Privacy Impact Assessment for Justice Information Systems

Working Paper

February 2001

Table of Contents

Privacy Impact Assessment for Justice Information Systems

Executive Summary:

Key players in the justice community, from law enforcement, to prosecution and defense, through the courts and correctional institutions, to probation and parole services, are using today's information technologies to improve the management of information in their daily operations. As the implementation of electronic information collection and sharing capabilities increases, so does public and governmental concern over the use, or potential misuse, of personal information contained in these systems.[1] Increasingly, justice leaders are being forced to identify and address information privacy issues, often without the assistance of a tested privacy policy, applicable law, or process guidelines.

Information privacy is a growing concern among the public, elected officials, and justice leaders for good reason. The inability or lack of desire to address privacy concerns associated with information management systems can result in dire consequences for the public and government agencies alike. 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 incorrect justice information may be associated with one's name and subsequently used to one's detriment. Such was the case with an Ohio man whose social security number was accidently associated with another individual who possessed a criminal history record.[2] 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. These advanced information systems 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. Today's technologies, applied in a strategic fashion, hold the promise of reduced paper work, quick information capturing, broad transmittal and access capabilities, improved information quality, and reduced long-term costs.

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 highly efficient and effective multi-million dollar information management systems to a screeching halt. Therefore, ongoing privacy policy development and privacy impact assessments are critical to protecting the public's privacy and the justice system's technology investment.

What does it take to protect privacy?

Identifying and assessing privacy issues associated with the electronic collection, access, use, and dissemination of personal information in the justice system requires commitment from justice policy makers, information management specialists, and operational employees. Additionally, the costs associated with developing and implementing an information 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 public outcry, loss of public confidence and legislative funding, and real costs of modifying information systems to include privacy protections after system implementation.

A privacy impact assessment for justice information systems has been designed by state, local, and tribal justice leaders to assist state, local, and tribal justice agencies in developing and implementing information privacy policy. The drafters of this resource encourage all justice agencies to consider whether their current information system strategies include sufficient privacy policy. They suggest that you consider whether your agency should do a privacy impact assessment by answering the following questions:

1. Do you collect, use, or provide access to personally identifiable information?

2. Do you disclose or provide access to information to persons or agencies outside your organization?

3. Is your information system connected to other information systems?

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 needs to be concerned about privacy and should develop a privacy policy and prepare a privacy impact assessment.

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 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 and the Public Access Guideline for Justice Information Systems, 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 Impact Assessment for Justice Information Systems described below, 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 assigned to one independently.

Privacy Resources

In response to a growing need for assistance in this area, the United States Department of Justice, Office of Justice Programs, the Office of the Ontario Information and Privacy Commissioner, and the National Criminal Justice Association joined together with state, local, and tribal justice leaders to develop broad principles of justice privacy policy and tools to assist jurisdictions in assessing the privacy implications of their information systems.

The first document produced by this collaboration is the Privacy Design Principles for an Integrated Justice System (Privacy Design Principles).[3] The Privacy Design Principles, based on fair information practices adopted by the European Community, address privacy issues associated with collection, access, use, and dissemination of personal information in the justice system.

The second tool is the Public Access Guideline for Justice Information Systems (Public Access Guideline).[4] The Public Access Guideline discusses issues justice agencies face in maintaining an open justice system while protecting individual privacy. The Public Access Guideline is intended to assist state, local, and tribal justice agencies in developing public access policy that can be used in planning and design of their information systems and as part of their privacy impact assessments.

The third tool is a Privacy Impact Assessment for Justice Information Systems (PIA). The PIA is designed to help justice agencies follow applicable privacy law and apply the intent of the Privacy Design Principles and public access policies in their component agency systems and throughout information sharing mechanisms established with other agencies.

The purpose of the following PIA document is to:

1. Describe the importance and the process of undertaking a Privacy Impact Assessment.

2. Develop a series of questions to assess privacy risks in state, local, and tribal justice information systems.

3. Develop a process to assist state, local, and tribal governments in addressing privacy risks associated with justice information systems.

Conclusion

Information systems are integral to the operation of the justice enterprise. Information collection, access, use, and dissemination practices of the past are changing as agencies seek to implement more sophisticated technologies.

Increasingly, justice system leaders are being asked to develop justice information privacy policy for new technologies without the benefit of established law, regulation, or policy precedent. In developing what is often 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, Public Access Guideline, 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 21st Century.

Purpose of this Document:

The purpose of this document is to:

1. Describe the importance and the process of undertaking a Privacy Impact Assessment.
2. Develop a series of questions to assess privacy risks in state, local, and tribal justice information systems.
3. Develop a process to assist state, local, and tribal governments in addressing privacy risks associated with justice information systems.

Introduction:

Key players in the justice community, from law enforcement, to prosecution and defense, through the courts and correctional institutions, to probation and parole services, are using today's information technologies to improve the management of information in their daily operations. As the implementation of electronic information collection and sharing capabilities increases, so does public and governmental concern over the use, or potential misuse, of personal information contained in these systems.[5] Therefore, in addition to enhancing agency efficiency, managing privacy must be a priority of any information technology system in the justice sphere.

In response to the need to address privacy in justice information systems, the United States Department of Justice, Office of Justice Programs (OJP) in cooperation with the Office of the Ontario Information and Privacy Commissioner (IPC) and a National Criminal Justice Association (NCJA) state, local, and tribal practitioner task force, has produced a set of privacy tools for state, local, and tribal governments. The first tool is the Privacy Design Principles for Integrated Justice Systems (Privacy Design Principles).[6] The Privacy Design Principles, based on fair information practices adopted by the European Community, are intended to assist state, local, and tribal governments in developing privacy policy surrounding the electronic collection, use, and dissemination of justice information.

The second tool is the Public Access Guideline for Justice Information Systems (Public Access Guideline).[7] The Public Access Guideline discusses issues justice agencies face in maintaining an open justice system while protecting individual privacy. The Guideline discusses the effect of new technologies on traditional public access policies and offers a model for developing public access policy for electronic justice systems. The Guideline is intended to assist state, local, and tribal justice agencies in developing public access policy that can be used in planning and design of their information systems and as part of their privacy impact assessments.

The third tool is the Privacy Impact Assessment for Justice Information Systems (PIA) contained in this document. The PIA is modeled after a privacy impact assessment developed for government systems by the Ontario Management Board Secretariat, Ontario, Canada and an impact assessment for federal criminal justice systems developed by the United States Federal Bureau of Investigation.[8] The Privacy Impact Assessment for Justice Information Systems is based on the eight Privacy Design Principles and is intended to assist state, local, and tribal governments in implementing and using the privacy protections contemplated by the Design Principles and the Public Access Guideline.

What is information privacy?

"Privacy" is described as the inter-related 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 the subject of the Privacy Design Principles, Public Access Guideline, and the Privacy Impact Assessment for Justice Information Systems. This type of privacy is described as when, how, and to what extent you share personal information about yourself. The concept of information privacy is sometimes lumped together with terms such as confidentiality and security. The terms are not synonymous, however.

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 is in this sense that privacy is much broader than confidentiality. It entails restrictions on a wide range of activities relating to personal information: its collection, use, retention and disclosure.

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." 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.[9] 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, enhance privacy; while these two concepts are complementary, they are not the same. Simply focusing on security is not enough even though it is an essential component of protecting privacy.

Why is information privacy policy important in the justice community?

The use, or potential misuse, of personal information in the justice system can have dramatic consequences for individuals and their families. For example, in Ohio, a man's social security number was accidently associated with another individual's criminal history record. 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 an individual who has a damaging criminal record.[10]

Additionally, justice agencies experience tension between delivering public safety and justice services and protecting the information privacy rights of individuals. The justice system investigates and resolves questions of criminal guilt or innocense and civil conflicts. In order to effectively carry out this mandate, justice system agencies must collect and use personally identifiable information. Often this highly sensitive information must be collected and used without notice to or consent of an individual. Information collection and use applies not only to defendants or civil parties, but to their families, victims, witnesses, and others who participate in the justice process (e.g. jurors).

Therefore, to be effective, while remaining protective, justice agencies must carefully develop information privacy policies and assess the privacy impact of their information management systems.

What information privacy law and policies exist?

Historically, questions surrounding individuals' information privacy have been considered in many areas including medical, financial, educational, and consumer data.[11] Issues surrounding collection, use, and sharing of personal information have also been examined in the justice system, but have tended to focus on regulations and guidelines governing the criminal history record, information collected in research or for statistical purposes, criminal intelligence systems, and juvenile justice record keeping.[12]

Today's information technology has expanded electronic information sharing capabilities between the traditional justice agencies (law enforcement, prosecution, defense, courts, corrections, and probation and parole) and between these agencies and affiliated agencies, such as education, health, social services, and transportation. These expanded information sharing capabilities are giving rise to a new era in privacy policy.[13] The purpose of the Privacy Design Principles, Public Access Guideline, and the Privacy Impact Assessment for Justice Information Systems is to address privacy concerns associated with new and emerging information access, collection, use, storage, and dissemination capabilities of integrated justice information systems.

What is the trend of information technology in the justice community?

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.

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 National Criminal

Justice Association and the Search Group, Inc. developed a definition of integrated justice systems that has been adopted by OJP and its counterparts. As it is 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 integration of justice systems has grown from the desire 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 paper work, quick information capturing, broad transmittal and access capabilities, improved information quality, and reduced long-term costs.

How can privacy policy and impact assessments be implemented in state, local, and tribal justice information systems?

Jurisdictions seeking to protect privacy while improving justice information sharing capabilities can use the Privacy Design Principles, Public Access Guideline, and the Privacy Impact Assessment to assist them in forming privacy policy and procedures. The Privacy Design Principles should be discussed in the initial design of any agency information management system and at the initial design stages of any integrated information architecture. Used in this way, the principles are the first step to ensuring that the personal privacy of the suspected, accused, convicted, and acquitted, as well as victims, witnesses, and their families are managed effectively by the justice system.

The second step is to do a special review of how public access to information contained in the system may affect individual privacy and to assure that an appropriate public access policy is created and implemented. The third step is to conduct a privacy impact assessment. In short, the impact assessment acts as a privacy litmus test from the conceptual stage, through implementation, to the ongoing operation of an agency's information management system or an integrated justice system. The Privacy Impact Assessment ensures that agreed upon privacy policies, as well as governing law and regulation are implemented effectively, and that the policies and laws are affording the desired privacy protections.

Planning and implementation of integrated justice information systems is well underway in many state, local, and tribal jurisdictions. In addition, it is common to have one or more existing, or legacy, systems becoming part of a new integrated justice architecture, or becoming web or access enabled. These existing systems should not be immune from privacy review. The Privacy Impact Assessment, though ideally used in the first stages of planning and designing justice information systems, may also be used to assess privacy impacts of existing systems.

Getting Started on a Privacy Impact Assessment:

What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (PIA) is a process used to evaluate privacy implications of information systems. The process described in this document 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 developing an information flow map, applying a set of privacy questions to the information flow, identifying risks, and developing a solution to these privacy risks.

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

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;

2. a privacy analysis of the information flow that examines whether agreed upon privacy principles are adhered to, whether there is technical compliance 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 objective and goals of a Justice System Privacy Impact Assessment?

The objective of the PIA is to assist justice practitioners in identifying and addressing information privacy when planning, developing, implementing, and operating individual agency information management systems 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:
  - 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 Justice System Privacy Impact Assessment needed?

Relevance

A PIA is relevant where 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.

Personal information[14] 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;
- name, address, telephone number, fingerprints, blood type, or DNA;

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 multi-purpose identifiers (e.g. state identification numbers "SIDs") or biometrics;
- development and implementation of system integration policy and technologies that promote inter-agency 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 inter-agency 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 privacy considerations at the concept stage to detailed assessment at the system development and acquisition stage. 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 Privacy Impact Assessment?

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 these 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"[15] for the justice agency or integrated system. The information steward will be guided jurisdictionally applicable law or regulation, and may look to sources of policy guidance, such as the Privacy Design Principles for an Integrated Justice System.

The information steward should be 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 arms length, rather than from the inside out.

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 body, must ensure that:

- privacy law and policy is implemented appropriately;
- law and policy is actually affording the anticipated privacy protections.

To accomplish this mandate, the information steward may chose to appoint a privacy project manager (PPM)[16] to monitor privacy concerns during development, implementation, and operation of the integrated system.[17]

For example, at the outset of the integrated system design, the PPM[18] 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[19] ;
  - develop an agreement of a "baseline standard"[20] 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 inter-agency information sharing;
- provide 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 this document.

Assessing Privacy Risk

What is Risk?

The Privacy Impact Assessment 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.

First, is the risk to citizens involving their personal information, how it is used, and the propensity for individual harm from inappropriate use. As discussed in the Privacy Design Principles[21] and Public Access Guideline, 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.

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 integrated justice associated with failing to consider privacy implications of a justice information system 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;
- loss of 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;
- possible liability at the personal or agency level;
- underestimating privacy requirements such that systems need to be redesigned or retrofitted late in the development 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 tightly 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:

Authentication: definitively identifies individuals before they are allowed to request information resources;

Access control: permits individuals to access only those information resources they have been explicitly given permission to use;

Confidentiality: protects data from disclosure to unauthorized individuals;

Non-repudiation: verifies that transactions occurred, prevents one party from refuting the transaction to a second party;

Integrity: protects data from unauthorized modification or destruction;

Availability: minimizes business process disruption caused by information availability issues;

As you can see, the first three of these security services (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 A.

These areas scratch the surface of what technologists must be concerned with 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,[22] privacy impact assessments, standards, and public education.

The Privacy Impact Assessment for Justice Information Systems:

The PIA for Justice Information Systems is designed to assess privacy risk through evaluating an information system's use of the Privacy Design Principles, 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 the Privacy Design Principles for an Integrated Justice System working paper.[23] 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.[24]

Preparing the Privacy Impact Assessment for Justice Information Systems

Overview of the process

As noted above, 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 these steps.

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 PIA includes all three stages (information flow map, privacy analysis, and risk analysis), each stage 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 stage;

- 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.

Step One: Mapping the Information Flow

Mapping the information flow requires developing a decision tree (see example page 29) to understand the decision points relating to information collection, use, and dissemination within an agency system or an integrated justice system. This type of information flow mapping regularly takes place in designing justice agency or integrated justice information systems. The only addition to this 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.

At each decision point, policy makers, working in cooperation with the PPM and system designers, must determine the "attributes" of each "piece of information." A piece of information, for example, would be a person's income. The attributes refer to the nature or sensitivity of the information that is being disclosed and the conditions placed on the information regarding the its collection, use, dissemination, retention, and expungement.

For example, a piece of information can be classified as highly sensitive, sensitive, or non-sensitive. To help to determine how, when, and with whom the information may be disclosed or used, 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

These classifications may be applied to each piece of information as it is collected, used by agencies, and disclosed throughout the justice system. These classifications my also be applied to determining if pieces of information are disclosed <u>outside</u> the justice system, e.g. between law enforcement and education agencies, or the courts and the public.

In many cases where agency information management systems or integrated justice systems have been or are being designed, the information flow maps may have been created by system developers, albeit not from a privacy perspective. The existing information flow maps may provide a good basis from which to develop privacy attributes for individual pieces of information. In addition, where such information flow maps do exist, it is important to consult these maps, so that the privacy impact assessment mapping does not contradict or deviate from the information flows of the original system design.

The following is an example of the first step in mapping out the collection, use, and disclosure decision points of information flows in a traditional criminal justice system context. Please note that this is one example of a data flow model. Agency players 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.

Completing the information flows, as shown above, allows a PPM and his or her project team to map out where collection, use, and disclosure decisions occur and where the application of information attributes must be made. Additionally, the information flow-chart for each agency and for the integrated system helps to identify areas where additional rules may be needed to implement privacy policy for the collection, access, use, and disclosure of personal information.

Mapping out 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 offence. Ensuring integrity (accuracy) of the information within the various 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 inter-agency information exchange, the model can be reused. For example, the information flow model for the criminal justice system above needs only a few changes to be applicable for 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 as described below.

The next step in the mapping process is to focus on the specific pieces of information, or data elements, and apply privacy attributes to each. PPMs may find that many of the collection and information disclosure rules (attributes) already exist in the justice system. Where attributes have not been defined, policy decision makers (information steward) 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). It also has the content of the statement. At an appropriate time in the justice process, the header information can be disclosed to the accused. However, the content of the statement would have far more restricted circulation.

To assist policy makers in developing "workable" privacy attributes for sensitive information, this document suggests information categories such as in the traffic light metaphor above; "red, yellow, or green" information.

For example, take 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 in the justice system process. As well, an information attribute table would set out the privacy conditions of that data element. In this case, the income information would most likely be classified as "yellow" information: information that is neither denied to other agencies, nor given, pro forma, to other agencies. Before determining exactly how the income of the arrestee is disclosed, the policy makers must determine who should have appropriate access to this piece of information. For example, a disclosure rule could be that personal information related to financial information is restricted to access by pre-trial personnel and judges to determine applicability for indigent defense services, rather than fully accessible by other court staff.

An example of "green" 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. However, broader disclosure to other government agencies, the private sector, or the public may mean looking at this information with different privacy objectives. For example, if the information is contemplated for release outside the justice system, this information may fall into the "yellow" category where its disclosure should be more carefully considered.[25]

Often, a preferred default policy of privacy practitioners is the presumption of privacy on all the information unless the disclosure conditions identified for a piece of information or a set of information are met. This applies the most protective privacy policy to all information, allowing certain pieces to be used if disclosure conditions are met.

The opposite approach is to allow disclosure of all data, tagging certain pieces or types of information that require a higher dissemination threshold. This applies the "green light" attribute to all information, allowing certain identified pieces or types of information to be non-disclosed. Jurisdictions must determine for themselves which approach provides workable, appropriate privacy protection, while allowing for system functionality.

Finally, the information flow map is provided as a tool to go beyond the Privacy Design Principles and 'drill down' into the information flows of agency and integrated justice systems. This type of analysis is necessary to answering the following questionnaires that are key to the privacy impact assessment.

Step Two: Component Agency Privacy Analysis Question and Answer

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 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:

a. Is the information in the system being compiled for the purposes of identifying individual criminal offenders and alleged offenders and 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)?

    1. Is this compilation considered the "official criminal history record" for state reporting purposes?

    2. Is the system collecting this information funded in whole or in part with federal government funds?

        i If so, does the system comply with the requirements of 28 C.F.R. part 20?

b. Is information in the system being compiled for the purpose of criminal intelligence investigation of individuals, including reports of informants and investigators?

    1. 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?

    2. Is the system collecting this information funded in whole or in part with federal government funds?

    i. If so, does the system comply with the requirements of 28 C.F.R. part 23?

c. Does information in the system include information on juvenile offenders or suspected offenders, or their families?

1. 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?

d. Does the information in the system include information required by statute to be maintained and used for research or statistical purposes?

1. 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?

i If so, does the system comply with the requirements of 28 C.F.R. part 22?

e. 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?

f Has your agency undertaken a specific effort to identify any relevant law, regulation, or policy relating to the information mentioned above?

g. 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 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. Agency's completing their PIAs should seek legal counsel within their jurisdictions to ensure these requirements are implemented appropriately.

Privacy Design Principle Q&A

1. Are you following the Purpose Specification Principle?

a. Is there a written purpose statement for the system collecting personal information?

1. Set out the purpose statement(s).

b. Is the written statement(s) publicly available prior to the time of information collection?

c. If available publicly, is the written statement(s) set out in the organization's collection form(s) in a comprehensive and prominent manner?

d. Is the written purpose statement periodically reviewed and updated?

e. Has a clear relationship been established between the personal information being collected and the system's functional purpose and operational requirements?

f. Is the personal information collected pertinent to the stated purposes for which the information is to be used?

g. Are there limits on subsequent (secondary) use of the information?

h. Are there limits on third-party or private sector partnerships or relationships where personal information is or will be disclosed?

i If not, do these secondary use(s) conform to the stated purpose?

j Does the system have mechanisms to inform data subjects of third party, secondary use disclosure?

2. <u>Are you following the Collection Limitation Principle?</u>

a. Are you limiting the collection of personal information to the system's identifiable purpose?

b. Is personal information obtained by lawful and fair means?

c. Where appropriate, is personal information obtained with the knowledge or consent of the data subject?

d. 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. <u>Are you following the Data Quality Principle?</u>

a. Is the personal information collected for stated purposes:

1. accurate?

2. complete?

3. current?

4. verified?

b. Is the system collecting "original" or "new" information?

c. Is the personal information collected directly from the data subject?

d. Do you have a procedure for tracking:

1. requests to modify information?
2. determinations of the requests to modify?
3. modifications made based on the requests?
4. the source of the information that is used to modify the information?
5. when the last modification occurred?

e. Is there a procedure to provide notice of correction (modification) to:

1. subsequent justice system users?
2. third parties (secondary users)?

f Where appropriate, does the data subject have some means of accessing the information to ensure it is accurate and up to date?

g. 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?

h. When a person challenges the accuracy of a record, is he/she provided with information about:

1. the agency personnel responsible for the record?
2. administrative procedures governing inquiries?

i Do you have procedures for addressing:

1. data management issues?
2. record retention issues?

4. Are you following the Use Limitation Principle?

a. Is the use of the information relevant to the purpose for which the system is being designed (operated)?

b. Does the system limit the use or disclosure of personal information to the articulated purpose(s) in accordance with Principle 1?

c. Are any secondary uses limited to those:

1. with the consent of the data subject?

2. by the authority of law?

3. for the safety of the community (including victims and witnesses)?

4. pursuant to a public access policy?

d. If personal identifiers are used for purposes of linking across multiple databases, do these multiple databases have consistent purposes?

e. Do you have procedures to ensure a 'record of use' is maintained?

f. Is the 'record of use' attached to each piece of personal information?

g. Will the system prevent the derivation of new information or creation of previously unavailable information about an individual through aggregation from the information collected?

h. Is an agency or the system itself prevented from making determinations about individuals that would not be possible without the new information (referred to in 'g')?

i Do you have procedures in place to verify the new information (see 'g') for:

1. relevancy?

2. accuracy?

j Do you prohibit personal information from being sold or released under public access policy to private information gatherers (resellers)?

k. If not, is the released information "publically accessible"[26] pursuant to your public access policy?

l 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?

m. Does the system have mechanisms to inform data subjects of third party (public), secondary use disclosure?

5. <u>Are you following the Security Safeguards Principle?</u>

a. Does the system have security safeguards?

b. Have you documented the system's security safeguards that protect personal information against:

1. loss?

2. unauthorized access?

3. destruction?

4. use?

5. modification?

6. disclosure?

c. Are security safeguards provided according to:

1. sensitivity of the information?

2. risks to all involved parties?

d. Has there been an expert security review?

e. Have staff been trained in requirements and ethics for protecting personal information?

f Is staff aware of policies and consequences regarding breeches of security?

g. Are there controls in place over the processes that grant authorization to modify (add or delete) personal information?

h. Does the system allow user access and changes to personal information to be audited by:

1. date?

2. user identification?

i Are user accounts, access rights and security authorizations controlled and recorded by accountable systems or records management process?

j Are access rights only provided to users who actually require access for the systems stated purposes?

k. Are there contingency plans and mechanisms in place to identify:

1. security breaches?

2. disclosures of personal information in error?

l Are there mechanisms in place to communicate violations or errors to subsequent users to mitigate collateral risks?

m. Are there adequate, ongoing resources budgeted in maintenance plans for security upgrades with measurable performance indicators?

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

6. Are you following the Openness Principle ?

a. 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)?

b. Does openness include public access to the management practices of the information?

c. Does openness require clear communication to affected individuals where justice records are requested, sold, or released to third parties?

d. Does openness require clear communication to affected individuals where justice records are requested, sold, or released under the systems public access policy?

7. Are you following the Individual Participation Principle?

a. 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?

b. Does the system allow an individual to have communicated to him or her information relating to him or her:

1. within a reasonable time?

2. at a charge, if any, that is not excessive?

3. in a reasonable manner?

4. in a form that is readily intelligible to him/her?

c. Does the system provide for an explanation if a request is denied?

d. Is an individual able to challenge a denial?

e. 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?

a. Is there an individual or agency body who is accountable for complying with measures that give effect to:

1. the Privacy Design Principles?

2. the public access policy?

3. applicable law or regulation?

Step Three: Assessing the Component Agency Answers

After fully answering each of the questions above, the answers to questions 1-8 should be compared to the objectives of each corresponding Privacy Design Principle contained in the companion document, Privacy Design Principles for an Integrated Justice System.

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 public's interest in and growing concern about information privacy.[27] 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 noted to the integrated system PPM and should receive additional consideration.

Step Four: Integrated System Privacy Analysis Question and Answer

The integrated system PPM should answer the following questions, taking into consideration the results of the component agency PIAs:

1. <u>Does the integrated justice system follow the Purpose Specification Principle?</u>

a. Are the purpose statements of the component agencies' systems compatible?

b. 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?

a. Are the collection policies of the component agencies' systems compatible?

b. 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?

c. Have you determined which agency is responsible for data quality of the collected information (see below)?

d. 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?

a. Are the data quality assessments of the component agencies compatible?

b. If they are not compatible, can you identify the weakest "link(s) in the chain?"

c. 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?

a. Are the use limitation policies of the component agencies compatible?

b. Are the public access policies if the component agencies compatible?

c. Is information "publically accessible" under one component's public access policy "publically accessible" under all the other's public access policies?

d. Does the integrated system have mechanisms to inform data subjects of third party (public), secondary use disclosure?

e. Does the use of information throughout the integrated system derive new information (such as a compilation)?

f. Are the component agencies only using this information according to the agreed purpose of the integrated system?

g. Are component agencies aware that their decision-making may be based on “new” (aggregated) information?

h. Do the component agencies have safeguards, or review procedures, at these decision-making points?

i Does the integrated system limit the release of this new information to secondary sources such as:

1. the public?

2. private industry?

3. the media?

4. information resellers?

5. <u>Does the integrated justice system follow the Security Principle?</u>

a. Are security levels of the component agencies’ systems compatible?

b. Can you identify the weakest “link(s) in the security chain” in the integrated system?

c. Do you have a procedure in place to address (improve) security at this weakest point(s)?

d. Do you have procedures in place that allow you to improve (upgrade) security while still maintaining the inter-agency flow of information in the integrated system?

6. <u>Does the integrated justice system follow the Openness Principle?</u>

a. Are the openness standards of the component agencies compatible?

b. Are there openness standards for the integrated system itself?

c. Does the integrated system have a general policy of openness about developments, practices and policies with respect to the <u>management</u> of personal information (apart from the actual information)?

d. Does openness include public access to the management practices for the information?

e. Does openness require clear communication to affected individuals if agencies within the integrated system sell or release personal information to third parties?

f 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?

a. Are the individual access policies of the component agencies compatible?

b. Are the individual challenge procedures of the component agencies comparable?

c. 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?

a. 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?

b. 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?

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?

c. 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?

Step Five: Assessing the Integrated Justice System Answers

As in the component agency assessments, the answers to questions 1-8 should be compared to the objectives of each corresponding Privacy Design Principle contained in the companion document, Privacy Design Principles for an Integrated Justice System. 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 noted to the integrated system information steward and should receive additional consideration, as described below.

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 in 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 steward. 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 dialogue 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 dialogue during the planning phase of justice information system projects, and, where existing systems are involved, as soon as privacy policies and procedures are developed.

Conclusion:

Information systems are integral to the operation of the justice enterprise. Information collection, access, use, and dissemination practices of the past are changing as agencies seek to implement more sophisticated technologies.

Increasingly, justice system leaders are being asked to develop justice information privacy policy for new technologies without the benefit of established law, regulation, or policy precedent. In developing what is often 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.

The Privacy Impact Assessment for Justice Information Systems is designed as the third in a series of three policy tools for state, local, and tribal justice agencies. The PIA should be used in conjunction with its companion documents, Privacy Design Principles for an Integrated Justice System and the Public Access Guideline for Justice Information Systems.

Tools such as the Privacy Design Principles, Pubic Access Guideline, 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 21st Century.

Appendix 'A'

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 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. Fiber optic 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 fiber optic 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 will help 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 each user, these certificates can then be used as "tickets" to gain access to authorized files and directories. System operator should chose 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 multi-level, secure database products to ensure the safety of data. Multi-level 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 'B'

The Privacy Impact Assessment for Justice Information Systems has been prepared in a joint effort by state, local, and tribal justice leaders, the United States Department of Justice's Office of Justice Programs, Justice Management Division, and Federal Bureau of Investigation, the National Criminal Justice Association, and the Office of the Ontario, Canada Information and Privacy Commissioner.

A special thanks to the original drafters and reviewers of this document who participated in the June 8-9, 2000 Privacy Impact Assessment Workshop in Chicago, Illinois:

Brian Beamish

Director of Policy & Compliance, Ontario Information and Privacy Commission

Sol Bermann

Legal Project Manager, Technology Policy Group, Ohio Supercomputer Center

Christopher Bosch

Division Chief, Kansas City Missouri Fire Department

John G. Boufford

President, E-Privacy Management Systems

David Boyer

Information Technology Advisor, OJP, ACS Defense, Inc.

Timothy Burns

Justice Information Analyst, Pinellas County Dept. of Justice Coordination

Emily Busse

Staff Associate, National Criminal Justice Association

Dr. Ann Cavoukian

Commissioner, Ontario Information and Privacy Commission

Patricia F.S. Cogswell

Attorney, U.S. Dept. of Justice, Justice Management Division

Dr. Hugh Collins

Judicial Administrator, Supreme Court of Louisiana

Ed Crockett

Information Systems Manager, Kentucky Administrative Office of the Courts

Cabell Cropper

Executive Director, National Criminal Justice Association

Gregory Frost

Policy Planner, Tallahassee Police Department

Anne E. Gardner

Attorney-Advisor, U.S. Dept. of Justice, Office of Justice Programs

Kimberly Glenn

Information Services Manager, San Diego Police Department

Lee Guice

Staff Attorney, Kentucky Administrative Office of the Courts

Michael Gurski

Policy & Technology Officer, Ontario Information and Privacy Commission

Beth Haley

Attorney-Advisor, Administrative Law Unit, Federal Bureau of Investigation

Hunter Hurst

Director, National Center for Juvenile Justice

Paul F. Kendall

General Counsel, U.S. Dept. of Justice, Office of Justice Programs

Nobel Kennamer

Special Assistant, Los Angeles County Public Defender

Kent Koehler

QA/Tech Support Coordinator, Sedgwick County Emergency Communications

Luli Landis

Director of Marketing and Communications, Miami-Dade Country Clerks Office

Kent Markus

Professor, Capitol University Law School

Jay Maxwell

Chief Operating Officer, American Assn. of Motor Vehicle Administrators

Jim Peschong

Assistant Chief, Lincoln, Nebraska Police Department

Janet Quist

Director, Public Safety Programs, Public Technology, Inc.

Jiroko Rosales

Director, Court and Detention Services, City of Dallas

Randy Ross

Executive Director, Indian Center, Inc.

Dr. Peter Scharf

Co-Director, Center for Society, Law, and Justice, University of New Orleans

Christian Selch

Project Manager, Ohio Supreme Court

Julie Spence-Gefke

Juvenile Justice Consultant

Robert A. Stellingworth

Co-Director, Center for Society, Law, and Justice, University of New Orleans

Teri Sullivan

Director, Davidson County, Tennessee Justice Information System

Bob Wessels

Court Manager, Harris County, Texas

Carl Wicklund

Executive Director, American Probation and Parole Association

John Woulds

Director of Operations, The Data Protection Registrar, United Kingdom

[1] *See,* Opinion Research Corporation Int'l, 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).

[2] 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.

[3] The Privacy Design Principles can be obtained through the Office of Justice Programs at www.ojp.usdoj.gov/integratedjustice/ or at 202-514-3719.

[4] The Public Access Guideline can be obtained through the Office of Justice Programs at www.ojp.usdoj.gov/integratedjustice/ or at 202-514-3719.

[5] *See,* Opinion Research Corporation Int'l, 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).

[6] The document is entitled, Privacy Design Principles for an Integrated Justice System, and is available through the Office of Justice Programs at www.ojp.usdoj.gov/integratedjustice/ or 202-514-3719.

[7] The Public Access Guideline can be obtained through the Office of Justice Programs at www.ojp.usdoj.gov/integratedjustice/ or at 202-514-3719.

[8] These documents are available on-line at http://www.gov.on.ca/MBS/english/fip/pia/ and ________ respectively.

[9] As discussed in the Public Access Guideline, information can be categorized as "discloseable", "non-discloseable," or "publically accessible." Confidential information covers that information which is discloseable or non-discloseable, because it requires limiting access according to the requester's authority to receive the information. Publically accessible information does not carry this limitation.

[10] *Stolen Identity: Could it happen to you?* (MSNBC television broadcast, April 18, 2000), http://www.msnbc.com/news/397082.asp.

[11] *See*, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C.A. § 201 note, § 1320d (Supp. 2000); Family Educational Rights and Privacy Act of 1974, 20 U.S.C.A. § 1232g (2000); 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, please see proposed privacy acts: Internet Consumer Information Protection Act, H.R. 2882, 106th Cong. (1999),

and the Online Privacy Protection Act of 1999, S.809, 106th Cong. All federal statutes can be accessed at www.washlaw.edu. All public laws and bills can be accessed at http://rs9.loc.gov/home/thomas.html.

[12] *See, e.g.,* 28 C.F.R. Part 20, 22, 23 (1999).

[13] 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, 21st ANNUAL INTERNATIONAL CONFERENCE ON DATA PROTECTION AND INFORMATION PRIVACY, Hong Kong (Sept. 1999), http://www.pco.org.hk/conproceed.html.

[14] 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, Pub. L. 105-277 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, and proposed legislation: The Online Privacy Protection Act (S. 809).

[15] See Privacy Design Principles for Integrated Justice Systems, Design Principle 8 for a full explanation of the Accountability Principle. This document is available through the Office of Justice Programs at www.ojp.usdoj.gov/integratedjustice/ or 202-514-3719.

[16] 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.

[17] If the PIA is being undertaken by a single agency, the role 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 the privacy any resulting privacy concerns.

[18] 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 that the privacy impact assessment is completed.

[19] 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 owner's requirements.

[20] The baseline privacy standard is that level of privacy protection to 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.”

[21] See Privacy Design Principles for Integrated Justice Systems, Design Principle 2 (Collection) and Design Principle 8 (Openness).

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

[23] This document is available through the Office of Justice Programs at www.ojp.usdoj.gov/integratedjustice/ or 202-514-3719.

[24] 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, P.O. Box 28577, Providence, RI 02908, 401-274-7861, 5101719@mcimail.com.

[25] See the Public Access Guideline for assistance on developing public access policy for these types of disclosures.

[26] “Publically accessible,” meaning, that which by law or tradition is readily available to non-justice organizations or individuals without the need to state an authorized purpose.

[27] *See,* Opinion Research Corporation Int’l, 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).