Privacy and Information Quality Policy Development for the Justice Decision Maker

Global Justice Information Sharing Initiative

United States Department of Justice

Highlights

- Since 9/11, virtually all agree that enhanced justice information exchange is critical. While pursuing a broadscale sharing capability, decision makers within the justice and public safety communities must vigorously protect our constitutional privacy rights and ensure information quality and accuracy. In short: *you need privacy and information quality policies to guide your agency's information sharing efforts.* Difficult? Yes. Insurmountable? No. Many good resources already exist to help justice and public safety leaders make the best possible business decisions on privacy and data quality for their information sharing practices. This document serves as an additional tool.

- Privacy and information quality policies protect your agency and make it easier to do what is necessary—share information. Focus on these policies will (1) strengthen public confidence in your agency's ability to handle information appropriately, (2) strengthen support for your agency's information management efforts through developing technologies, and (3) ultimately promote effective and responsible sharing of information that supports those fundamental concepts of the justice system we embrace as Americans.

- In today's information sharing environment, well-developed privacy and information quality policies help an agency prevent problems. Failure to develop, implement, and maintain dynamic privacy and information quality policies can result in:

  - Harm to individuals.
  - Public criticism.
  - Lawsuits and liability.
  - Inconsistent actions within agencies.
  - Proliferation of agency databases with inaccurate data.

  Each agency should evaluate and strengthen privacy and information quality policies to make them more relevant to twenty-first century technology.

- Privacy and information quality concerns directly affect the whole justice community, including law enforcement, prosecution, defense, courts, parole, probation, corrections, and victim services, as well as members of the public having contact with the justice system. The personally identifiable information maintained by agencies—if handled inappropriately—can cause problems for those affected. In worst cases, personal safety is jeopardized.

- Success of privacy and information quality policy improvement efforts depends on appointing a high-level member of your agency to champion the initiative. That person should assemble a policy development-and-review team of agency stakeholders, including managers, legal staff, system operators, technical support staff, and other personnel responsible for information management. The team must have the power to both develop and analyze a plan and then implement that plan. The plan must include input and review from interested and/or affected persons outside of the agency.

- Processes developed when most records were on paper may not translate well in the electronic and digital age. A privacy and information quality policy development-and-review effort will promote and facilitate modern information management and help you remain in control of your agency's technologies.

- The process promoted here does not require you to "start from scratch." There are historical and increasingly accepted "Fair Information Practices" to guide your agency's efforts.

- This document introduces the framework for a systematic consideration of privacy and information quality policies and practices within your agency. A companion *Privacy Policy Development Guide* has been designed by the U.S. Department of Justice's Global Privacy and Information Quality Working Group to assist your team in its efforts to develop or revise agency privacy and information quality policies.

Foreword: What's in This for Me?

You would be hard-pressed to find an opposing view: justice and public safety leaders—indeed, the American public—want justice-related entities to do a better job of sharing information to promote the well-being of our citizens and local neighborhoods and to protect homeland security. With the continually advancing field of technology, the technical capability to solve information sharing challenges now exists. If you can access your bank account as easily in Duluth, Minnesota, as you can in Tokyo, Japan, surely an officer in one county can share sex offender data with a parole worker in the neighboring town. But justice leaders know all too well the unfortunate truth—sharing information is not a given. While pursuing a critical, broadscale justice information sharing capability, decision makers must simultaneously ***vigorously*** protect citizens' constitutional rights. In short, *privacy and information quality policies are needed to guide agency information sharing efforts.* We may want our justice leaders to exchange information, but we want that sharing to be *appropriate*, we want that information to be *accurate,* and we demand safeguards be in place to protect our individual rights. Difficult? Yes. Insurmountable? Not at all.

Many good resources and guidelines have been created to assist justice leaders in making the best business decisions for information sharing.

Since 1998, the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ), has supported a group of your peers to tackle these exact concerns. DOJ's Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) addresses timely justice-related information sharing issues, such as questions of privacy and information quality. What follows, developed by the Global Privacy and Information Quality Working Group, is a sound first step in this area: a blueprint for initiating and completing a process to ensure that your agency develops and maintains essential privacy and information quality policies involving the collection, use, and dissemination of information. Additional resources that address the range of justice and public safety leaders' information sharing challenges and opportunities are included in "Global Resources for the Justice Decision Maker," concluding this document.

Introduction

Should you be concerned about developing or reviewing your agency's privacy and information quality policies? Ask yourself:

1. ***Does my agency control, disclose, or provide access to information to persons or agencies outside of my organization?***

2. ***Does my agency's information system(s) contain data or information connected to or shared with other information systems or agencies?***

3. ***Does my agency collect, use, or provide access to "personally identifiable information" (information that identifies individuals by reason of the content)?***

4. ***Does my agency have a stake in the accuracy of the information it manages?***

A "yes" to any of the above questions suggests that your agency should make it a priority to review privacy and information quality practices. Government policymakers and agency heads must take action to cause that review to occur.

Increasingly, the sharing of information is ***key*** to agency success in the twenty-first century. The ease of sharing information promoted by new technologies and the vital importance of ensuring that information is accurate make the implementation and maintenance of privacy and information quality policies and practices essential to any agency's information operations. With the growth in the assimilation, utilization, and sharing of **personally identifiable information**—information that can be linked to individuals—that has come with modern technologies, effective measures to ensure appropriate levels of privacy protection are increasingly important. Additionally, information created or compiled by your agency must be accurate or it is of little value. When you share information with another entity, there is the implicit expectation that the data you provide is *accurate* and that there are steps to ensure *information quality*; likewise, you expect the same from other agencies when receiving information. Promoting information quality by internal safeguards and procedures helps to ensure the accuracy of the information you handle.

Unless effective privacy and information quality safeguards are being utilized at every level of your agency's information and data-handling operation, you may be exposing yourself and others to unacceptable risks from inaccurate information or problems caused by failing to honor essential privacy expectations. When agencies collectively maintain appropriate levels of attention to privacy and information quality, the sharing of information is facilitated in a responsible and effective manner.

Having a "security policy" related to data or information is not enough. Security policies alone do not adequately address the privacy and information quality issues contemplated in this discussion. Although *privacy* and *security* both relate to handling data and information—and are both essential to justice-related information sharing[1]—they have different implications and considerations. "Security" relates to how an organization protects information during and after collection. "Privacy" addresses why and how information is collected, handled, and disclosed and is concerned with providing reasonable quality control regarding that information. Considering the breadth of the issue, some existing "privacy policies" may

fail to address these concerns in that they relate to *access to records* instead of defining privacy protections.[2]

Using computers to share databases and cross-reference digital information has heightened privacy and information quality concerns. Yet, as a practical matter, privacy and information quality policies and procedures affect every aspect of an agency's work, not just technology and operations. These concerns involve agency policy aspects, legal considerations, public relations, and interagency relationships. It is essential that agency leaders demonstrate an appreciation of the importance of these issues by appointing an influential member of agency management to champion the policy development initiatives proposed herein. Because adoption of a privacy policy may require a change in an agency's procedures, it may require a corresponding shift in agency "mind-set." The involvement of a high-level member of the administration will help ensure that the necessary changes are accepted and implemented.

As a justice or public safety leader, if you are still unsure about the fundamental importance of privacy and information quality safeguards, picture your agency in the following scenarios.

Case Studies: Is Privacy and Information Quality an Issue?

In December 2002, former U.S. Drug Enforcement Administration agent Emilio Calatayud was sentenced to prison and fined on charges related to his use of protected law enforcement computer systems and databases. He obtained information from these protected systems, which he then provided to a Los Angeles private investigation firm in return for at least $22,500 in secret payments.

Ensuring that those within your agency honor privacy restrictions is essential. They cannot honor that which is not clearly defined and articulated.

A private investigator hired by an obsessed fan was able to obtain the address of television and film star Rebecca Schaeffer through her California motor vehicle records. The fan used this information to stalk and to kill Schaeffer. The Driver's Privacy Protection Act (Public Law 103-322) was passed in 1994 in reaction to this stalking death, enhancing the privacy protections for driver's license information.

Having good information quality and privacy controls in place will help to reduce the possibility of agency criticism and can help defer criticisms when they occur.

An Ohio man's social security number was accidentally associated with another individual's criminal history record. After losing his job, home, and family, the man became aware of the mistake within a law enforcement information system. While the man was able to have the data corrected within the law enforcement system, he was unable to reverse—or even stem—the continuing damage caused by the mistake. The false information was contained in data sold to private information vendors that was, in turn, distributed nationally. There was no way to trace all disseminations of the erroneous information. At any time, the erroneous information can resurface to falsely attribute this man with a criminal history record.

Ensuring the accuracy of data your agency creates, compiles, and distributes is crucial. Failure to do so can have severe impact on the lives of innocent people.

Recently, the Texas Department of Public Safety proposed incorporating facial recognition biometrics into its driver's license photograph database to help stop the issuance of licenses to those using deception or fraud. The proposal passed with little debate in the Texas Senate but came to an abrupt halt in the Texas House of Representatives. Privacy-related concerns about the use of new technology, raised by the American Civil Liberties Union (ACLU) and others, led to a lopsided defeat of the proposal. Concerns about what the system "might" do overshadowed the value of what it was intended to do.

Ensuring that controls are in place for how information is used in your agency will assist your agency in justifying new initiatives and answering concerns about potential abuses of information.

These case studies highlight the importance of addressing privacy concerns when collecting, using, and disseminating **personally identifiable information**. Privacy and information quality ***are*** issues that ***must*** be addressed within every agency in the criminal justice system.

Moving From Concept to Action

The case for maintaining effective policies related to privacy and information quality has been made. Now, how should an agency respond? By ensuring that it has in place appropriate and relevant policies addressing the management of information. The following is a blueprint for agency action.

Start Right: Assign the Task to an Influential Member—

The development of privacy policies must be assigned to someone with the ability to "stick to the task" and remain focused on what needs to be done. Unless the person assigned this task is recognized as having a high level of authority, it may be difficult to obtain acceptance of the efforts made. This project manager should be a person who has the power to enlist the assistance of others within the organization to undertake the analysis and implement the efforts needed to systematically develop the policies and procedures. The project manager should be a person who can directly report to chief policymakers and chief administrators, while at the same time holding others accountable for their efforts, in order to ensure that the project remains on task. The project manager must be able to build an effective project team to make the effort successful in a reasonable length of time.

Have a Good Foundation: Establish a Project Team—

A project team should include stakeholders from within the agency

who are affected by privacy and information quality issues. A typical team will include technical staff familiar with system development and operation; those who use the system(s) regularly in their work; agency legal staff; persons able to craft policy language in a manner consistent with agency formats and expectations; and others having a key role in the agency's collection, maintenance, use, dissemination, and retention of information.

Use a Systematic Approach: Begin the Efforts—

- *Recognize the Stakes:* Implementation of new technologies may promote cost savings and efficiency yet still run afoul of privacy concerns and objections. Unaddressed privacy issues can overwhelm the arguments of benefits and cost savings in support of new technologies. If policymakers and the public are not comfortable with an agency's ability to responsibly handle information, the concerns and fears expressed by even a few opponents can lead to rejection of sensible initiatives.

- *Define Broad Objectives and Risks:* Early in the process, in considering the agency's mission and the substance of its initial efforts, the team should develop broad policy objectives and determine the risks to both public safety and protection of individual rights. Do not forget to include analysis of victims' issues when defining risks. Victim-related information requires careful privacy policy consideration; violations of personal privacy may mean life or death for victims of domestic violence and other crimes.

  Once the policy objectives are developed, the agency's top policy leaders (e.g., key legislators, executive branch heads, court administrators, or chief judges/ justices) should be given an opportunity to endorse the objectives. With this agency buy-in of broad objectives and goals, actual policy development or revision can begin. Decisions should reasonably balance efforts to protect individual rights against the overall public safety mission of the agency and justice system. The risks inherent in any determination should be carefully evaluated and considered.

- *Capitalize Upon the Value of External Input:* An important early step in the development or revision efforts is to seek outside input from legislators, community advocates, victims' advocates, media representatives, privacy advocates, commercial information services sector members, representatives of agencies with whom you share information, and citizens or other interested parties. Broad stakeholder input will help define the focus of your efforts, provide innovative ideas, and support final decisions and plans. You should invite input from those who will use the information your agency maintains, as well as from those who may be critical of your agency's efforts.

  The input of these "outside sources" can help the project team obtain a balanced perspective and become aware of areas or concerns that might otherwise be overlooked. Opposition to or support for initiatives can come from unexpected places; therefore, including sources in the information-gathering stage that are likely to criticize, oppose, or support your policy efforts may help you identify and address issues more effectively. Involvement in the process that leads to a sense of policy "ownership" promotes the overall integrity of the initiative.

- *Define Applicable Laws and Regulations:* An essential early task is the review and identification of all relevant privacy laws and regulations. Every agency should be mindful of legal and regulatory obligations or restrictions applicable to agency operations. Privacy impact assessments may be required by law or regulation. Major policy issues, such as those related to public access to information, disclosure of information solely at agency initiative, protection of sensitive or confidential information, and public notification laws, need to be considered. Provisions of law or rule will need to be interpreted and applied to agency actions. This may be one of the more difficult steps in the overall effort, since there are a myriad of laws and regulations that affect information management and privacy. Some states and other jurisdictions now have chief privacy officers who may provide assistance in these efforts.

- *"Chart" Your Information Flow and Processes:*[3] Having a comprehensive understanding of the flow of information and information processes within your agency is essential. Creating "data and information flowcharts" that identify key points when privacy issues are implicated will assist in gaining that understanding. The chart should indicate when privacy or information quality issues are

implicated by the collection, use, or dissemination of personal information. To the extent possible, your agency should create audit logs or trails to track what personal information is being accessed and by whom. When an agency shares or obtains information with others outside the agency, a separate analysis of that data and information flow should be completed. Any comprehensive privacy or information quality policy must address the key points in the flow of information.

- *Apply "Fair Information Practices" Guidelines:* Any review of privacy and information quality principles should consider what are referred to as "Fair Information Practices," or FIPs. These eight basic FIPs were developed and formalized in the early 1980s to address issues related to the commercial use and sharing of personally identifiable information. Although the FIP guidelines are over 20 years old and were developed in a commercial context, they still constitute the basis upon which sound information quality and privacy policies can be developed. Since the FIPs are well known and widely accepted, outside interests reviewing your policies are likely to use them when providing input or voicing criticism. The FIPs are designed to:

  1. Define agency purposes for information to help ensure agency uses of information are appropriate. ("Purpose Specification Principle")
  2. Limit the collection of personal information to that required for the purposes intended. ("Collection Limitation Principle")
  3. Ensure data accuracy. ("Data Quality Principle")
  4. Ensure appropriate limits on agency use of personal information. ("Use Limitation Principle")
  5. Maintain effective security over personal information. ("Security Safeguards Principle")
  6. Promote a general policy of openness about agency practices and policies regarding personal information. ("Openness Principle")
  7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. ("Individual Participation Principle")
  8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. ("Accountability Principle")

  Each agency must evaluate the applicability and appropriateness of these FIPs in the context of its mission and responsibilities. The FIPs provide a framework for a systematic review of privacy and information quality policies and practices. They help agency leaders to understand which information quality and privacy protection efforts are important and needed. However, the FIPs are guidelines, not absolutes. For example, some agencies may need to ensure that articulation and policy implementation of the "Use Limitation Principle" do not unduly restrict the agency's use of information. The eight FIPs are summarized at the end of this document.

- *Implement, Train, and Hold Accountable:* The team should develop a training plan that will reach all within the agency who will be responsible for implementing or abiding by the privacy policies.

The training plan should take into account the role and duties of those being trained. Methods of holding agency members accountable for abiding by the policies should be identified and incorporated into training. For example, unauthorized access to an agency's data or information by an agency member may form the basis for internal discipline but may *also* constitute a criminal violation of state law. The ramifications of a violation of the agency privacy policy should be clearly identified in agency training. Agency personnel should be required to engage in "refresher training" from time to time.

- *Test and Evaluate:* Finally, once implemented, the developed policy should be tested to determine whether it truly results in the anticipated privacy protections. A programmed review of the results of the policy implementation, including a planned feedback mechanism, should be factored into the policy itself. Each policy should be reviewed on a regular basis to ensure it continues to address changes in the law, as well as current agency practices. In addition, the review should include analysis of technological advancements that may enhance implementation of the policy. One method of ensuring such review is to "sunset" the policy on a certain future date, requiring the policy to be reviewed and renewed prior to its expiration.

Conclusion

Modern information management realities demand that agencies develop and implement comprehensive privacy and information quality policies, incorporating good information practices and design principles. Many agencies have few (if any) policies in place, while others may be dealing with privacy and information quality issues on a case-by-case basis. A systematic, developmental approach will ensure that issues and concerns are addressed before individual harm occurs or practices become a matter of agency or administrator embarrassment, criticism, or liability.

By initiating the development of comprehensive privacy and information quality policies in a systematic manner, policymakers and chief administrators can help ensure that their operations reasonably and fairly address privacy and information quality concerns. The careful selection of a high-level project manager and implementation of a balanced project team approach will significantly enhance the opportunity for the effort to be successful. Use of generally recognized FIPs to structure the policy development will facilitate the overall effort.

To assist those assigned the responsibility of implementing the approach suggested here, a ***Privacy Policy Development Guide*** is being developed to better outline the process and provide access to supplementary resources. These additional tools will facilitate actual privacy and information quality policy development or the review of these efforts. The Guide is designed to help those in charge handle their important privacy-related activities efficiently and effectively.

Footnotes

1 DOJ's Global Advisory Committee has formed working groups to handle both information sharing "security" and "privacy" issues. Please see "Global Resources for the Justice Decision Maker" at the end of this document for further information.

2 Many agencies have what is labeled a "privacy policy." In reality, many of these policies simply address the process by which outside entities obtain information from the agency under the federal Freedom of Information Act or the local "public records access" equivalent. While having a policy that defines information disclosure under applicable public records law is an aspect of a systematic approach to privacy and data management, such a policy does not address the issues and concerns that are the focus here. Such a policy is a step in the right direction but does not complete the journey.

3 SEARCH, The National Consortium for Justice Information and Statistics (with funding from the Bureau of Justice Assistance) has done extensive work with the Justice Information Exchange Model (JIEM) Project to facilitate the charting of your information flow. Information about the JIEM Project, including project documents and training opportunities, is available at www.search.org/integration/info_exchange.asp.

Fair Information Practices—Basic Principles

1. *Purpose Specification Principle*
   Identify the purposes for which all personal information is collected, and keep subsequent use of the information in conformance with such purposes.

2. *Collection Limitation Principle*
   Review how personal information is collected to ensure it is collected lawfully and with appropriate authority, and guard against the unnecessary, illegal, or unauthorized compilation of personal information.

3. *Data Quality Principle*
   Implement safeguards to ensure information is accurate, complete, and current, and provide methods to correct information discovered to be deficient or erroneous.

4. *Use Limitation Principle*
   Limit use and disclosure of information to the purposes stated in the purpose specification, and implement realistic and workable information-retention obligations.

5. *Security Safeguards Principle*
   Assess the risk of loss or unauthorized access to information in your systems, and ensure ongoing use conforms to use limitations.

6. *Openness Principle*
   Provide reasonable notice about how information is collected, maintained, and disseminated by your agency, and describe how the public can access information as allowed by law or policy.

7. *Individual Participation Principle*
   Allow affected individuals access to information related to them in a manner consistent with the agency mission and when such access would otherwise not compromise an investigation, case, court proceeding, or agency purpose and mission.

8. *Accountability Principle*
   Have a formal means of oversight to ensure the privacy and information quality policies and the design principles contained therein are being honored by agency personnel.

Global Resources for the Justice Decision Maker

Visit www.it.ojp.gov/global

United States Department of Justice

Since 1998, the U.S. Department of Justice's (DOJ) **Global Justice Information Sharing Initiative (Global) Advisory Committee** (GAC or "Committee") has concentrated its diverse expertise on challenges to and opportunities for justice and public safety data exchange. Members of this federal advisory committee actively pursue broadscale information sharing, communicating their recommendations directly to the nation's leading justice official—the U.S. Attorney General.

Being intimately acquainted with practitioners' demands, GAC representatives are particularly gratified to support the development and distribution of resources for those in the field—they, too, are producers, consumers, and administrators of the same crucial justice-related data.

To use an automobile analogy, ***Privacy and Information Quality*** concerns are just one wheel on the Global car. ***Intelligence, Infrastructure/Standards,*** and ***Security*** solutions are necessary to drive justice information sharing forward. To that end, GAC's advice and counsel have yielded the following resources to help justice officials make the best business decisions possible:

- The ***National Criminal Intelligence Sharing Plan*** (Plan) provides a cohesive vision and practical solutions to improve law enforcement's ability to detect threats and protect communities. The office of the U.S. Attorney General has endorsed the Plan and is committed to making the resources available to carry out its goals.

- The **Global Justice Extensible Markup Language (XML) Data Model (Global JXDM)**—What began in March 2001 as a reconciliation of data definitions evolved into a broad endeavor to develop an XML-based framework to enable the entire justice and public safety community to effectively share information at all levels of government—laying the foundation for local, state, tribal, and federal justice interoperability.

- ***Applying Security Practices to Justice Information Sharing*** is a field compendium of current best practices and successful models for justice-related information technology (IT) security. The publication covers key IT security topics from detection and recovery to prevention and support.

- The **Justice Standards Clearinghouse for Information Sharing** is a Web-based standards clearinghouse promoting a central resource of information sharing standards and specifications that have been developed and/or implemented across the nation.

- The **OJP IT Initiative/Global Justice Information Sharing Initiative Web site** is a comprehensive "one-stop shop" developed for interested justice and public safety practitioners at all levels of government and all stages of the information sharing process. In addition to housing the resources outlined above, topics include:

  - GAC publications, minutes, presentations, and announcements.
  - Featured information sharing initiatives and organizations.
  - Computer system information exchange processes.
  - New policy and technology developments.
  - Model information sharing systems.
  - Information sharing "lessons learned."
  - Promising practices.
  - Peer-to-peer networking.
  - Events calendar.
  - Latest justice IT news.

For updates and access to all above resources, visit www.it.ojp.gov/global. To speak with someone about DOJ's Global Initiative or GAC events—including biannual GAC meetings open to the public—or obtain hard copy documents, please call Global staff at (850) 385-0600, extension 285.

BJA

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