Global Justice Information Sharing Initiative

United States Department of Justice

Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives

This *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives* was prepared by SEARCH, The National Consortium for Justice Information and Statistics; Francis X. Aumand III, Chairman; and Ronald P. Hawley, Executive Director. The project directors were Kelly J. Peters, Deputy Executive Director; and Owen M. Greenspan, Director, Law and Policy. Ms. Peters and Eric C. Johnson, Justice Information Services Specialist, prepared the Guide. Consultant Laurie Beyer-Kropuenske contributed to the guide. SEARCH collaborated with the Global Privacy and Information Quality Working Group (GPIQWG) of the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global). Global serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Representatives from the DOJ's Privacy Office and the U.S. Department of Homeland Security's Privacy Office and Civil Rights and Civil Liberties Office also contributed to this assessment tool.

This project was supported by Grant No. 2005-NC-BX-K171, awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the authors and do not represent the official position or policies of the United States Department of Justice.

Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives

Privacy Policy Technical Assistance Providers and Partnership Offices

Global Privacy and Information Quality Working Group
http://www.it.ojp.gov/topic.jsp?topic_id=55

Global Security Working Group
http://www.it.ojp.gov/topic.jsp?topic_id=58

Institute for Intergovernmental Research
http://www.iir.com/

The Justice Management Institute
http://www.jmijustice.org/Home/PublicWeb

National Center for State Courts
http://www.ncsconline.org/

SEARCH, The National Consortium for Justice Information and Statistics
http://www.search.org

U.S. Department of Homeland Security, Privacy Office
http://www.dhs.gov/privacy

U.S. Department of Homeland Security, Office for Civil Rights and Civil Liberties
http://www.dhs.gov/xabout/structure/editorial_0371.shtm

U.S. Department of Justice, Bureau of Justice Assistance
http://www.ojp.usdoj.gov/BJA/

U.S. Department of Justice, Privacy and Civil Liberties Office
http://www.usdoj.gov/pclo/

See Appendix E for specific privacy tools, documents, and resources offered by these partners.

Privacy, Civil Rights, and Civil Liberties

This *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives* allows justice practitioners to examine the privacy implications of their information systems and information-sharing collaborations so they can design and implement policies to address vulnerabilities identified through the assessment process.

Recent efforts to support privacy policy development frequently extend their focus to include civil rights and civil liberties as components in the privacy environment.

Civil rights imply a government role in ensuring that every citizen receives equal protection under the law and has equal opportunities to enjoy the privileges of citizenship.

Civil liberties restrict the government from interfering with a citizen's right to free speech, religious preference, and other choices and opportunities spelled out in the Bill of Rights.

The Global Privacy and Information Quality Working Group provides resources accessible online to assist justice agencies interested in considering the civil rights and liberties implications of their information collection and sharing initiatives.

Products include:

- *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*,
- *Privacy, Civil Liberties and Information Quality Policy Development for the Justice Decision Maker* and
- *Privacy, Civil Rights and Civil Liberties Policy Templates for Justice Information Systems*.

Please visit the Global Privacy and Information Quality Working Group Web site for more information on the working group and on the products it produces.

Information may be the wild card in the justice enterprise deck.

Its expanded utility, made possible in large part by advances in information technology, strengthens public safety and supports the development and growth of state, local, and regional fusion centers[1] and other important data-sharing collaborations.

However, its inappropriate or reckless use may irreparably damage reputations, threaten individual liberty, place personal safety at risk, or deny individuals access to some of life's most basic necessities such as employment, housing, and education.

Greater information-sharing capabilities and opportunities are accompanied by equally greater responsibilities for protecting the privacy of the information being used and exchanged.

Information is maximized to its full potential only when it is used in the most responsible manner possible, with carefully designed privacy protections that recognize not only the tremendous benefits that information sharing can provide, but also the damages that can occur when information is used and exchanged in a manner that conflicts with common expectations of privacy and confidentiality.

Justice agencies recognize the value of information technology (IT) and improved data sharing. Agencies strive to incorporate the most sophisticated technologies possible, as well as to devise policies and procedures that allow their operation in sensitive justice domain environs.

To assist with this critical but often daunting task, the U.S. Department of Justice (DOJ), via the Global Justice Information Sharing Initiative (Global),[2] is creating tools and resources to help state, local, and tribal practitioners develop privacy policies. **This Guide adds another resource to that toolkit, providing a methodology for state, local, and tribal information-sharing initiatives to analyze risks related to ensuring the privacy of the personally identifiable data that they collect**. This risk assessment—more commonly known as a **privacy impact assessment or PIA**—is a crucial first step in successful privacy policy development.

Familiarity with the following three terms will be helpful as you review this guide. (Appendix F provides a more extensive glossary.)

Personally Identifiable Information (PII): Information from which an individual can be uniquely identified, such as name, address, date of birth, and social security number, and any information linked or linkable to the individual.

Privacy Impact Assessment (PIA): A series of questions that evaluate the processes through which personally identifiable information is collected, stored, protected, shared, and managed by an electronic information system or online collection application.

Privacy Policy: A legally binding notice of how an agency handles an information contributor's personal data. The privacy policy should contain details about collecting information and secondary uses of data, including how information is shared with third parties and who those third parties are.

1 A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the *National Criminal Intelligence Sharing Plan* (NCISP). Source: **http://www.it.ojp.gov/topic.jsp?topic_id=209**.

2 The Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support the broad-scale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment. For more information, see **http://www.it.ojp.gov/topic.jsp?topic_id=8**.

Background

Now more than ever, data and information are among the most important tools in fighting crime and administering justice. Each day, critical decisions about detainment, sentencing, arrest, and adjudication are based on information that is collected, shared, accessed, and collated with other pieces and types of information.

A PIA is just one piece of the privacy policy puzzle.

Step 1: Analyze Your Information Systems and Information Sharing Initiative, and Conduct the Privacy Threshold Analysis

Step 2: Identify and Analyze Information Exchanges

Step 3: Conduct the PIA

Step 4: Develop Privacy Policy

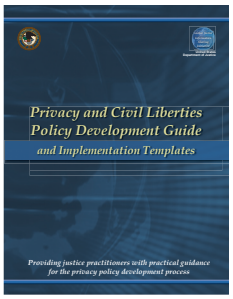
Beyond these activities, fusion centers collect, analyze, and collate data from a wide array of sources and databases into intelligence products that help jurisdictions predict, prevent, prepare for, and respond to a variety of criminal and terrorist activities, natural disasters, and other public safety events. These information-sharing activities are essential to the safety of our communities, citizens, and country.

Following numerous media reports of hackers, lost data and incidents where personal information is exposed to potential wrongdoers (see Appendix B for recent examples), surveys find that America's interest in privacy protections is growing.

Concurrently, justice agencies leverage limited resources to obtain the most powerful information technologies available. These agencies cannot risk their significant technological investments, loss of access to vital data, and the impact of negative publicity by not pursuing the strongest privacy protections possible. This is particularly relevant considering the constant pressure from lawmakers and the public to effectively gather, analyze, and use information to fight crime and to help prevent future terrorist attacks.

Information sharing across new and disparate databases and among or between independent organizations requires a structured methodology for addressing privacy and for creating effective policies to protect it. This is particularly important when multiple law enforcement organizations participating in an interjurisdictional information-collecting collaboration each maintain policies reflecting their own processes and philosophies for data collection, storage, and use.

These factors convinced members of Global, the Bureau of Justice Assistance (BJA), the DOJ, and other partners to reenergize efforts to develop practical tools and resources, and to identify best practices in the privacy realm, to support privacy policy development among state, local, and tribal justice agencies.



Their first step was to develop the Global Justice Information Sharing Initiative's *Privacy Policy Development Guide and Implementation Templates*, produced by Global's Privacy and Information Quality Working Group, which was released in 2006 and updated in 2008.[3] The Development Guide, a hands-on resource that leads users through specific steps in developing privacy policy, is intended for justice practitioners interested in moving beyond privacy awareness into direct policy development.

The partners then formally organized technical assistance (TA) providers to aid state, local, and tribal agencies as they developed privacy policies. This TA providers group continues to develop policy development resources and tools for justice practitioners.

A PIA was one tool that BJA and the TA providers group agreed would be useful for privacy policy development—as well as a valuable instrument that TA providers could use when they work with practitioners. PIAs are required by federal law under certain circumstances for federal information systems,

3 The Development Guide was reissued in 2008 and augmented with civil liberties components to the original privacy policy instructional text. *Privacy and Civil Liberties Policy Development Guide and Implementation Templates* is available at **http://www.it.ojp.gov/documents/Privacy_Guide_Final.pdf**. This and other justice information sharing resources are listed in Appendix E.

but there are few similar mandates at the state, local, or tribal levels. **A PIA allows leaders of an information-sharing initiative to analyze privacy risks and exposures of data stored and exchanged by organizations participating in multijurisdictional information collaborations. Resulting policies specifically address these risks.**

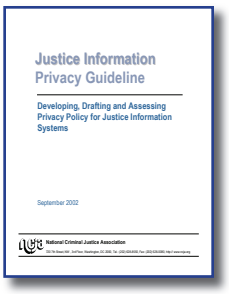
While the E-Government Act of 2002 resulted in significant federal-level privacy policy activity, particularly in PIA use for new or significantly modified IT systems, there has been little activity on the state, local, or tribal fronts in privacy policy development or PIA use to examine IT system privacy vulnerabilities.

PIAs for State, Local, and Tribal Information-Sharing Systems

This Guide builds on the work of the Global Justice Information Sharing Initiative, an understanding of current PIA use at the state, local, and tribal levels, and recent federal-level successes in PIA development.

Users should first understand the PIA's role in overall strategic planning and, specifically, in privacy policy development.

1. A governing structure of stakeholders is formed to develop a strategic information-sharing plan. Among this plan's features is a commitment to privacy policy development. The process begins by conducting a privacy threshold analysis (PTA) to determine what systems need a PIA.
2. If the PTA reveals the need for a PIA, system designers should be aware that, ideally, the PIA process begins early in system development. It should be an iterative work through the development life cycle.
3. Specific information exchanges among and between stakeholder organizations will be identified and analyzed during the strategic and tactical development of an information-sharing system. This analysis will identify information that will be exchanged, with whom, and if there are associated privacy implications.
4. The PIA process begins. The PIA poses a series of questions that help stakeholders understand the risk their system may pose to the privacy of personally identifiable information.
5. Privacy policies emerge as the result of the identification and analysis that occurs during the PIA process, generating discussion and decision-making on how to address, and mitigate if necessary, the identified privacy vulnerabilities. Even after policies are established, the PIA calls for the implementation of policy controls and ongoing audits.



In particular, this Guide builds upon the *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*, which was released by the National Criminal Justice Association in September 2002.[4] These privacy guidelines were developed by state, local, and tribal justice practitioners, the DOJ and associations representing justice organizations and practitioners. They provided some of the first-ever information and direction for justice agencies interested in protecting the privacy of the data they maintained—particularly as they began justice system integration—and in avoiding the negative consequences often associated with inadequate privacy considerations. We encourage review of this document for a more detailed and historical discussion of privacy policy development.

This Guide builds on that work and others to offer a user-friendly template for state, local, and tribal organizations to use in conducting a PIA. The goal is to educate stakeholders about the need for such an assessment, while providing a practical tool for conducting one.

4 Among the groups involved in the document's design were the Office of Justice Programs of the U.S. Department of Justice; the Office of the Ontario (Canada) Information and Privacy Commissioner; the National Criminal Justice Association; a broad base of other justice associations; and state, local, and tribal justice leaders. It is available at **http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/privacyguideline.pdf**.

This Guide provides the following:

- An overview of the PIA process, as outlined below.
- A PIA template based on the Fair Information Practice Principles (FIPPs)[5] that leads policy developers through appropriate privacy risk assessment questions. The template is provided as Appendix A and as a Word document tool available on the BJA Web site, **http://www.ojp.usdoj.gov/BJA/**, and the Global Web site, **http://www.it.ojp.gov/index.jsp**.
- Two methods to institutionalize the PIA process for information systems development: model legislation and a draft governor's executive order. Model legislation is provided as Appendix C, and the draft executive order as Appendix D.

What Is a PIA?

A privacy impact assessment allows agencies to adequately assess privacy risks in their information-sharing initiatives. It lays the groundwork for comprehensive and effective policies to protect information while maximizing technological infrastructures and data-sharing opportunities.

Taking a cue from Congress's E-Government Act, which requires PIAs for new or significantly modified IT systems, a PIA supports the notion that, before diving into full privacy policy development, **state, local, and tribal jurisdictions should first identify, analyze and assess the risks associated with information systems when it comes to the privacy of the data and information they store and share**. Once risks are identified and analyzed, policies can specifically address and mitigate them.

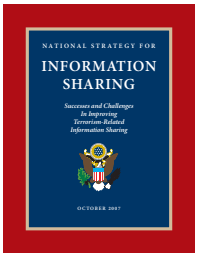
A PIA evaluates privacy implications when information systems are created or when existing systems are significantly modified. PIAs can also be conducted for existing IT systems that don't fall into either of these two categories. Routine PIA use is a cost-effective demonstration of sound public policy.

Example of Federal PIA: Potential Risk and Mitigation

The Federal Trade Commission (FTC) conducted a PIA of its Redress and Enforcement (RED) database, which is used to manage the personal information of individuals against whom the FTC has obtained judgments for violations of statutes and rules enforced by the commission.

The PIA identified the potential risk of collecting personal information, particularly social security numbers (SSNs) and employee identification numbers (EINs). To mitigate this risk, the FTC limited the collection of information to only essential data on defendants and associated persons. The FTC also did not store the personal information of victimized consumers in the RED database, and it encrypted the defendants' SSNs and EINs that it did collect so that only authorized staff could view them.

Why Is a PIA Important?



In October 2007, the White House released its *National Strategy for Information Sharing*.[6] Although focused on terror-related information, the strategy represents wise counsel if used more broadly. Protecting information privacy and associated legal rights is a foundational element. The strategy includes core principles that reflect basic privacy protections and best practices. Many parallel or duplicate the PIA process proposed here.

Information systems used by law enforcement and other justice disciplines are perhaps more closely scrutinized than other government or privately operated information systems, and are therefore held to higher standards.

5 FIPP is a general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. Different organizations and countries have their own terms for these standards. For more information, see **http://www.ftc.gov/reports/privacy3/fairinfo.shtm**.

6 Available at **http://www.whitehouse.gov/nsc/infosharing/index.html**.

Higher standards are expected for information that can deprive individuals of their personal freedom or that can put individuals such as victims and witnesses at risk. Additionally, criminal justice data are often collected without the consent of a data subject, who may be an alleged offender, a crime victim, or a witness. Greater diligence in data handling is crucial for safeguarding the interests of individuals who have little or no choice about becoming involved in the criminal justice system.

Essential to American democracy is the ability to hold government accountable for its actions through a variety of state and federal transparency laws that allow citizens to gain access to public meetings and official records.

Conducting a PIA illustrates a jurisdiction's commitment to, and thoughtful analysis of, protection of the public's information. Maintaining public trust is at the core of the PIA concept; this is particularly true for criminal justice agencies. The public must be assured that personal and confidential data will be collected and used lawfully.

There are many practical and philosophical reasons to conduct a PIA. Addressing privacy concerns early in the design process can encourage policymaker support, as well as financial support, for a system. An effective PIA process may not gain public support but is likely to stimulate healthy debate and deflate potential opposition to important information-sharing capabilities.

Failing to recognize privacy values can result in system shutdown, forced data destruction, costly modifications, implementation delays, and more restrictive legislative mandates, as well as personal and agency embarrassment.

Primarily, however, a PIA should be conducted to ensure that personal and confidential information entrusted to an agency is protected to the highest degree possible, sparing record subjects—whose interaction with the justice system is already almost assuredly causing tension—further trauma or even victimization by the improper use and exchange of their data.

The U.S. Office of Management and Budget (OMB) provides federal agencies with the following guidance for conducting PIAs in accordance with the E-Government Act of 2002.[7] The OMB recommends PIAs when agencies:

- Convert from a paper-based to an electronic system.
- Change anonymous data to non-anonymous data.
- Undertake significant system management changes.
- Adopt or alter business processes so there is significant data merging, centralization, or matching in the databases.
- Enable new public access to the systems, such as via passwords.
- Incorporate databases of information in identifiable form obtained or purchased from commercial data sources into their existing information systems.
- Work together on new interagency uses or exchanges of information in identifiable form.
- Alter business processes so there is significant new internal flow or collection of information in identifiable form.
- Alter the character of data, which means adding new information in identifiable form that raises the risks to personal privacy, such as adding health data.

7 OMB memorandum, Sept. 26, 2003 (M-03-022), titled *OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002*, is included as Appendix G.

Do You Need a PIA?

You should first conduct two fundamental analyses to determine whether your system needs a PIA:

- First, analyze your system and information-sharing initiative itself—basically by asking this simple question: "What systems might need a PIA?"
- Then, conduct a "privacy threshold analysis," also called a PTA, to determine whether your system collects personally identifiable information, also called PII.

What Systems Need a PIA?

Examine your information system(s) and information-sharing initiative itself. The question is, "What systems need a PIA?" The answers are easy: generally, *any new data system*, and especially any new information-sharing initiative, that collects PII should be subjected to a PIA as part of the planning process. In addition, *any significant modification of an existing system* should also be the subject of a PIA *if* the modifications are associated with the collection, use, access, or dissemination of PII.

Therefore, determining whether your system(s) collect personally identifiable information is the second fundamental analysis you need.

The Privacy Threshold Analysis

If in doubt as to whether a PIA is appropriate, a **privacy threshold analysis** can ascertain whether a PIA is needed for a systems upgrade or improvement. The first question is, "Does the system store, use, or otherwise maintain personally identifiable information?" If your answer is yes, consider the following:

PRIVACY THRESHOLD QUESTION 1

What information about individuals could be collected, generated, or retained?

Rationale. Creating a list of the types of personally identifiable information a system will use requires designers to appropriately consider the types of PII data their systems will collect. Obvious types are name, address, or social security number. Less obvious types are information that can be linked or that is linkable to specific individuals. As the PTA tool created by the U.S. Department of Homeland Security notes,[8] information about individuals can even include their images captured by cameras monitoring specific locations, or include information about a person's health status that may be detected by a system designed to capture radioactivity levels sensitive enough to determine whether an individual received chemotherapy. Privacy can be threatened when seemingly innocuous pieces of personal information—such as individual preferences that facilitate a Web site's use or proof of age when a driver's license is shown to participate in a separate age-restricted activity—are "bundled" in a single record. Privacy can also be endangered by the use of global positioning devices, cell phones, personal digital assistants, surveillance cameras, radio frequency identification tags, home wireless networks, and other technologies that could be monitored to provide information on where a person lives or works.

PRIVACY THRESHOLD QUESTION 2

Can you identify the statutory authority under which your system operates?

Rationale. No system should exist outside statutory authority. If your agency is operating a system not bound by any statute, problems exist that are larger than just privacy, i.e., illegal operations and illegal information collection. At a minimum, the federal Privacy Act and other laws apply to federal information, and state laws apply to state information.[9]

PRIVACY THRESHOLD QUESTION 3

Has a PIA ever been conducted on your information system?

Rationale. PIAs are generally conducted at the beginning of an information system's design phase, or when a system undergoes a significant upgrade. However, if your system collects, maintains, or generates PII, it would be wise to conduct a PIA even if your system doesn't fall into these two categories. A PIA will identify the privacy implications and characteristics of your IT system and will allow you to mitigate privacy vulnerabilities before a breach occurs.

Your answers to these questions will reveal the privacy policy needs of your system, and will help you to decide whether to continue on to a full PIA.

8 Available at **http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf**.

9 Tribal users may also want to consult the Indian Civil Rights Act of 1968.

Steps to Developing the Privacy Policy: Where the PIA Fits In

STEP 1

Systems and Privacy Threshold Analyses. Analyze the information system and information use, maintenance, and sharing to determine what systems need a PIA. Then, conduct a PTA for each system.

Take these additional steps after determining your system or information-sharing initiative's privacy policies needs:

STEP 2

Identify and analyze your shared information. It is important to articulate the information exchanges that will occur in your system in order to understand how information will be shared across the system and with participating organizations. Knowing the agencies and organizations involved, what data they will share, when, under what circumstances and what it will be used for is critical in understanding any privacy implications. It helps to follow a consistent, intuitive approach to capturing information-exchange requirements. The Justice Information Exchange Model (JIEM)[10] methodology, developed by SEARCH with funding from BJA, provides such an approach. For each exchange, JIEM identifies **who** is involved (what agencies/organizations), **why** the exchange is taking place (business process), **when** it takes place (business events and conditions), and **what** information is being exchanged. All of the analysis captured in JIEM—both the context and content of information exchange—can be useful in understanding potential privacy risks, as well as in specifying privacy rules within a privacy policy.

STEP 3

Conduct the PIA (use the template in Appendix A).

Timing of the PIA

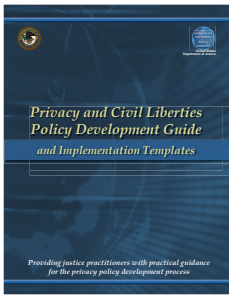
Privacy concerns must be addressed as part of an overall strategic planning process for information systems development, enhancement, and replacement, or any time a system is modified, updated, and/or revised. Committees formed to oversee planning and implementation should make conducting a PIA their first step, followed by the development of privacy policies based on information obtained during the assessment process.

Ideally, a PIA should be conducted and privacy policies developed when a system is designed or significantly upgraded; however, a PIA can be conducted at any time. In fact, if you are operating an information-sharing system without assessing privacy risks or developing privacy policies, these tasks should top your priority list.

You may not be able to fully answer every question on the PIA depending on how early the PIA process is initiated during system design. The PIA template included with this Guide can be conducted at various stages over a period of time as system development advances and there is greater clarity around data collection, use, dissemination, and other factors that may delay PIA completion. The PIA should be updated over time to reflect any changes to the system that may impact privacy. This PIA can also be used to assess the privacy implications of existing systems that are *not* undergoing significant upgrade.

STEP 4

Develop your privacy policies. (Use the Global Justice Information Sharing Initiative's *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*, **http://www.it.ojp.gov/documents/Privacy_Guide_Final.pdf**.)



10 See **http://www.search.org/programs/info/jiem.asp**.

Should You Publicize the Completed PIA?

A completed PIA can be a valuable public relations tool to proactively address privacy and other identified concerns as a system nears implementation. Prominent posting of a completed PIA on a Web site or at an agency's office allows the public and policymakers to evaluate its thoroughness and accuracy. The PIA also demonstrates an agency's role as a trusted data steward. An agency may also consider other methods, such as press releases, to increase public awareness of its completed PIA. These actions implement the FIPPs Transparency Principle.

Who Conducts the PIA?

Fundamental to information-sharing system development is (1) agreement on guiding principles and (2) identification of strategic and tactical issues. **Conducting a PIA during the strategic planning process ensures that privacy issues are addressed early and are accommodated in the system design and governance**. Ideally, a PIA is completed by information system stakeholders (the governance group) as part of a strategic planning process, and in collaboration with the agency's legal counsel, record managers, those responsible for data privacy, those responsible for freedom of information responses, and system security personnel.

The completed PIA is then submitted to the information system's governing/decision-making body. PIA results will show decision-makers what policies are needed, or any other work that might be necessary. In smaller organizations or information-systems efforts, PIA responsibilities may belong to an individual rather than a group; nevertheless, smaller agencies may still wish to include stakeholders and other individuals from outside their agencies to assist in PIA preparation. They can identify privacy issues and suggest ways to mitigate them. Interested and/or affected parties to supplement internal agency resources could include:

- Privacy advocates
- Private/public records managers
- Civil liberties organizations
- Elected officials
- Legislative research staff
- IT associations
- Other justice IT professionals
- Prosecutors
- Public defenders
- Judges
- Corrections, probation, and parole

There may be other interested groups in addition to those listed above, such as public safety-minded local businesses, that could provide technical resources. A local hospital or medical provider may have a Health Insurance Portability and Accountability (HIPAA) expert whose knowledge in protecting health information could be useful in assessing your system's privacy implications. If no local civil liberties groups or public defenders are available, nonprofit organizations with outreach efforts around social justice issues, such as local churches and faith communities, could assist.

In addition to gaining valuable expertise, allowing stakeholders to participate in the PIA preparation process demonstrates an agency's commitment to inclusiveness and openness. Ultimately, the PIA process should be as inclusive as possible to address the perspectives of members of the public who may be impacted by the system. Including stakeholders in your review process gives you an opportunity to address their privacy concerns, and may even eliminate some.

Ultimately, it is the responsibility of the governing body in a multi-organizational effort, or the agency executive in a smaller initiative, to address the risks revealed by the PIA. These leaders will then determine whether the risks are acceptable, can be mitigated via policy development or could result in a decision not to move forward with the project.

PIA Components

The federal Office of Management and Budget Guidance (OMB M-03-022, included as Appendix G) provides, in part, that a PIA analyze and describe:

- Information to be collected (e.g., nature and source).[11]
- Why it is being collected (e.g., to determine eligibility).
- Intended use (e.g., to verify existing data).
- With whom the information will be shared (e.g., another agency for a specified programmatic purpose).
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent. (Note: This is of particular importance since collection of criminal justice data is often not voluntary or provided with consent.)
- How the information will be secured.

A popular standard mechanism for developing privacy policies in both the public and private sectors is the Fair Information Practice Principles, known informally as the FIPPs, first espoused in the 1973 U.S. Department of Health, Education and Welfare (HEW) report, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. In 1980, the Organization for Economic Cooperation and Development (OECD), using the HEW principles as a foundation, released the following eight principles in an effort to facilitate international trade. These eight principles are today woven into many PIA templates:

1. **Purpose Specification**: Why personal information is collected. The purpose for the collection of personal information should be stated no later than when the information is collected, and subsequent uses of the information should be limited to that purpose or to other compatible purposes.

State PIA Raises Key Points

A PIA conducted by Minnesota's Bureau of Criminal Apprehension on its eCharging Services Project raised the following questions:

- Does the data classification of incident report drafts change after a final incident report is submitted to the prosecutor?
- Does the action a prosecutor chooses to take on an incident change its data classification?
- Since eCharging will be deployed in phases, does it need different or temporary data classifications for its pilot project?

2. **Collection Limitation**: Careful review of how personal information is gathered to avoid unnecessary collection of personal information. Personal information should be collected with the knowledge or consent of the information subject when possible.
3. **Data Quality**: Data should be accurate, complete, current, and relevant to the purpose for which it is collected.
4. **Use Limitation**: Data use and access should be limited by the purpose statement. It can be used for purposes other than those identified in the purpose statement only with the consent of the information subject or by authority of law.
5. **Security Safeguards**: Evaluate risk of loss or unauthorized access to information and implement appropriate security safeguards. Security should also guard against unauthorized destruction, modification, use or disclosure.
6. **Openness**: Agency notice on how it collects, maintains, and disseminates data. An openness policy should identify and provide the usual residence of the information controller, and also establish the existence and nature of personal information.
7. **Individual Participation**: Subjects allowed to review data about them and to correct if necessary. Information should be provided to subjects at a reasonable cost, within a reasonable

11 JIEM modeling, discussed earlier, is an effective way to analyze and describe the information to be collected, why it is being collected, its intended use, and with whom the information will be shared.

time period, and in an intelligible form. Individuals denied access to their information should be allowed to challenge that denial.

8. **Accountability**: Oversight and enforcement of the other design principles.

The PIA template provided as Appendix A incorporates these principles.

PIA Outcome

A completed PIA:

- **Identifies privacy vulnerabilities and risks** for stakeholders, owners, agency heads, and others accountable for a system's operation.
- **Includes a summary of mitigating actions** to address identified privacy risks. The individual completing the PIA should have the authority to direct mitigation steps, not just to recommend changes after the fact. A PIA that states risk, and which describes what will be done in the future to mitigate it, is a statement of poor privacy policy implementation and of a hope to improve. A PIA stating that identified privacy risks were mitigated along the way demonstrates that privacy was built into the system and was not just a theoretical goal.
- Most importantly, **identifies what privacy policies must be developed to avoid, mitigate or eliminate risk** to data maintained in the system.

Stakeholders can share the PIA to engage the public, policymakers, and others in a dialogue about the system, thereby fostering greater public trust. Policies that result from the PIA can include:

- Enhanced security features, such as improved audit capability or enhanced physical security.
- Updated records retention schedule.
- Publication of the purpose statement and privacy policy on the agency Web site or in a state register.
- Audit procedures.
- Challenge processes for data that originates in other systems.

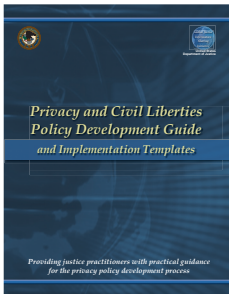
DHS Conducts PIA, Results in Notice and Redress

The U.S. Department of Homeland Security (DHS), Customs and Border Protection (CBP), conducted a PIA of its Automated Commercial Environment (ACE) System, a program to monitor passage of commodities, materials, crew members, and passengers across U.S. borders.

As a result of the PIA process, participating truck carriers are asked to provide their drivers notice regarding the collection and use of their information as well as how to seek redress if their record is inaccurate. CBP created a fact sheet to provide drivers additional notice. See **http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_aceitds.pdf**.

The PIA will ultimately serve as the first step in identifying the privacy implications and vulnerabilities of your information system. It is a road map for developing a thoughtful and comprehensive privacy policy to protect personal and confidential information, and will serve the needs of your agency and the public.

For comprehensive guidance, best practices and a template for policy development, please see the Global Justice Information Sharing Initiative's *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*, **http://it.ojp.gov/documents/Privacy_Guide_Final.pdf**.



Institutionalizing the PIA Process

Conducting a PIA at the state, local, and tribal levels is a best practice that should become a standard component of any strategic planning process aimed at automation and information sharing.

As noted previously, the E-Government Act of 2002 requires federal agencies to conduct PIAs of new or significantly modified information systems. Few states have statutory requirements to conduct PIAs, either of new, significantly modified or existing information systems. If your state is considering institutionalizing a PIA process, both model legislation in Appendix C and a governor's executive order in Appendix D provide suggestions for such undertakings.

As outlined in this Guide, the consequences of inadequate or careless data protections are too severe for state, local, and tribal justice jurisdictions to delay assessing the privacy implications and vulnerabilities of their information systems. News stories about agencies that failed to properly protect their data, and that let personal and confidential information fall into the wrong hands, are all too common. Don't let your agency make the headlines for the wrong reasons.

APPENDIX A
Privacy Impact Assessment Template

Privacy Impact Assessment Template

Information Sharing System(s) Assessed:

System Name	
Purpose	

Assessment Date: _____

Organizations Involved:

Assessors:

Project Manager: _____

Final PIA Submitted to: _____

Date Submitted: _____

Approved By: _____

Approval Date: _____

This template is offered as a Word document tool that can be filled out electronically. We recommend using the Word tool, which enables the easy entry of narrative responses. Download the PIA Template at the Bureau of Justice Assistance Web site, http://www.ojp.usdoj.gov/BJA/, or the Global Web site, http://www.it.ojp.gov/index.jsp.

Instructions

- There are 43 questions in eight PIA categories. Questions are coded by color, depending on who should respond (see Legend).

- The **Question** column poses a question for response or action, and the **Rationale** column provides further detail and in some cases, instruction.

- Respond in the **Answer** column as appropriate (Yes, No, N/A, or a narrative response). Attach materials, if needed.

In the **Assessment of Risk** column, make a judgment as to the *Likelihood*, *Severity*, and *Risk Tolerance Level* of the privacy risk.[12] Use these guidelines:

Likelihood that risk will occur
Remote: The risk probably will not occur because the risk would be difficult to realize, or there are solid means in place to limit the risk appropriately.

Possible: The risk has a chance of occurring, but it may be difficult or there are policies or procedures in place to help avoid the risk.

Likely: Due to conditions and capabilities, the risk is likely to occur.

Severity of identified risk
Low: The risk is manageable through planning and action, and the impacts generally are minimal.

Medium: The risk will be mitigated through planning and action, although if it occurs, it will still have some impact on some of the more important areas of concern.

High: The risk will have serious impacts and without extensive planning and action, its consequences would be severe.

Your tolerance for that risk
Avoidance: Avoidance is often used for risks that have the capacity for negative impact, but have little known recourse. In privacy projects, a decision to avoid risks often means a decision not to let your agency put itself in the situation where it could incur the risk. Therefore, your decision would also be to avoid the cause of the risk.

Assume: The decision to assume a risk means accepting the risk as is, and not implementing any policies or procedures to lessen it. This is often the decision in cases where the risk is so minimal and of limited impact should it occur that the cost of implementing a mechanism to minimize or reduce it would be far greater than the agency's concern.

Mitigate: This is the most common decision to make for identified risks: to implement policies, procedures, and other controls to limit the risk to an acceptable level.

Transfer: Transfer the responsibility for a system or the risk itself to another party that can better accept and deal with the risk and/or has the resources necessary to properly mitigate the risk.

- In the **Corrective Action/Recommendation** column, record the corrective action or recommendation that your initiative will take to mitigate the identified risk.

- In the **Priority** column, record the priority level of the risk, either 1 (high priority), 2 (moderate priority) or 3 (lowest priority).

Legend Questions are coded by the color of the person(s) most likely to be able to respond.
System Administrator
Data Privacy Officer or Legal Counsel
Records Staff
Technical/System Security Staff

12 For more about risk assessment, see *Law Enforcement Tech Guide for Information Technolgy Security: How to Assess Risk and Establish Effective Policies,* prepared by SEARCH and published by the Office of Community Oriented Policing Services, U.S. Department of Justice. Available at http://www.search.org/programs/safety/tech-guide.asp.

PIA Category 1: Purpose Specification						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
☐	1. Is there a written purpose statement for collecting personally identifiable information?	A purpose statement helps an agency decide what data it needs to collect and may be required by state law.				
☐	2. Is the purpose statement posted or otherwise easily accessible to the public when information is collected?	The purpose for information collection should be stated no later than at data collection. Subsequent data use should be limited to stated or compatible purposes. Making your purpose statement available to the public provides greater openness.				
☐☐	3. Do you have statutory authority for collecting this data? If so, include citation(s).	State and/or federal laws may limit what data can be collected.				
☐	4. Describe the relationship between collected data and the system's purposes so extra data are not collected.	The amount and type of data needed to achieve a program's purpose should be analyzed.				
☐	5. Will there be a periodic review of collected data to make sure they are still needed? If so, include the review schedule.	Privacy is promoted when government agencies routinely review data and storage to ensure that excessive data are not collected.				
☐	6. Is the written purpose statement periodically reviewed and updated?	Written purpose statements should be reviewed periodically to ensure they reflect the current information-sharing environment.				

PIA Category 2: Collection Specification						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
☐	7. Is the collection of personal information limited to the system's identifiable purpose?	Limiting the collection of personal information minimizes the possible use of inaccurate, incomplete or outdated information. It also reduces the information that can be compromised should a breach occur.				
☐	8. Is personal information obtained by lawful and fair means?	Information should be obtained in a way that is not inappropriately intrusive. The provider should not be misled or deceived about why it is collected.				
☐	9. Where appropriate, is personal information obtained with the knowledge or consent of the data subject?	Consent can be expressed or implied, but it must be unequivocal. Implied consent may be inferred from the action or inaction of the information provider.				
☐☐	10. Are collected data elements classified to limit public or data-subject access? If so, describe how.	Data classification determines who has access and for what purposes.				
☐☐	11. Are data collected on juveniles?	Generally, state and federal laws provide special rules for juvenile data.				
PIA Category 3: Data Quality						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
☐	12. Are there business practices/ procedures to verify data are accurate, complete, and current? If yes, describe procedures.	While this may not be a statutory requirement in your state, you should consider adopting this concept as a best practice.				
☐	13. Is the system the source of the data?	If not, you may need to consider how to ensure data accuracy and completeness.				

PIA Category 3: Data Quality (continued)						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
	14. Is the data collected directly from the individual?	Collecting data directly from a data subject might increase data accuracy.				
	15. Do procedures for data management detail retention and disposal issues?	Most states require a records retention schedule for data maintenance.				
	16. Do you have a procedure for tracking: • Modification requests? • Determinations of requests to modify? • Modifications based on the requests? • Source used to modify the information? • When the last modification occurred?	Agencies must make reasonable efforts to minimize the possibility of using inaccurate, incomplete, or outdated information. This should include effective processing of modification requests so a data subject's record includes the result of the request along with the information consulted in response to the request, and the date that any modification occurred.				
	17. Is there a procedure to provide notice of correction or modification to: • Subsequent justice system users? • Third parties (secondary users)?	Agencies may want to consider establishing logs and audit trails to identify justice system users and third parties who received personal information. This would allow agencies to notify down-the-line users when data are modified from those originally transmitted.				
	18. Where access by the data subject is not appropriate, are there other methods to ensure that information is accurate and up to date? If yes, what are the other methods?	When accuracy cannot be verified by the data subject because of sensitivity (e.g., intelligence data), agencies may consider other methods to ensure data quality and timeliness, such as examining the reliability of the contributor, matching the data against other reliable sources, seeking verification from third parties, and other approaches.				

PIA Category 4: Use Limitation						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
	19. Is use or disclosure of personal information limited to the purposes articulated in Principle 1?	Personal data must be collected for specified, explicit, and legitimate purposes and not used in a way that is incompatible with those purposes.				
	20. Is the disclosure of personally identifiable data limited by state or federal law or policy?	Disclosure can be limited by state or federal law or by agency policies. In answering this question, agencies should address methods limiting data disclosure.				
	21. Are secondary uses limited to those: • With the data subject's consent? • By the authority of law? • Pursuant to a public access policy?	Reasonable steps should be taken to inform the provider how the information will be used, and that the information may be used beyond the purposes for which it was collected. His or her consent may or may not be sought in these instances.				
	22. By law, can outside entities access data held by your system? If so, list the outside entities, their authorized purposes and any statute citations.	Unless state or federal law authorizes data sharing, you may need the subject's consent or a court order before sharing data with outside agencies or third parties. Your state law may also permit data sharing through a contract or memorandum of understanding.				
	23. Is access to sensitive data limited to staff/contractors who need the data for their work? If so, describe how.	Employee/contractor access can be limited by policies and procedures or system design.				

PIA Category 5: Security Safeguards						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
	24. Does reasonable technical security protect data against unauthorized access or disclosure?	Reasonable security is crucial. A "reasonableness" standard reflects that no security is foolproof, and that what is reasonable will change as technology improves. Security is also based on the data's sensitivity/classification.				
	25. Is there reasonable physical security in place?	Technical security receives more attention, but physical security is also important.				
	26. Have user-access profiles been assigned on a need-to-know basis?	User access should be limited to the data that each employee needs for official duties.				
	27. Do controls and procedures exist for the authority to add, change or delete personally identifiable data?	Read-only access can control who alters system data.				
	28. Has staff been trained to protect personal information?	Regular training will help staff keep abreast of technical, legal, and other critical issues.				
	29. Are there plans and mechanisms in place to identify: • Security breaches? • Disclosure of personal information in error?	Agencies should consider plans to identify security breaches or inappropriate disclosures of personal information. Mechanisms should be established to quickly notify affected parties so they can mitigate collateral damage.				
	30. Does security include auditing to track system use (e.g., by whom and when data are accessed or updated)?	Audit trails allow the investigation of inappropriate access or use.				

PIA Category 6: Openness Principle						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
☐☐	31. Is contact information for your agency's privacy officer and for the privacy officers for any source systems accessible by the public? Attach a list of the names/contact information.	Source systems are systems from which you receive data. It is a good business practice to know not only your own privacy officer, but also the officers for source systems.				
☐☐	32. Do you have written policies and procedures that explain how the public and data subjects can access data?	Agencies should adopt general openness policies about practices and procedures for the use and protection of personal information. Agencies should make these policies available with reasonable effort upon request.				
☐☐	33. Does your agency require a privacy notice before data are collected?	State law may require that a data subject be given a privacy notice on how collected data will be used and shared.				
☐☐	34. Does your agency require notice to affected individuals when data are requested, sold or released to third parties?	Agencies should make their personal information management policies readily available to information providers with reasonable effort. A third party receiving information must also adhere to responsible protection requirements.				

PIA Category 7: Individual Participation						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
☐☐	35. Can an individual, or an individual's agent, obtain confirmation of whether the data collector has information relating to him or her?	Record subjects should be able to request access to their personal data at reasonable intervals without excessive delay or expense. Information should be in intelligible form and include any available information about the source.				

PIA Category 7: Individual Participation (continued)						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
	36. Do procedures explain a data subject's right to challenge data accuracy and/or completeness?	Information shown by the data subject to be inaccurate, incomplete, out of date, or irrelevant should be revised, modified, corrected, or removed.				
	37. Are these procedures posted or readily available?	Policies and procedures providing authority to access personal information for review should be provided with reasonable effort to the subject.				
	38. Are there procedures to flag challenged data and to post additional data related to the challenge?	Agencies may want to flag challenged data and to post data provided by the challenger to alert subscribers that data is being challenged and to provide them with the latest and most complete information.				
	39. Can you resolve data challenges when data originated with another agency?	Laws may allow data subjects to challenge data wherever it is maintained, even if the data did not originate with the agency that is being challenged. Coordinating data challenges with the agency where the data originated would be the most effective way to reach a decision about data from another official source. Also, assisting data subjects in locating inaccurate or incomplete data wherever it is maintained is a valuable public service and a best practice.				
	40. Can you verify data subjects' identities prior to allowing them access to data? If yes, describe measures.	Many jurisdictions require subjects to submit fingerprints to verify that they are the subjects of the information they seek.				

PIA Category 8: Accountability						
Code	**Question**	**Rationale**	**Answer**	**Assessment of Risk**	**Corrective Action/ Recommendation**	**Priority [1,2,3]**
	41. Does your agency have an individual responsible for complying with records management laws and policies? If so, provide name/contact.	An individual should be designated to monitor compliance with these laws and policies, and to establish procedures for receiving and resolving complaints.				
	42. Are there penalties for unauthorized use of data? If yes, describe the penalties.	Agencies may consider internal penalties up to and including termination and prosecution for improper and/or unauthorized use of personal information. Outside agencies may lose access to such information for similar improper and/or unauthorized use.				
	43. Can you easily provide access to all of the public data when requested?	Systems that contain some public data should be designed to allow easy production of the data for the public. Your state law may require it.				

APPENDIX B
Privacy in the News

Inadequate protection of personal and confidential information by justice agencies can attract unwanted attention, which may result in negative publicity, decline of public trust, and legislative reactions that affect funding.

Consider the case of a 43-year-old Florida man who sued a local sheriff's office for $1.5 million after being turned down for a number of jobs because background checks revealed sealed criminal record information and a grand theft conviction for a different individual with the same name born the same year.

In addition to identification issues, there are also claims that law enforcement agencies unnecessarily withhold data from the public.[13] A newspaper's recent review of the Illinois State Police's handling of data requests from a variety of requestors, including crime victims, families, insurance companies, and the media, showed that the majority of requests were denied on various bases or were simply ignored.[14]

In 2003, hackers gained access to a data system run by the Minnesota Chiefs of Police Association that contained information on more than 8 million law enforcement contacts with individuals, and which was accessible to nearly 200 law enforcement agencies in the state. Poor security allowed unlawful access to protected data on adults, juveniles, offenders, gun permit holders, victims, and witnesses.

The security breach attracted the attention of state legislators and privacy advocates. Although the system was a valuable law enforcement tool, it operated outside of public scrutiny while violating state data practices laws, such as commingling juvenile and adult data.[15] In addition to violating Minnesota's Government Data Practices Act,[16] the system failed to follow most of the FIPPs. The privacy concerns and outcry sparked by the breach resulted in the permanent shutdown of the system and the destruction of its 8 million records, depriving law enforcement of a significant amount of useful information.

Had the system's operators conducted a PIA, they would have recognized the privacy vulnerabilities of their system. A PIA would have highlighted a number of key issues including:

- Inadequate technical security
- Statutory obligations to provide data subject access
- Inability to provide public data access
- Failure to publicly post public and data subject access procedures
- Inappropriate merging of adult with juvenile data.

Several years later the privacy community actively participated in the development of a replacement system to ensure tight control with greater transparency. In the post-9/11 era, this was a painful wake-up call for Minnesota's criminal justice community.

Another casualty of poor privacy planning was the Multistate Anti-Terrorism Information Exchange Program (MATRIX), a federally funded data-mining system developed by Seisint, a Florida-based contractor working with the Florida Department of Law Enforcement. MATRIX was initially developed after 9/11 to help identify terrorist suspects. The system analyzed government and commercial databases, searching for links between known terror suspects and possible conspirators.

13 "State Police Reject Many Requests for Public Information, Report Says," Associated Press, April 25, 2007. Available at **http://state-police-news.newslib.com/story/97-3245424/**.

14 Ibid.

15 **http://www.ipad.state.mn.us/newsletters/0404fyi.pdf**.

16 2007 Minnesota Statutes Chapter 13, **https://www.revisor.leg.state.mn.us/statutes/?id=13**.

MATRIX received a $4 million grant from the U.S. Department of Justice in 2003 and was slated for additional federal funds.[17] Sixteen states covering more than half the U.S. population participated in MATRIX.[18] However, the failure by MATRIX developers and participants to develop appropriate privacy policies and to publicize the existence of their system attracted significant opposition by privacy advocates and negative publicity in the news media.[19]

As new states were being approached to join MATRIX, other states began to reconsider their earlier decision to participate. Based on widespread privacy concerns, the program lost federal funding in June 2005.

News stories of inappropriate data use by justice agency employees are not frequent, but consider these headlines:

- "LA Police Officer Uses Database to Snoop on Stars," excerpt from the *Los Angeles Times* published in the Privacy News, April 10, 2003.
- "Police Abuse Database," *Detroit Free Press* examination of Michigan's Law Enforcement Information Network, August 4, 2001.

Justice information system designers can avoid the unenviable attention paid to those listed here by proactively addressing the privacy implications and vulnerabilities of their systems so policies are in place to prevent embarrassing incidents, and procedures are also available to quickly reduce the impact of system breaches should they occur.

17 Anita Ramasastry, "Why We Should Fear Matrix," American Civil Liberties Union, Nov. 5, 2003, **http://writ.news.findlaw.com/ramasastry/20031105.html**.

18 See "The Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Program," Congressional Research Service Report for Congress, Aug. 18, 2004. Available at **http://www.fas.org/irp/crs/RL32536.pdf**.

19 The MATRIX program was seen as substantially similar to another controversial data-mining program that sought to create a database of public and private information of "unprecedented scale," known as Total Information Awareness. It was led by retired Adm. John Poindexter, a central figure in the Reagan-era Iran/Contra scandal, and run by the Information Awareness Office of the Pentagon's Defense Advanced Research Projects Agency. Privacy concerns caused that program to be shut down in 2003. **http://www.usatoday.com/news/washington/2003-09-25-pentagon-office_x.htm**.

APPENDIX C
Model Legislation

Section 1.100 PURPOSE
To ensure that all criminal justice data information systems developed, procured, or significantly modified minimize the risk of inappropriate impacts on the privacy of individuals, the "Data System Privacy Review Act" is enacted.

Section 1.200 DEFINITIONS

a. "Criminal justice agency" has the meaning given provided in section [insert citation to appropriate state law] and includes courts.
b. "Information data system" means any technology system or project that collects, maintains or disseminates personally identifiable data.
c. "Personally identifiable data" means data from which an individual human being can be uniquely identified including but not limited to:
    (a) first and last name;
    (b) physical address;
    (c) e-mail address;
    (d) telephone number;
    (e) social security number;
    (f) credit card information;
    (g) bank account information; and
    (h) any combination of personal information that could be used to determine an individual's identity.
d. "Privacy impact assessment" or "assessment" means a series of questions approved by [insert authority] to evaluate how personally identifiable information is collected, stored, protected, shared and managed by an electronic information system or online collection application.
e. "Significantly modify" means any changes to a system that are not routine improvements, systems maintenance, software upgrades, or routine equipment replacement.

SECTION 1.300 GENERAL PROVISIONS

a. A criminal justice agency or court developing, procuring, or significantly modifying an existing information data system containing personally identifiable information shall complete a privacy impact assessment authorized by [insert authority] before the system is implemented.
b. Completed assessments shall be posted on the criminal justice agency's Web site and maintained in the agency's principal office for four years.
c. Completed assessments shall be submitted to [insert authority; e.g., chief information officer, chief privacy officer, attorney general's office] for review and approval.
d. The [insert authority] shall report annually on January 15 to the Legislature all of the assessment completed in the prior year.

SECTION 1.400 PENALTIES

a. Agencies or courts failing to complete and submit a completed assessment in a timely manner may forfeit current and future funding for information technology systems.

Criminal justice agencies and system proponents could also encourage adoption of the following executive order (Appendix D) by their state's governor.

APPENDIX D
Sample Executive Order

IMPROVING DATA PROTECTION AND SECURITY BY STATE AGENCIES

I, GOVERNOR _____ OF THE STATE OF _____, by virtue of the authority vested in me by the Constitution and applicable laws, do hereby issue this executive order:

WHEREAS, _____'s state agencies are the data stewards of personally identifiable information about its citizens in their possession and have a duty to protect that data from misuse. Appropriate management of sensitive information, including social security numbers, driver's license numbers, financial account numbers, and other similar sensitive personal information, respects the privacy of those individuals associated with that data.

WHEREAS, *sensitive information which is not adequately protected, can cause individuals to suffer a variety of consequences including invasion of privacy, personal embarrassment, stalking, harassment, identity theft or other criminal misuses of their data*.

WHEREAS, identity theft costs our nation's citizens and businesses billions of dollars in losses each year. Misuse of sensitive data can also place individuals at risk for harassment, stalking and other criminal acts.

NOW THEREFORE, I hereby order that:

1. The state's Chief Information Officer will be responsible for coordinating the implementation of improved privacy measures.
2. Within 90 days, the state's Chief Information Office shall develop and disseminate a Privacy Impact Assessment (PIA) Directive for use by state agencies for all new or significantly modified information data systems. The Directive will address: what information is to be collected, why the information is being collected, intended use of the information, with whom the information will be shared, what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), how individuals can grant consent, and how the information will be secured.
3. Within one year, all state agency heads shall conduct Privacy Impact Assessments on all existing systems which maintain personally identifiable information to include names and addresses, social security numbers, driver's license numbers, and financial institution account information of more than (10,000) individuals.
4. Prior to requesting any state funds to develop, procure, or significantly modify a data system, state agency heads shall conduct a Privacy Impact Assessment.
5. Completed Privacy Impact Assessments shall be prominently posted on a state agency's Web site for at least two years.

Pursuant to (insert cite), this executive order will be effective until (insert date).

APPENDIX E
Resources List

Bureau of Justice Assistance, U.S. Department of Justice: **http://www.ojp.usdoj.gov/BJA/**

Global Justice Information Sharing Initiative: **http://www.it.ojp.gov/topic.jsp?topic_id=8**

Privacy and Civil Liberties Policy Development Guide and Implementation Templates: **http://www.it.ojp.gov/documents/Privacy_Guide_Final.pdf**

Privacy, Civil Rights, and Civil Liberties: Policy Templates for Justice Information Systems: **http://it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf**

Global Security Working Group: **http://www.it.ojp.gov/topic.jsp?topic_id=58**

Institute for Intergovernmental Research: **http://www.iir.com/**

The Justice Management Institute: **http://www.jmijustice.org/Home/PublicWeb**

National Criminal Justice Association: **http://www.ncja.org**

Justice Information Privacy Guideline: **http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/privacyguideline.pdf**

Office of Management and Budget Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002: **http://www.whitehouse.gov/omb/memoranda/m03-22.html#a**

Privacy and Civil Liberties Office, U.S. Department of Justice: **http://www.usdoj.gov/pclo/**

Privacy Impact Assessments Official Guidance: **http://www.usdoj.gov/pclo/pia_manual.pdf**

Privacy Threshold Analysis: **http://www.usdoj.gov/pclo/privacy_threshold_analysis.pdf**

Privacy impact assessment template: **http://www.usdoj.gov/pclo/pia-template.pdf**

SEARCH, The National Consortium for Justice Information and Statistics: **http://www.search.org**

"Privacy and Criminal History Records:" **http://www.search.org/programs/policy/privacy.asp**

"Compendium of State Privacy and Security Legislation:" **http://www.search.org/programs/policy/compendium/**

Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies: **http://www.search.org/files/pdf/ITSecTechGuide.pdf**

Report of the National Task Force on the Criminal Record Backgrounding of America: **http://www.search.org/files/pdf/Report%20of%20NTFCBA.pdf**

Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update: **http://www.ojp.usdoj.gov/bjs/abstract/umchri01.htm**

National Conference on Privacy, Technology and Criminal Justice Information, Proceedings of a Bureau of Justice Statistics/SEARCH Conference: **http://www.search.org/files/pdf/Privacyproceed.pdf**

Report of the National Task Force on Privacy, Technology and Criminal Justice Information: **http://www.ojp.usdoj.gov/bjs/abstract/rntfptcj.htm**

Federal Models

Internal Revenue Service: **http://www.cio.gov/Documents/pia_for_it_irs_model.pdf**

U.S. Agency for International Development: **http://www.povertyfrontiers.org/ev02.php?ID=1337_201&ID2=DO_TOPIC**

U.S. Census Bureau: **http://www.census.gov/po/pia/**

U.S. Department of Defense: **http://www.dla.mil/public_info/efoia/PIA.html**

U.S. Department of Homeland Security: **http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm**

U.S. Department of Homeland Security *Privacy Threshold Analysis* form: **http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf**

U.S. Department of Interior: **http://www.doi.gov/ocio/privacy/pia.htm**

U.S. Nuclear Regulatory Commission: **http://www.nrc.gov/about-nrc/plans/privacy-impcat-asess.html**

International Models

Australia: The Office of the Privacy Commissioner has produced a PIA guide: **http://www.privacy.gov/au/publications/pia06/index.html**

Canada: The Treasury Board of Canada Secretariat has produced a useful PIA e-learning tool: **http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp**

New Zealand: Office of the Privacy Commissioner, Privacy Impact Assessment Handbook: **http://www.privacy.org.nz/library/privacy-impact-assessment-handbook**

For a collection of online resources from around the world, collated by the New Zealand Privacy Commissioner's Office, see: **http://www.foi.gov.uk/**

APPENDIX F
Glossary

Access: The ability to view or obtain copies of data by authorized personnel, data subject, or the public.

Accurate data: Data which is reasonably free from error.

Agency(ies): Any state, local, or tribal criminal justice agency(ies) or the courts.

Audit trail: Process for recording (logging) a sequence of activities on a system; such as user log-ins and log-outs. More expansive audit trails would record each user's activity in detail—what commands were issued to the systems, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Criminal justice agency: An agency responsible for enforcement of local, state, federal, or tribal criminal laws.

Criminal justice integration: 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, tribal, and national systems. Generally, the term is employed in describing justice information systems that eliminate data entry, provide access to information that is not otherwise available, and ensure the timely sharing of critical information.

Information exchange analysis: A process used to identify and document the context and content of information exchange between business partners and their information systems. Context includes: who is involved (what agencies/organizations), why the exchange is taking place (business process), and when it takes place (business events and conditions). Content identifies what information is being exchanged. Both context and content of information exchange provide key elements used to build rules within a privacy policy.

Disclosure: The release, transfer, provision of access to, or divulging of personally identifiable information in any manner, electronic, verbal, or in writing, to an individual, agency, or organization outside of the agency that collected.

Invasion of privacy: Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. The Privacy Act of 1974 requires federal agencies that maintain systems of records to establish safeguards to prevent "substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained."[20]

Online collection application: Web site or online service to collect personally identifiable information or prospect information online, even though that information may be immediately deleted or not maintained for further use by an organization.

Personally identifiable information: Refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (from M-07-16, *Office of Management and Budget Memorandum for the Heads of Executive Departments and Agencies: Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007).

20 5 U.S.C. 552a(e)(10).

Privacy: An individual's interest in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.

Privacy impact assessment: A series of questions that evaluate the processes through which personally identifiable information is collected, stored, protected, shared, and managed by an electronic information system or online collection application, and describe how the privacy impact is mitigated.

Records management: The efficient and systematic control of the creation, receipt, maintenance, use, and disposition of records.

System security: Physical and technical methods employed to protect data for unauthorized access and use.

Significantly modified data system: Alterations to a system that are not routine equipment replacements or software upgrades. Significant modifications can be judged in a variety of ways including financial investments.

System owner/proponents: Any court or criminal justice agency personnel who control, own, or operate a data system. Depending on the size of the agency, it may be headed by a chief law enforcement officer or another administrative authority. Typically, the individual(s) is responsible for maintaining internal and external political and financial support for a system.

Transparency laws: State and federal laws that ensure that government records and certain meetings are open and accessible to the public. Transparency laws promote civic involvement in the functioning of government at all levels. The federal Freedom of Information Act and state Open Meeting Laws are examples of transparency laws.

User profiles: User profiles are limits on what data individual employees can access based on their job responsibilities. The profile defines the characteristics that an individual must have to legally access certain confidential information, e.g., someone directly involved in an investigation as opposed to someone who works for the law enforcement agency conducting the investigation.

APPENDIX G
Office of Management and Budget Memorandum (OMB M-03-022), *OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002*

In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

a. Conversions – when converting paper-based records to electronic systems;

b. Anonymous to Non-Anonymous – when functions applied to an existing information collection change anonymous information into information in identifiable form;

c. Significant System Management Changes – when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

   - For example, when an agency employs new relational database technologies or Web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.

d. Significant Merging – when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:

   1. For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.

e. New Public Access – when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

f. Commercial Sources – when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

g. New Interagency Uses – when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

   1. For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross-agency IT investment.

h. Internal Flow or Collection – when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:

   1. For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

i. Alteration in Character of Data – when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).