuals with a relationship to the justice system?
   - Has the information steward assigned responsibility for completing PIAs and conducting ongoing privacy assessments to a privacy project manager (PPM) or other individuals or bodies?

PIA step five: Assessing the integrated justice system answers

As in the component agency assessments, the answers to the foregoing eight questions should be compared to the objectives of each corresponding privacy design principle contained in Chapter Three. The PPM has responsibility for weighing the results of the questionnaire against the privacy design principle objectives.

Questions 1-8 above are phrased to help identify possible areas of information privacy vulnerabilities within an integrated justice system. Where a question is answered in the negative ("No"), agency representatives should document the following items for each such answer:

1. What is the reason(s) that you answered "No"?
2. Is there a law, regulation, or articulated policy that would except the integrated system from compliance with a particular policy suggested by the privacy design principle connected to this question?
3. Is there a logical exception related to the purpose of the integrated system (e.g., law enforcement investigation or intelligence gathering)?
4. What can be done to the system to make the answer to this question "Yes"?
5. If you must retain the identified privacy risk, what plans or procedures are in place to mitigate possible effects of the identified risk?

The documented answers should become a formal part of the integrated justice system PIA. Where the integrated system falls short of meeting the privacy objectives, these areas should be brought to the attention of the integrated system information steward and should receive additional consideration, as described below.

PIA step six: Resolving privacy issues

Successful privacy policy development and implementation requires a combined effort of policy leaders, information technology managers, and line-system users. This combined effort is needed when developing and implementing privacy policy in a single justice agency system, as well as in an integrated justice system.

Privacy policy development is largely the responsibility of high-level policy executives within the justice system: the information stewards. Results of an agency or integrated system PIA may identify privacy vulnerabilities within the system that are not addressed by existing law, regulation, or policy. In these instances, the information steward should work to develop policy and procedures to mitigate personal information privacy risk at the identified points in the system. Broad principles, such as the privacy design principles, may assist the information steward in this task. The information steward should also consult the original data flow maps. A modification in data flow may serve to mitigate risk in some instances.

The information steward may also determine that certain policy questions rise to a level that require public discussion and political debate. In these instances, privacy policy development may need to be supplemented by legislative action. It is the task, albeit an often difficult task, of the information steward to bring such privacy issues to the attention of the legislature. It is important, however, for the information steward to take immediate steps to mitigate risk while awaiting legislative action on the identified privacy issues, even though privacy policies or procedures may have to be changed to conform to resulting law.

One of the risks to any justice information system is the risk created by negative public perception. Information stewards should consider mitigating this risk through education and open dialog with the media and the public about their privacy policy and assessment strategies. The PIA can assist information stewards and system

managers in identifying those areas that may draw public concern and developing thoughtful public response. It is important to begin an open dialog during the planning phase of justice information system projects and where existing systems are involved, as soon as privacy policies and procedures are developed. Chapter Eight expands on this topic.

Chapter Eight:

Privacy Policy Education and Training

Purpose: to stress the nature and importance of privacy policy education and training for not only agency leaders, practitioners, and staff, but also the public

Everyone bears responsibility for a workable balance of public access, public safety, and privacy—everyone—legislators, the judiciary, justice leaders and practitioners, other executive agencies, profit and nonprofit companies, the media, and individuals themselves. Each has a role in assuring the responsible collection, maintenance, use, and dissemination of justice information. Each needs to be educated and trained on the benefits and consequences of using justice information, especially as affected by electronic information technologies. The discussion below provides suggestions for developing education and training resources for the justice system and for the public.

Education and Training for Leaders, Practitioners, and Staff

Privacy and public access policy is only as effective as the people who make it work. Within the justice system, various levels of education and training need to take place to support effective implementation of a privacy and public access policy. These levels include high-level decision makers, managers, line practitioners, and staff.

In many jurisdictions over the last five or six years, the "information privacy status quo" has been upset by the implementation of new information technologies. For example, information that has always been called "public" is now truly public—and widely accessible. Justice leaders and practitioners alike are faced with new privacy policy and, in some cases, legal requirements, the successful implementation of which requires a culture change within their organizations.

What is this culture change? The culture change is twofold and requires the reconciliation of competing ideas. First, it involves recognizing that privacy is a critical issue in planning for and operating justice information systems. Second, the culture change involves providing for true access to public information and structuring

daily business operations around a presumption of public access. To effect the change in culture, education and training is critical at all levels, from legislators who bear the responsibility for privacy policy to staff who deal directly with requests for information. The discussion below highlights why education is important to each level and suggests some mechanisms for providing targeted training.

Decision makers: Executive, legislative, and judicial

Judges, elected officials, and agency directors will ultimately set the tone for privacy policy through case law, statutes, and administrative rules. These leaders are also affected by the recent attention to the issue of privacy and are being asked to provide immediate solutions. Often leaders are required to make decisions with little knowledge about the real effects information technologies are having on day-to-day information collection, use, and sharing in the justice system.

As true in almost all policy development, it is incumbent upon justice managers and practitioners to advise and inform these leaders about the practical privacy consequences of information use, collection, and disclosure within the various justice disciplines. One suggested method is to provide leaders with anecdotal evidence of where privacy policy has worked and where and why it has failed.

Operational managers

Operational managers hold the most difficult position with respect to developing and implementing privacy policy. This responsibility often includes informing decision makers about privacy consequences, as well as leading by example within the agency to set the tone in supporting careful use of personally identifiable information, while promoting public access and customer service. Managers' responsibilities may also extend to developing working policy; i.e., taking legislative, judicial, or high-level executive decisions and developing processes that implement this policy. This may include making many of the hard decisions as to what information within their systems is nondiscloseable, discloseable, or publicly accessible.

In tackling difficult decisions, it is important for justice managers to share ideas with other justice agencies. This is essential in an integrated system context, and is true for a single agency as well. At this time, no one person or agency has all the answers to developing and implementing a foolproof privacy policy. Some agencies have been working with the difficult issues longer than others, however. As with all good policy, it should not be formed in a vacuum.

Justice managers are also responsible for developing procedures that seek to implement well-considered privacy policy goals. Procedures, themselves, however, should not operate as de facto access limitations or privacy protections. If procedures are outdated or inefficient, they should be reevaluated.

For example, a gentleman on vacation was run down by an electric-powered vehicle at a well-known theme park. Although the theme park usually prefers to settle such matters without involving traditional law enforcement and court processes, the gentleman made an incident report to the local (city) police department. After returning home, he attempted to get a copy of the police report. He called the city police department and was told that the local sheriff's department was handling his report. He contacted the sheriff's department and was advised that he needed to

write a letter requesting the report. He wrote a letter requesting the "accident report." He received a letter from the sheriff's department stating that what he required was not an "accident report," but rather a "crash report"; he would need to write another letter requesting the crash report. The gentleman responded as directed. He received another letter from the sheriff's office notifying him that the crash report would cost $2.50 and please enclose that amount. The gentleman responded with a letter requesting the "crash report" and enclosing $2.50. The gentleman received a response from the local sheriff's office stating that his request was received, but the local sheriff only keeps such reports for 21 days, and as that time had expired, the report now resided at the state records center in another city–and the story continued.

In this true example, the failure of the privacy policy did not rest on one particular law, rule, manager, or staff. The culture of the agency and its procedures did not support public access and customer service, and the traditional access rules acted as a de facto nondisclosure policy. These types of access processes no longer make sense in an electronic world and are no longer being accepted pro forma by the public.

Manager education should incorporate training on the various responsibilities of justice managers above.

Justice practitioners

"Justice practitioners," as addressed in this discussion, refers to line professionals, such as police officers; assistant prosecutors; defense counsel; courtroom deputies; court clerks; and corrections, probation, and parole officers. These groups, though not responsible for implementing privacy and public access policy, must understand the effects of their day-to-day practice on the collection, use, and dissemination of information. The awareness requirement is not meant to impede their functions but to guide them in how they collect, use, and disseminate personal information. The goal is to avoid reckless violation of policy by understanding the interplay of the three concepts: public safety, privacy, and public access.

Leadership from justice managers establishing the importance of privacy along with the presumption of public access is important to supporting practitioners' interaction with the public. Practitioners should also be aware of and understand the meaning of their own agency's data. Such education should encourage informed decision-making in working with justice information.

Educating "frontline" staff

For purposes of this discussion, frontline staff refers to those justice staff members who provide the administrative and customer interface between the justice system and the public. Frontline staff are responsible for working under the policies developed by leaders and justice managers. Like practitioners, frontline staff are influenced by good leadership, therefore highlighting the need for managers to create a culture that balances public safety, privacy, and public access (customer service).

In the past, resistance to filling requests for public information was, in many cases, the result of staff acting out managers' nondisclosure attitudes, or fear of releasing inappropriate information that might damage their agency or another individual. The

goal of the privacy policy is to eliminate pervasive nondisclosure attitudes and fear of liability. Managers are required to put good policy in place that allows staff to respond effectively without fear of personal or professional consequences from releasing information. To operate effectively, staff must be provided a basis of general privacy concepts, but not get bogged down in the details. Difficult decisions should be made at the managerial level, so staff can perform effectively.

For example, an agency may design an electronic information system so that line staff have direct access to public information for which the agency is responsible. Discloseable or nondiscloseable (yellow and red) information is protected in the system by requiring a password. Staff attempting to access this information would know to contact a supervisor or to follow a different set of parameters for processing the request. Otherwise, the public information (green) is readily available without requiring staff to evaluate the request or the information.

Education and Training for the Public

The public, as defined at the beginning of this document, consists of groups or individuals who are not directly related to the justice system. In order to interact with the justice system in a reasonable fashion, the public needs to be educated and trained on how and why the justice system collects, uses, and disseminates personal information. The public also needs to be informed about the responsibility it bears as a secondary user of justice information and the possible privacy consequences of its own misuse.

The first part of education and training is to develop and make widely available thoughtful resources (whether print or electronic) that assist the public in interacting with the justice system. In so doing:

- **Set the context for the public.** Provide information on basic civic issues. For example, what are the three branches of government? In which branch of the government does this particular agency reside? With what level of government are they interacting in seeking this information (federal, state, county, city, tribal)? If dealing with an integrated justice system, what is an integrated justice system? What agencies are participating in the integrated justice system?
- **Explain the information.** Why is information collected by the justice system? Why has information been publicly accessible historically? Why does collected information continue to be made public? How is the information intended to be used by the agency or integrated system? What accuracy and "freshness" of the information can be expected? In what form is the information available (paper, electronic)?
- **Explain the information request process.** How is a request made? To whom? What is the cost (if any)? When can a response be expected? In what format will the requester receive a response?
- **Explain the public's rights and remedies.** If something in the information is incorrect, what is the complaint/correction procedure? If there is a failure in the public access process, what is the complaint procedure? Who is the agency or integrated system privacy contact? What is the telephone number and address of this individual (or department)?

- **Lead by example.** Provide examples of commonly requested public records and how and where to request these documents.

Many of the answers to the questions above can be drawn directly from the agency or integrated system's privacy policy "statement of purpose." Other elements can be drawn from jurisdictionally specific law, regulation, or administrative rules. If there is information that the public requires in order to interact with the agency or integrated system that is not covered in a law, regulation, rule, or policy, the agency or integrated system's information steward should be notified and asked to resolve this issue.[78]

The second part of education and training is to inform the public of their own responsibilities as secondary users of justice information:

- **Explain what the agency or integrated system intends the information to represent in a public context.**[79] Identify the quality, timeliness, and completeness of the information, and advise the public of possible consequences in using the information for purposes other than for which it was intended.
- **Set forth liability limitations and other contractual parameters.** Such limitations are most likely in an information "sale" context. In a strictly public access context, liability limits may involve guarantees of timeliness and completeness of the agency's or integrated system's original records at the time of release. For example, a jurisdiction may inform the public of the consequences of secondary use and disclosure by explaining that the official information, or justice record, can be obtained only from their agency or integrated system. Other records provided by commercial information vendors may contain similar information, but the agency or integrated system cannot guarantee the accuracy of the commercial information.

The better informed the public is about the availability and consequences from using justice information, the better it can act and react in a reasonable fashion with the justice system. The public should not be surprised about what information is available. For the most part, this information has been available historically. The public should understand the nature of the information and how, when, and why it was collected by the justice system. The public should understand the intended use of the information. The public should understand how to interact with justice agencies and integrated systems to access, review, and correct personal information. The public should understand the possible privacy consequences, and its own possible liability, from use of the information for purposes not intended by the justice system.

Access to justice information, especially personally identifiable justice information, although an important undertaking, is not a risk-free undertaking. Better education and training of the public, as well as justice leaders, practitioners, and staff, however, can mitigate some of the risks involved.

---

[78] It is noted in the privacy impact assessment that the information steward may not have all the answers. Some issues rise to the level that require legislative or judicial decision. It is the information steward's responsibility at this point to bring the issue to the attention of the appropriate government body.

[79] This idea is directly related to the mitigation of risk discussion advising an agency or integrated system to know the meaning of its own information. Any agency or integrated system should be able to articulate the meaning of its information, whether released by single record or in bulk.

Conclusion

Privacy of personal data (information privacy) encompasses when, how, and to what extent you share personal information about yourself. Information privacy involves the right to control one's personal information and the ability to determine if and how that information should be obtained and used. It entails restrictions on a wide range of activities relating to personal information: its collection, use, retention and disclosure.

Information systems are integral to the operation of justice agencies. The implementation of more sophisticated technologies is changing information collection, access, use, and dissemination practices of the past. For example, integrated justice systems include the criminal justice process, as well as civil court records, juvenile justice information, and probate and family proceedings. Increasingly, integrated justice systems also interact with information systems of affiliated agencies, such as health, welfare, and transportation.

Justice system leaders are being asked to develop justice information privacy policy, often without the benefit of established law, regulation, or policy precedent. In developing new privacy policy, it is important for justice leaders to consider traditional information practices, as well as the effects of new information collection, use, and dissemination technologies. Tools such as the privacy design principles, privacy policy template, and the privacy impact assessment for justice information systems, while not the "silver bullets" for privacy policy, are intended to assist justice leaders in developing information privacy policies critical to justice system operation in the twenty-first century.

Appendices

Appendix A:

Fair Information Practices

The Fair Information Practices can be summarized as follows:

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

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

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

4. **Use limitation principle.** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with Paragraph three except (a) with the consent of the data subject or (b) by the authority of law.

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

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

7. **Individual participation principle.** An individual should have the right to (a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) have communicated 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) be given reasons if a request made under (a) and (b) is denied, and to be able to challenge such denial; and (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

8. **Accountability principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.

Appendix B:

Safe Harbor Privacy Principles

Issued by the U.S. Department of Commerce, July 21, 2000

The European Union's (EU) comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Union to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that applies to the processing of personal data in the Member States.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the Principles must comply with the Principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an organization joins a self- regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor. Organizations may also qualify by developing their own self-regulatory privacy policies, provided that they conform

with the Principles. Where in complying with the Principles, an organization relies in whole or in part on self-regulation; its failure to comply with such self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts. (See the annex for the list of U.S. statutory bodies recognized by the EU.) In addition, organizations subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy may also qualify for safe harbor benefits. In all instances, safe harbor benefits are assured from the date on which each organization wishing to qualify for the safe harbor self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidelines set forth in the Frequently Asked Question on Self-Certification**.**

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor. To qualify for the safe harbor, organizations are not obligated to apply these Principles to personal information in manually-processed filing systems. Organizations wishing to benefit from the safe harbor for receiving information in manually-processed filing systems from the EU must apply the Principles to any such information transferred after they enter the safe harbor. Organizations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the Principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently Asked Questions apply where they are relevant.

"Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

Notice: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but, in any event, before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.[(1)]

Choice: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party[(1)] or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the individual's sexual orientation), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt-in choice. In any case, an organization should treat any information received from a third party as sensitive where the third party treats and identifies it as sensitive.

Onward Transfer: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding, or enters into a written agreement with third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way, and the organization has not taken reasonable steps to prevent or stop such processing.

Security: Organizations creating, maintaining, using, or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration, and destruction.

Data Integrity: Consistent with the Principles, personal information must be relevant to the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable, accurate, complete, and current for its intended use.

Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend**,** or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow-up procedures for verifying that the attestations and assertions that businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of a failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

(1.) It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

Appendix C:

Data Security Issues and Options

As has been stated throughout this document, privacy entails more than just security. Security services—such as authentication, access control, and confidentiality—are of tremendous importance to organizations in implementing their privacy policies. In determining how most appropriately to protect your data, there are many purely technical issues for data owners to consider. The choice of which type of technology to use, and how it should be used, is best decided after the programmatic and policy decisions are made (e.g., Who does the data owner want to have access? How should users access data? What access methods are necessary for the user's jobs?). The most important factor is to ensure that a comprehensive security infrastructure is designed with specific security and privacy goals in mind. Below are a number of highlighted security issue areas and some suggested technology options to provide for increased security. These suggestions are not meant to be limiting, nor are they meant to be an exhaustive listing. These options are offered as a reference to justice information system managers based on experiences of various justice entities.

Network Security

Perimeter security. Routers, firewalls, and intrusion detection systems should be implemented to tightly control access to networks from outside sources. Routers and firewalls filter and restrict traffic based upon very specific access control decisions made by the network operators, thereby limiting the types of unauthorized activities on a network. Conversely, the goal of intrusion detection systems is to monitor usage of information systems and data in near-real-time and to block patterns of behavior that appear to violate system security or privacy policies. Routers, firewalls, and intrusion detection systems are almost always used in a coordinated manner to provide a high level of service assurance. These systems can also be used to establish control points between various internal segments of an organization's network.

Network access. Data owners may want to develop policies to limit data interchange between intranets, thereby minimizing network security risks. Before developing technical solutions to implement these policies, data owners must assess how this will impact the agency's overall system integration objective. Because of potential

performance issues, these solutions may not be viable. Data owners are encouraged to determine user needs (e.g., Do users need laptop and dial-in access?) prior to establishing policies that will prevent needed access. It is prudent to configure network access to discourage anonymous download operations.

Telecommunications. Fiberoptic network cabling is preferred over copper wiring for systems requiring high levels of protection. It has been proven by security practitioners that network signals (e.g., data packets and voice transmissions) are less easily intercepted from fiberoptic cabling than from other copper-based alternatives.

System Security

Advanced authentication. Definitively identifying users before they access an organization's network is a key component in protecting information resources. Start by choosing an authentication system with encrypted password protocols. By establishing password procedures, such as requiring a specified format for passwords, password aging, and active use of audit trails, you can close the loopholes that intruders use to compromise systems. Higher levels of protection can be achieved by implementing advanced mechanisms using cryptographic or biometric authentication. Before choosing an advanced authentication system, it is imperative that data owners evaluate user access, hardware, and other requirements.

Encryption. Many security practitioners believe that encryption technologies, such as those provided by public key infrastructures (PKI), are an essential component in comprehensive privacy and security solutions. We highly recommend that organizations investigate the feasibility of implementing PKI and component technologies such as certification servers for their networks. Certification servers maintain the "electronic identity" (e.g., digital certificates) for each of the organization's authorized users. Based on the access rights assigned to each user, these certificates can then be used as "tickets" to gain access to authorized files and directories. The system operator should choose an encryption solution commensurate with the level of (1) risk of possible interception or disclosure; (2) sensitivity of the data transmitted; and (3) access necessary for authorized users.

Audit trails. The use of audit procedures (e.g., tracking who is accessing the data, what data was accessed) combined with analysis of audit logs and follow-up for unauthorized or anomalous activity is essential for long-term system security and privacy.

Physical security. System and network administrators should tightly control physical access to computer and network hardware. Only authorized members of the technical staff should be allowed access to systems.

Database integrity. It may be advisable, depending on the sensitivity of the data, to utilize multilevel, secure database products to ensure the safety of data. Multilevel secure databases segregate data into areas where users may or may not have access, depending on levels of authorized access. Such user-access permissions are set by a database administrator. Additionally, limiting data access via database engine passwords or digital certificates separate from the operating system password adds another layer of security.

User Awareness and Training

In addition to concerns about technical risks, one of the largest data protection issues revolves around what is commonly referred to as "social engineering." Social engineering involves the unauthorized disclosure of sensitive information by an individual authorized to have the information. For instance, computer intruders frequently make telephone calls to individuals in an organization, masquerading as a fellow employee. The intruders then attempt to talk the employee into divulging sensitive information such as passwords, network addresses, or ID numbers. The most effective mitigation strategy for social engineering as well as other human integrity issues is periodic training for authorized users on the organization's security and privacy policies.

Appendix D:

Washington State Courts Policy

I. AUTHORITY AND SCOPE

A. These policies govern the release of information in the Judicial Information System (JIS) and are promulgated by the JIS Committee, pursuant to JISCR 12 and 15(d). They apply to all requests for computer-based court information subject to JISCR 15.

1. These policies are to be administered in the context of the requirement of Article I, §10 of the Constitution of the State of Washington that "Justice in all cases shall be administered openly, and without unnecessary delay," as well as the privacy protections of Article I, §7.

2. These policies do not apply to requests initiated by or with the consent of the Administrator for the Courts for the purpose of answering a request vital to the internal business of the courts. See JISCR 15(a).

II. DEFINITIONS

A. Records

1. "**JIS record**" is an electronic representation (bits/bytes) of information either stored within, derived from, or accessed from the OAC. (Amended February 27, 1998.)

2. "**JIS legal record**" is a JIS record that is the electronic duplication of the journal of proceedings or other case-related information which it is the duty of the court clerk to keep, and which is programmed to be available in human readable and retrievable form. Case information reflecting the official legal file and displayed by JIS programs are JIS legal records.

B. JIS Reports

1. "**JIS reports**" are the results of special programs written to retrieve and manipulate JIS records into a human readable form, other than the JIS legal record.

2. "**Compiled reports**" are based on information related to more than one case or more than one court. As used in this policy, "compiled reports" do not include index reports.

C. Data Dissemination Management

1. "**Data dissemination**" is the reporting or other release of information derived from JIS records.

2. The "**data dissemination manager**" is the individual designated within the Office of the Administrator for the Courts and within each individual court and assigned the responsibility for administration of data dissemination, including responding to requests of the public, other governmental agencies, or other participants in the judicial information system. The name and title of the current data dissemination manager for each court and the Office of the Administrator for the Courts shall be kept on file with the Office of the Administrator for the Courts.

D. Electronic Data Dissemination Contract

The **"electronic data dissemination contract"** is an agreement between the Office of the Administrator for the Courts and any entity, except a Washington State court (Supreme Court, court of appeals, superior court, district court, or municipal court), that is provided information contained in the JIS in an electronic format. The data dissemination contract shall specify terms and conditions, as approved by the Judicial Information System Committee, concerning the data including but not limited to restrictions, obligations, and cost recovery agreements. Any such contract shall at a minimum include the language contained in Exhibit A— Electronic Data Dissemination Contract. (Amended February 27, 1998.)

III. ACCESS TO JIS LEGAL RECORDS

A. **Open Records Policy**. The following principles apply to the interpretation of procedural rules or guidelines set forth in this policy.

1. Information related to the conduct of the courts' business, including statistical information and information related to the performance of courts and judicial officers, is to be disclosed as fully as resources will permit.

2. In order to effectuate the policies protecting individual privacy which are incorporated in statutes, case law, and policy guidelines, direct downloading of the database is prohibited except for the index items identified in Section III.B.6. Such downloads shall be subject to conditions contained in the electronic data dissemination contract. (Amended February 27, 1998.)

3. Dissemination of compiled reports on an individual, including information from more than one case, is to be limited to those items contained in a case index, as defined in Section III.B.6.

4. Privacy protections accorded by the Legislature to records held by other state agencies are to be applied to requests for computerized

information from court records, unless admitted in the record of a judicial proceeding, or otherwise made a part of a file in such a proceeding, so that court computer records will not be used to circumvent such protections.

5. **Contact Lists**: Access to JIS information will not be granted when to do so would have the effect of providing access to lists of individuals for commercial purposes, defined as set forth in RCW 42.17.260(6) and WAC 390-13-010; i.e., that in connection with access to a list of individuals, the person requesting the record intends that the list will be used to communicate with the individuals named in the record for the purpose of facilitating profit expecting activity.

6. Except to the extent that dissemination is restricted by Section IV.B, or is subject to provisions in the electronic data dissemination contract, electronic records representing court documents are to be made available on a case-by-case and court-by-court basis as fully as they are in hard copy form. (Amended February 27, 1998.)

B. All access to JIS information is subject to the requirements of the criteria for release of data specified in JISCR 15(f): availability of data, specificity of the request, potential for infringement of personal privacy created by release of the information requested, and potential disruption to the internal ongoing business of the courts. JIS information provided in electronic format shall be subject to provisions contained in the electronic data dissemination contract. (Amended February 27, 1998.)

1. Court data dissemination managers will restrict the dissemination of JIS reports to data related to the manager's particular court, or court operations subject to the supervision of that court, except where the court has access to JIS statewide indices.

2. Routine summary reports will be made available to the public upon request, subject to the payment of an established fee and so long as such request can be met without unduly disrupting the ongoing business of the courts.

3. Access to JIS legal records, in the form of case-specific records, will be permitted to the extent that such records in other forms are open to inspection by statute, case law, and court rule, and unless restricted by the privacy and confidentiality policies below.

4. Individuals, personally or through their designees, may obtain access to compiled legal records pertaining to themselves upon written request, accompanied by a signed waiver of privacy.

5. No compiled reports will be disseminated containing information which permits a person, other than a judicial officer or an attorney engaged in the conduct of court business, to be identified as an individual, except that data dissemination managers may disseminate the following:

   a. Public agency requested reports. Reports requested by public agencies which perform, as a principal function, activities directly

related to the prosecution, adjudication, detention, or rehabilitation of criminal offenders, or to the investigation, adjudication, or enforcement of orders related to the violation of professional standards of conduct, specifically including criminal justice agencies certified to receive criminal history record information pursuant to RCW 10.97.030(5)(b).

b. Personal reports, on the request or signed waiver of the subject of the report.

c. On court order.

6. An index report, containing some or all of the following information, may be disseminated: (Amended February 27, 1998.)

a. Filing date;

b. Case caption;

c. Party name and relationship to case (e.g., plaintiff, defendant);

d. Cause of action or charge;

e. Case number or designation;

f. Case outcome; and

g. Disposition date.

(III.B.6.f. and III.B.6.g. added December 5, 1997.)

An index report provided in electronic format shall be subject to the provisions contained in the electronic data dissemination contract. (Amended February 27, 1998.)

7. A report sorted by case resolution and resolution type, giving index criteria except individual names, may be compiled and released. (Section added June 21, 1996.)

IV. JIS PRIVACY AND CONFIDENTIALITY POLICIES

A. Information in JIS records which is sealed, exempted, or otherwise restricted by law or court rule, whether or not directly applicable to the courts, may not be released except by specific court order.

B. Confidential information regarding individual litigants, witnesses, or jurors that has been collected for the internal administrative operations of the courts will not be disseminated. This information includes, but is not limited to, credit card and P.I.N. numbers, and social security numbers. Identifying information (including, but not limited to, residential addresses and residential phone numbers) regarding individual litigants, witnesses, or jurors will not be disseminated, except that the residential addresses of litigants will be available to the extent otherwise permitted by law. (Section amended September 20, 1996; June 26, 1998.)

C. A data dissemination manager may provide data for a research report when the identification of specific individuals is ancillary to the purpose of the research, the data will not be sold or otherwise distributed to third

parties, and the requester agrees to maintain the confidentiality required by these policies. In such instances, the requester shall complete a research agreement in a form prescribed by the Office of the Administrator for the Courts. The research agreement shall (1) require the requester to explain provisions for the secure protection of any data that is confidential, using physical locks, computer passwords and/or encryption; (2) prohibit the disclosure of data in any form which identifies an individual; (3) prohibit the copying or duplication of information or data provided other than for the stated research, evaluative, or statistical purpose. (Amended June 6, 1997.)

V. PROCEDURES

A. Uniform procedures for requesting JIS information, and for the appeal of decisions of data dissemination managers, shall be as set forth in policies issued by the Office of the Administrator for the Courts pursuant to JISCR 15(d).

B. In any case where a report is provided, the report must be accompanied by a suitable disclaimer noting that the court can make no representation regarding the identity of any persons whose names appear in the report, and that the court makes no representation as to the accuracy and completeness of the data except for court purposes.

VI. ACCESS TO AND USE OF DATA BY COURTS

Courts and their employees may access and use JIS records only for the purpose of conducting official court business. Such access and use shall be governed by appropriate security policies and procedures.

VII. ACCESS TO AND USE OF DATA BY CRIMINAL JUSTICE AGENCIES

A. "Criminal justice agencies" as defined in RCW Chapter 10.97 shall have additional access to JIS records beyond that which is permitted the public.

B. The JIS Committee shall approve the access level and permitted use(s) for classes of criminal justice agencies including, but not limited to, law enforcement, prosecutors, and corrections. An agency that is not covered by a class may request access.

C. Agencies requesting access under this provision shall identify the information requested and the proposed use(s).

D. Access by criminal justice agencies shall be governed by an electronic data dissemination contract with each such agency. The contract shall:

1. Specify the data to which access is granted.

2. Specify the uses which the agency may make of the data.

3. Include the agency's agreement that its employees will access the data only for the uses specified.

VIII. ACCESS TO AND USE OF DATA BY PUBLIC PURPOSE AGENCIES

A. "Public purpose agency" includes governmental agencies included in the definition of "agency" in RCW 42.17.020 and other non-profit organizations whose principal function is to provide services to the public.

B. Upon approval by the JIS Committee, public purpose agencies may be granted additional access to JIS records beyond that which is permitted the public.

C. Agencies requesting additional access under this provision shall identify the information requested and the proposed use(s). In reviewing such requests, the JISC will consider such criteria as:

1. The extent to which access will result in efficiencies in the operation of a court or courts.
2. The extent to which access will enable the fulfillment of a legislative mandate.
3. The extent to which access will result in efficiencies in other parts of the criminal justice system.
4. The risks created by permitting such access.

D. Access by public purpose agencies shall be governed by an electronic data dissemination contract with each such agency. The contract shall:

1. Specify the data to which access is granted.
2. Specify the uses which the agency may make of the data.
3. Include the agency's agreement that its employees will access the data only for the uses specified

IX. E-MAIL

The JIS provides e-mail for official court business use only. Access to judicial officers' and court employees' e-mail is restricted. Access to a judicial officer's e-mail files shall only be granted with the permission of the judicial officer involved. Request for access to a court employee's e-mail or to logs containing records on an employee's e-mail shall be subject to the review and approval of the county clerk if the employee is employed in the clerk's office, or the presiding judge or court administrator if the employee is employed by the court. Nothing in this policy shall be used as a reason to withhold records which are the subject of a subpoena or otherwise available to the public.

X. VERSION HISTORY

These policies shall take effect 30 days from the date of their adoption by the Judicial Information Systems Committee, May 19, 1995.

Adopted May 19, 1995
Amended June 21, 1996
Amended September 20, 1996
Amended June 6, 1997
Amended December 5, 1997
Amended February 27, 1998
Amended June 26, 1998

Acknowledgments

The *Justice Information Privacy Guideline* was developed through a cooperative effort of the National Criminal Justice Association, the United States Department of Justice, Office of Justice Programs (OJP), and the Office of the Ontario Information Privacy Commissioner. A special thanks to the developers and drafters of this document:[80]

Dr. Ann Cavoukian, Information Privacy Commissioner, Ontario, Canada

Mr. Paul F. Kendall, General Counsel, Office of Justice Programs (former)

Ms. Anne E. Gardner, Assistant U.S. Attorney, Eastern District of Arkansas

Mr. Brian Beamish, Director of Policy and Compliance, Information and Privacy Commission, Ontario, Canada

Mr. Michael Gurski, Policy and Technology Officer, Information and Privacy Commission, Ontario, Canada

Mr. David Boyer, Office of Justice Programs, Information Technology Consultant, ACS Defense, Inc.

Ms. Patricia F. S. Cogswell, Attorney-Advisor, U.S. Department of Justice, Justice Management Division

Thanks to the following individuals who contributed their time and insights to the Privacy Guideline.

Ms. Brenda Barber
Integrated Justice Program Manager
Arkansas Crime Information Center
Arkansas

Ms. Sheila Barton
Deputy Executive Director
SEARCH
Sacramento, CA

[80] Note: Individuals are listed with their professional affiliations at the time they participated in drafting the Guideline.

Honorable Patrice Bataglia
County Commissioner
Dakota County
Mendota Heights, MN

Mr. Robert Belair
General Counsel for SEARCH
Mullenholz, Brimsek & Belair
Washington, DC

Mr. Sol Bermann
Legal Project Manager
Technology Policy Group
The Ohio Supercomputer Center
Columbus, OH

Honorable John P. Bessey
Judge
Court of Common Pleas
General Division
Columbus, OH

Ms. Mary L. Boland
Assistant State's Attorney
Chicago, IL

Mr. Christopher Bosch
Division Chief
Kansas City, Missouri, Fire Department
Kansas City, MO

Mr. John G. Boufford
President
E-Privacy Management Systems
Lakefield, Ontario

Ms. Terrie Bousquin
Chief Information Officer
New Mexico Supreme Court
Judicial Information Division
Santa Fe, NM

Mr. Donovan D. Brown, Sr.
Chief Prosecutor
Navajo Nation
Office of Chief Prosecutor
Window Rock, AR

Mr. Timothy Burns
Justice Information Analyst
Pinellas County Department of Justice Coordination
Clearwater, FL

Ms. Emily S. Busse
Staff Associate
National Criminal Justice Association
Washington, DC

Mr. Alan Carlson
Director San Francisco Office
Justice Management Institute
El Cerrito, CA

Mr. James Carmack
Deputy Director
NCRLE
Little Rock, AR

Mr. Melvin J. Carraway
Superintendent
Indiana State Police Department
Indianapolis, IN

Honorable Thomas M. Cecil
Judge
Sacramento Superior Court
Sacramento, CA

Dr. Hugh M. Collins
Judicial Administrator
Supreme Court of Louisiana
New Orleans, LA

Mr. Gary Cooper
Executive Director
SEARCH
Sacramento, CA

Ms. Janet Cornell
Information Technology Consultant
Office of CIO
Maricopa County
Phoenix, AZ

Ms. Karen Costello
Victim/Witness Assistance Coordinator
Craighead County Office of Victim/Witness Assistance
Jonesboro, AR

Mr. Frank Cox
Chief Deputy Public Defender
Office of the Public Defender
San Rafael, CA

Mr. Ed Crockett
Information Systems Manager
Administrative Officers for the Courts
Pretrial Services
Frankfort, KY

Mr. Cabell Cropper
Executive Director
National Criminal Justice Association
Washington, DC

Ms. Rebecca Daugherty
FOI Service Center Director
Reporters Committee for Freedom of the Press
Arlington, VA

Mr. Robert Deyling
Chief, Judges Support Branch
Article III, Judges Division
Administrative Office of the U.S. Courts
Washington, DC

Mr. Paul Edmonson
Deputy City Attorney
San Diego City Attorney
San Diego, CA

Mr. Paul S. Embley
UCJIS Project Manager
Commonwealth of Kentucky
Frankfort, KY

Ms. Katherine Hunt Federle
Director
Justice for Children Project
Columbus, OH

Mr. J. Robert Flores
Vice President, Senior Counsel
National Law Center for Children and Families
Fairfax, VA

Mr. Gregory A. Frost
Executive Assistant to the Police Chief
Tallahassee Police Department
Tallahassee, FL

Mr. Anthony J. Gagliano
Deputy Judicial Administrator
Supreme Court of Louisiana
New Orleans, LA

Ms. Julie Spence Gefke
Director, National Interoperability Task Force
National Law Enforcement Corrections Technology Center
Denver, CO

Mr. Ted Gest
President
Criminal Justice Journalists/ Sr. Fellow at University of Pennsylvania
Washington, DC

Ms. Kimberly Glenn
Information Services Manager
San Diego Police Department
San Diego, CA

Ms. Karen Gottlieb
Court Consultant
Nederland, CO

Mr. Robert E. Greeves
Policy Advisor
Office of General Counsel
Office of Justice Programs
Washington, DC

Ms. Lee Guice
Staff Attorney
Administrative Office of the Courts
Frankfort, KY

Ms. Elizabeth Haley
Assistant General Counsel
Federal Bureau of Investigation
Washington, DC

Ms. Ailsa Hamilton
Director
Ontario Integrated Justice Systems
Ontario Provincial Government
Toronto, Ontario, Canada

Mr. James Floyd Harris
Manager of Records
Courts and Detention Services
City of Dallas
Dallas, TX

Mr. Dennis Hausman
Justice Information Network Coordinator
Department of Information Services
Olympia, WA

Dr. Thomas A. Henderson
Executive Director
Office of Government Relations
National Center for State Courts
Arlington, VA

Mr. Domingo S. Herraiz
Director
Office of Criminal Justice Services
Columbus, OH

Ms. Karen Huey
Deputy Chief of Staff
Ohio Attorney General's Office
Columbus, OH

Dr. Hunter Hurst
Director
National Center for Juvenile Justice
Pittsburgh, PA

Mr. Michael D. Johnson
United States Attorney
Eastern District Arkansas
Little Rock, AR

Dr. Candice M. Kane
Executive Director
Illinois Criminal Justice Information Authority
Chicago, IL

Ms. Carol Kaplan
Bureau of Justice Statistics
U.S. Department of Justice
Washington, DC

Mr. Matthew C. Keck
Assistant Attorney General
Michigan Department of Attorney General
Lansing, MI

Mr. Paul Keister
Director, Information Technology
National Association of Counties
Washington, DC

Mr. J. Clark Kelso
Professor of Law
University of the Pacific (McGeorge School of Law)
Sacramento, CA

Mr. Noble Kennamer
Special Assistant Public Defender
Los Angeles County Public Defender
Cerritos, CA

Honorable Catherine D. Kimball
Associate Justice
Louisiana Supreme Court
New Orleans, LA

Mr. Kent Koehler
QA/Technical Support Coordinator
Sedgwick County Emergency Communications
Wichita, KS

Ms. Luli Landis
Director of Marketing and Communications
Miami-Dade County Clerk's Office
Miami, FL

Mr. Barry Mahoney
President
Justice Management Institute
Denver, CO

Mr. Kent Markus
Professor
John Marshal School of Law
Columbus, OH

Mr. John Maxwell
Chief Operating Officer
AAMVAnet, Inc.
Arlington, VA

Ms. Amy Melick
Deputy Attorney General
Office of the Attorney General
State of New Jersey
Trenton, NJ

Mr. Patrick McCreary
Program Manager
Office of the Assistant Attorney General
Washington, DC

Mr. Harlin McEwen
Chairman, Communications and Technology Committee
International Association of Chiefs of Police
Ithaca, NY

Ms. Janice McMann
Correctional Records Manager
Washington State Department of Corrections
Olympia, WA

Mr. Kevin Morrell
Information Technologies Manager
North Miami Beach Police Department
North Miami Beach, FL

Ms. Terri Morrison
Association Legal Counsel
Colorado State Court Administrator's Office
Office of Probation Services
Denver, CO

Ms. Heather Morton
Policy Associate
National Conference of State Legislatures
Denver, CO

Ms. Deirdre Mulligan
Staff Counsel
Center for Democracy and Technology
Washington, DC

Mr. Randall L. Murphy
Administrator
Management Services Department
Lake County
Waukegan, IL

Ms. Shannon O'Connor
Program Manager
Bureau of Justice Assistance
U.S. Department of Justice
Washington, DC

Mr. Mark O' Hara
Government Affairs Counsel
National Criminal Justice Association
Washington, DC

Ms. Sue Outland
Director of Research and Planning
Superior Court of Arizona
Juvenile Court Center
Phoenix, AZ

Ms. Theresa A. Pardo
Project Director
Center for Technology in Government
University at Albany/SUNY
Albany, NY

Mr. Jim Peschong
Assistant Chief
Lincoln Police Department
Lincoln, NE

Dr. Donald E. Price
Chief of Information Technology
Washington State Department of Corrections
Olympia, WA

Mr. Charlie Pruitt
Deputy Director
Arkansas Crime Information Center
Little Rock, AR

Ms. Janet Quist
Director
Public Safety Programs
Public Technology, Inc.
Washington, DC

Ms. Lee Robinson
Project Leader
Justice Information System
Metro Nashville
Nashville, TN

Mr. Robert Roper
Chief Information Officer
Colorado State Court Administrator's Office
Denver, CO

Ms. Jiroko Rosales
Director
Court and Detention Services
City of Dallas
Dallas, TX

Mr. Randy Ross
Executive Director
Indian Center, Inc.
Lincoln, NE

Chief Lynn S. Rowe
Chief of Police
Fifth District Department of Correctional Services
Des Moines, IA

Mr. Thom Rubel
Director
State Information Technology Programs
National Governors' Association
Washington, DC

Ms. Pamela Scanlon
Executive Director
Automated Regional Justice Information System (ARJIS)
San Diego, CA

Dr. Peter Scharf
Co-Director
Center for Society, Law & Justice
University of New Orleans
Metairie, LA

Ms. Natalie Schell
Staff Associate
National Criminal Justice Association
Washington, DC

Mr. Ari Schwartz
Senior Policy Analyst
Center for Democracy and Technology
Washington, DC

Mr. Christian Selch
Project Manager
Supreme Court of Ohio
Columbus, OH

Ms. Caren Shantz
Attorney
Center for Arkansas Legal Services
Little Rock, AR

Mr. Tom Shepherd
Director
Iowa Office of Information Technology Innovations
State of Iowa
Information Technology Department
Des Moines, IA

Mr. Hal Sklar
Senior Counsel
Federal Bureau of Investigation
Criminal Justice Information Services Division
Clarksburg, WV

Mr. Louis T. Smith
Chief Information Officer
Kentucky Justice Cabinet
Frankfort, KY

Mr. David Sobel
General Counsel
Electronic Privacy Information Center
Washington, DC

Ms. Martha Steketee
Senior Research Associate
National Center for State Courts
Arlington, VA

Mr. Bob Stellingworth
Co-Director
Center for Society, Law & Justice
University of New Orleans
Metairie, LA

Ms. Karen Sublett
Deputy Director
Office of Justice Programs
U.S. Department of Justice
Washington, DC

Ms. Teri Sullivan
Director
Justice Information System
Metro Government of Nashville
Nashville, TN

Mr. Mark C. Thompson
Director of Administration
New Hampshire Department of Justice
Concord, NH

Ms. Jennifer Walden
Systems Analyst
Texas Department of Information Resources
Austin, TX

Mr. Richard Ward III
Deputy Director
Bureau of Justice Assistance
U.S. Department of Justice
Washington, DC

Mr. Bob Wessels
Court Manager
County Courts of Law
Houston, TX

Mr. Ron Wiborg
Contracts and Grants Manager
Hennepin County Corrections
Minneapolis, MN

Mr. Carl Wicklund
Executive Director
American Probation and Parole Association
Lexington, KY

Ms. Dianne T. Williams
Deputy Director
Georgia Criminal Justice Coordination Council
Atlanta, GA

Mr. John Woulds
Director of Operations
The Data Protection Registrar
(Wycliffe House)
Wilmslow, United Kingdom

Glossary

The words and terms below are defined according to the sense and context in which they are used in this *Guideline*.

Confidentiality: Pertains to limiting access to personal information to those with specific permission to receive it and preventing its disclosure to unauthorized third parties.

Consistent use: Data use or reuse in conformity with the stated purpose(s) for which the data were collected initially.

Criminal history record: Compilation of an individual's arrest and disposition information.

Criminal justice process: Encompasses the arrest and prosecution of adults charged with criminal offenses.

Enterprise architecture: Refers to the specifications of an information technology that spans multiple organizations and allows those organizations to share and use information in a seamless and transparent way.

Enterprise-wide technology: A technology system spanning law enforcement, courts, corrections, and other justice components.

Firewall: Refers to hardware or software designed to act as a barrier to hostile incoming traffic.

Information steward: A high-level executive or group largely responsible for developing and periodically assessing the effectiveness of privacy policy applicable to personal information during the design, development, and ongoing operation of a justice agency's information system.

Information privacy: Privacy of personal data, which involves the right to control one's personal information and the ability to determine how that information should be obtained and used.

Integrated justice information system: One that encompasses more than one agency and enables access, collection, use, and dissemination of critical information at key decision points throughout the justice process, including the capability to automatically query regional, statewide, and national databases and to report key transactions regarding people and cases to local, regional, statewide, and national systems.

Justice information: Includes both civil and criminal justice data.

Legacy system: An information system based on old technology.

Personal information: Information about an identifiable individual, such as race, marital status, criminal or employment history, medical data, social security or telephone number, or fingerprints.

Personally identifiable justice information: Information that, when released, is linked to an individual or, through analysis, can be linked to an individual.

Platform: Computer.

Privacy: Refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information in the justice system. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data (information privacy).

Public access: Refers to the public's interest in monitoring justice system processes through access to justice information.

Public safety: Pertains, in an information context, to justice agencies' collection, use, and disclosure of information to promote criminal or civil justice functions.

Technology architecture: The underlying technology structure and protocols that determine the specifications to which the technology is built and that describe how information can be stored and accessed.

The public: Includes a broad group of people and organizations (individuals, for-profit and nonprofit entities, and media) outside the traditional justice system agencies (law enforcement, prosecution, defense, courts, corrections, probation, parole, and victims services). Nontraditional justice agencies—such as social services, health, fire/EMS, and transportation—may be public depending on the context in which traditional justice agencies are sharing information with them.