Global Justice Information Sharing Initiative
United States Department of Justice

Executive Summary for Justice Decision Makers:

Privacy, Civil Rights, and Civil Liberties Program Development

Decision makers within the justice and public safety communities must vigorously protect information privacy, civil rights, and civil liberties. Establishing and implementing these protections will guide an agency's information gathering and collection, storage, and sharing efforts and strengthen trust and public confidence by promoting effective and responsible sharing of information that supports fundamental privacy concepts. Difficult? Yes. Insurmountable? No.

What Is Privacy?

Privacy is a core right protected by federal and state constitutions and expected by citizens. Protecting information privacy, a subset of broader privacy interests, is a fundamental responsibility of justice agencies that collect and share personally identifiable information. Privacy is not just the right to be left alone or the right to be free from unreasonable searches and seizures or the freedom of association. Rather, privacy also includes the fair gathering, collection, and use of personally identifiable information. Privacy policies articulate appropriate gathering and collection of and allowable uses for information and provide accountability for misuse.

What Are Civil Rights and Civil Liberties?[1]

The term "civil liberties"[2] generally means the freedom from intrusive or undue government interference, while "civil rights"[3] refers to the rights of individuals to participate fairly and equally in society and the political process. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Privacy, civil rights, and civil liberties interests—or "privacy" interests—embrace all privacy interests, whether rooted in civil rights law, civil liberties guarantees, or the protection of information privacy interests of individuals or organizations.

What Are the Risks of Not Having Privacy Protections?

Given today's enhanced ability to gather, collect, store, and share vast amounts of personally identifiable information, a well-developed privacy, civil rights, and civil liberties protection policy can help an agency prevent problems. Failure to develop, implement, and maintain appropriate protections for both information and use of technology can result in:

- Harm to individuals.
- Public criticism and loss of confidence in and cooperation with the agency.
- Lawsuits and liability.
- Limited ability to share information.
- Proliferation of agency databases with inaccurate or incomplete data.
- Damage to the credibility of agencies that act on inaccurate or incomplete data.

Privacy Scenarios and Their Relation to Privacy Protection Policies

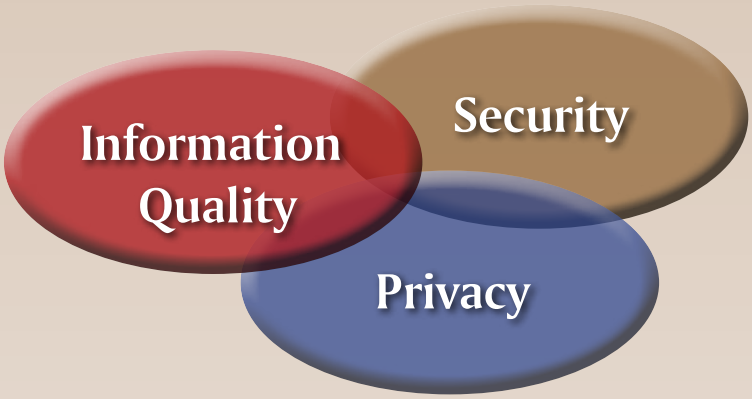
The following are privacy scenarios that can occur in any jurisdiction across the country. Each may have a number of privacy-related consequences, though only one or more are illustrated.

Office of Probation and Parole Sued by Domestic Violence Victim

A domestic violence victim won a lawsuit filed against the department of corrections' probation and parole office and received $250,000 in damages after being revictimized by her ex-spouse, a probation officer who accessed her information in a database containing her new address. The couple had recently divorced because of reports of repeated domestic violence, and the woman had moved to a different part of the state. Despite the allegations, the department had not limited the officer's system access or permissions, nor had the woman's electronic record been assigned proper security to ensure that the location of her new residence was withheld from unauthorized access. The probation officer was fired and is awaiting criminal proceedings.

Consequence: Harm to individuals and financial costs for the agency.

(continued on page 3)



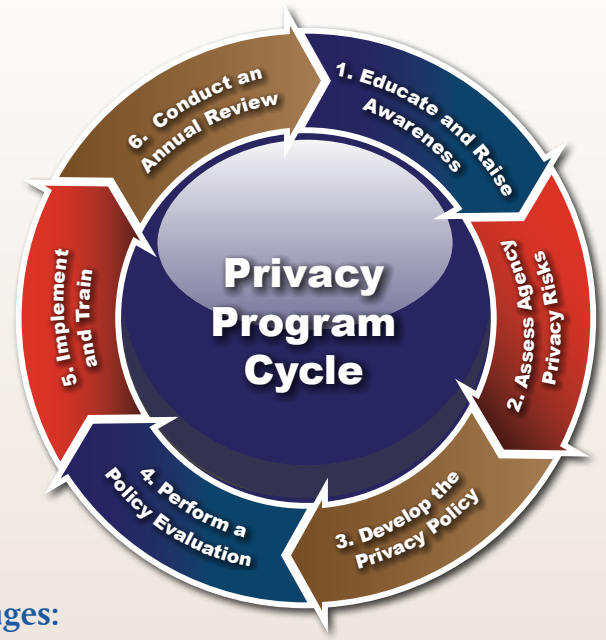
How Does Privacy Intersect With Information Quality and Security?

Information quality plays an extremely important role in the protection of privacy rights of individuals. Issues of privacy and information quality (IQ) are inherently linked, because both influence the appropriate use of justice information. Entity privacy policies should address information quality issues. In practice, the accuracy, timeliness, completeness, and security of information connected to an individual or organization may raise as many concerns as the release of the information or its public availability.

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. Security policies implement privacy policies by ensuring compliance with the manner and extent to which information is allowed to be shared by the privacy policies. Having a security policy related to data or information is not enough. Security policies alone do not adequately address the privacy, civil rights, civil liberties, and IQ issues contemplated in this discussion. 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 both in procedures and in system processes.

What Can You Do to Establish Privacy Protections?

Privacy is not a project; privacy is an ongoing program. As entities consider establishing and implementing privacy protections for the information they collect, store, maintain, access, and share through their business processes and procedures, they are encouraged to follow the stages recommended in the Privacy Program Cycle.



Stages:

1. **Educate and Raise Awareness** on the importance of having privacy, civil rights, and civil liberties protections within the agency.
2. **Assess Agency Privacy Risks** by evaluating the process through which your agency collects, stores, protects, shares, and manages information.
3. **Develop the Privacy Policy**[4] to articulate the legal framework and policy position of an organization on how it handles information the agency seeks or receives and uses in the normal course of business.
4. **Perform a Policy Evaluation** to determine whether the privacy policy adequately addresses current standards and privacy protection recommendations.
5. **Implement and Train** personnel and authorized users on the established rules and procedures.
6. **Conduct an Annual Review** and make appropriate changes in response to implementation experience, applicable law, technology, and public expectations.

Why Develop Privacy Policies?

A comprehensive privacy program serves as a fundamental lynchpin to developing a system of trust that allows agencies to share personally identifiable and other sensitive information. There needs to be trust—not only within and between justice partners sharing information but also by the public, whose information is being collected and utilized—that justice agencies are serving as responsible stewards of their personally identifiable information and operating with respect for individual privacy and the law. Without this trust, information sharing initiatives will not thrive and are ultimately doomed to public condemnation and civil liability.

Where to Turn for More Information

To support justice agencies in their efforts to implement privacy, civil rights, and civil liberties policies and protections for the information they collect, store, maintain, access, and share, the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) has published a *Global Privacy Resources* booklet as a road map to guide justice entities through the diverse resources available for each stage of the Privacy Program Cycle. The resources presented are developed for state, local, and tribal (SLT) entities by DOJ's Global or Global partners or through DOJ collaborations with other federal agencies, such as the U.S. Department of Homeland Security (DHS). To view this *Global Privacy Resources* booklet, as well as all resources for a Privacy Program Cycle, refer to www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

Privacy Scenarios and Their Relation to Privacy Protection Policies (continued from page 1)

Report Details Missteps in Data Collection

Intimate information was collected about the lives of 52,000 people and stored in an intelligence database accessible to about 12,000 federal, state, and local law enforcement authorities and to certain foreign governments. This organization did so without systematically retaining evidence that its data collection was legal, without ensuring that the data it obtained met its needs or requests, without discovering or reporting abuses, without providing clear policy guidance, and without following retention regulations. Lawmakers called the violations unacceptable and permanently shut the database down. **Consequence: Loss of ability to gather information.**

Judge Limits Police Taping

In rebuke of a surveillance practice greatly expanded by a police department after the September 11 attacks, a federal judge ruled that police must stop the routine videotaping of people at public gatherings unless there is an indication that unlawful activity may occur. In the ruling, the judge found that the police department had not followed established guidelines under which police are allowed to conduct investigations, including videotaping of political events only if there are indications that unlawful activity may occur and only after obtaining the proper permissions, neither of which had occurred. **Consequence: Loss of public confidence in law enforcement and loss of support.**

Officer Leaks Suspicious Activity Report Details

While socializing with a friend after work, a police officer talked about a suspicious activity report he had read in which the friend's neighbor was suspected of a possible sex crime involving young teens. That privacy breach quickly turned into a rumor that spread throughout the community. The person said to be a suspect, as well as his family members, immediately became victims of harassment and the brunt of jokes around town. Less than a week later, the investigation revealed that the neighbor was not the perpetrator but, in fact, it was someone who had traveled to the community from a neighboring state. Even though the rumor proved false, the casual leaking of information caused permanent damage to the reputation of the individual and his standing in the community. **Consequence: Demonstrable harm to an individual's reputation and loss of public trust in the agency.**

About Global

www.it.ojp.gov/global

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

DOJ's Global Advisory Committee (GAC) recommends that local, state, tribal, and federal justice decision makers make privacy protections a priority. Global supports the initiatives of DOJ and aids Global member organizations and the people they serve through a series of important collaborative efforts. These include the facilitation of Global working groups.

About the Global Privacy and Information Quality Working Group (GPIQWG)

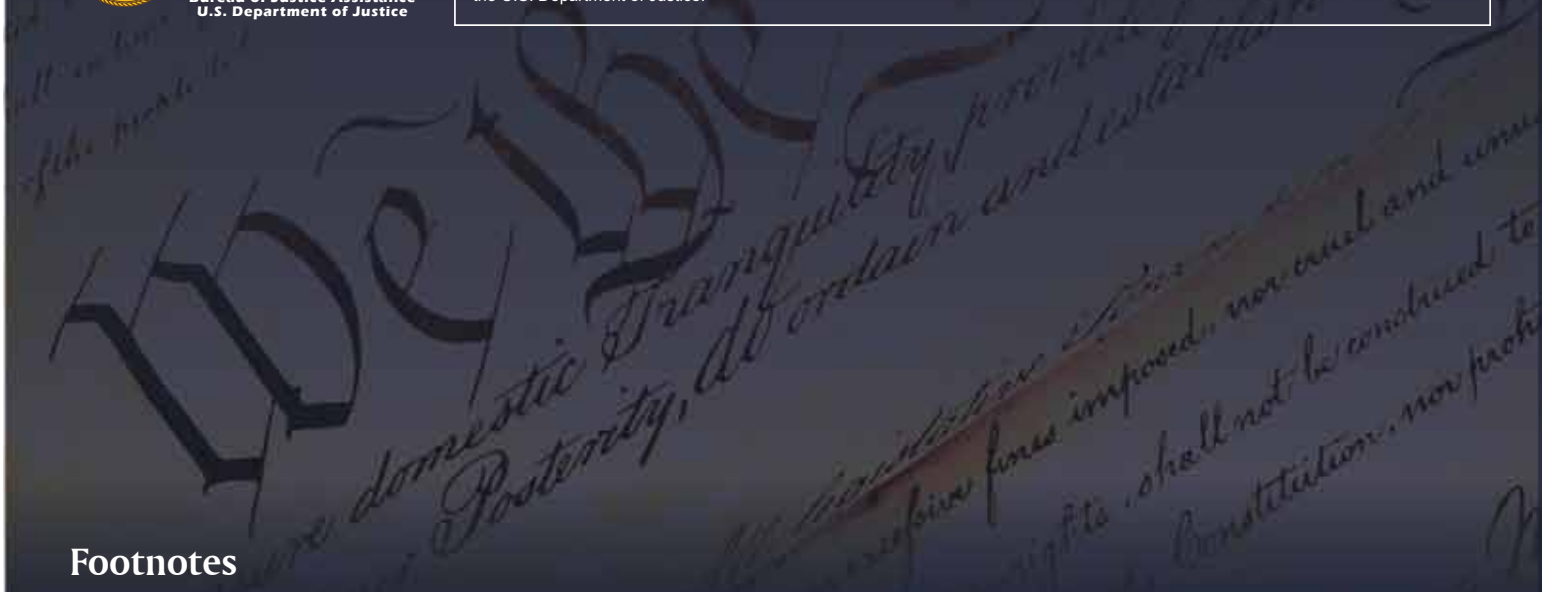
www.it.ojp.gov/privacy

The Global Privacy and Information Quality Working Group (GPIQWG) is one of five Global working groups. GPIQWG is a cross-functional, multidisciplinary working group of Global and is composed of privacy and local, state, tribal, and federal justice entity representatives covering critical topics such as intelligence, biometrics, information quality, privacy, civil rights, and civil liberties. GPIQWG assists government entities, institutions, and other justice agencies in ensuring that personally identifiable information is appropriately collected, maintained, used, and disseminated within evolving integrated justice information systems.

GPIQWG, on behalf of DOJ's Global, developed this executive summary to support justice agencies in their efforts to educate agencies and raise awareness of the importance of establishing and implementing a privacy program.

BJA
Bureau of Justice Assistance
U.S. Department of Justice

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, 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 publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.



Footnotes

1 For more information on privacy, civil rights, and civil liberties, refer to the U.S. Department of Justice (DOJ) Global Justice Information Sharing Initiative's (Global's) *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*, Section 4: Understanding Foundational Concepts.

2 According to DOJ's Global, the term "civil liberties" refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

3 The term "civil rights" refers to those rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. These civil rights to personal liberty are guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

4 The authors acknowledge that agencies may already have privacy policies in place (for example, in Standard Operating Procedures) that may need to be reviewed and updated as part of this step in the Privacy Program Cycle.

rev. 9/6/11