Global Justice Information Sharing Initiative

Privacy and Information Quality Working Group Meeting Summary

Williamsburg, Virginia
February 26, 2004

Meeting Background, Purpose, and Introductions

The Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), convened the Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG or "Working Group") meeting on February 26, 2004, in Williamsburg, Virginia. This location was selected to facilitate GPIQWG members' attendance at the *Conference on Privacy and Public Access to Court Records*, sponsored by the Courtroom 21 Project, held February 27-28, at the College of William and Mary Law School.

The Working Group primarily convened for the purpose of reviewing and gathering Group input on integrated justice privacy and data quality policy, specifically toward the release of two Global-facilitated resources:

1. The *Privacy and Information Quality Policy Development for the Justice Decision Maker* ("Paper I" or "Policy Paper") – a high-level overview document aimed at the justice executive, underscoring the need for privacy policy development and outlining fundamental steps toward that goal.

2. The *Privacy and Information Quality Policy Developer's Sourcebook* ("Paper II" or "Sourcebook") – a more exhaustive, practical, "hands-on" companion tool to the privacy policy document, building on the principles enumerated in Paper I.

Mr. Cabell Cropper, GPIQWG Chair and Executive Director of the National Criminal Justice Association, chaired the meeting and set forth the following agenda and key discussion points:

- Global Privacy and Information Quality Working Group 2004
  - Report on the Global Executive Steering Committee (GESC) Strategic Planning Session
  - Discussion of Activities and Priorities Suggested by GESC

- Document Review: *Privacy and Information Quality Policy Development for the Justice Decision Maker*
  - Final Review and Feedback
  - External Vetting Strategy
  - Distribution Strategy

- Resource Development: The *Privacy and Information Quality Policy Developer's Sourcebook*
  - Discuss Draft Table of Contents
  - Identify Resources
  - Assignments and Timeline

- Use Limitation Principle
  - Application to the Justice Field

- Next Steps, Next Meetings

Chairman Cropper invited participants to introduce themselves and share their areas of interest relating to privacy and information quality. Mr. Patrick McCreary, Bureau of Justice Assistance, OJP, offered welcoming remarks, commenting that in the coming year, privacy issues will be "one of the most visible areas of concern" for justice information sharing. He complimented Chairman Cropper's leadership in tackling this important issue, noting that the Working Group's approach, "leveraging ongoing efforts, collaborating, epitomizes what we are trying to do with Global." The following individuals were in attendance:

Mr. Robert Boehmer
Illinois Criminal Justice Information Authority
Chicago, Illinois

Mr. David Byers
Arizona Supreme Court
Phoenix, Arizona

Mr. Alan Carlson
The Justice Management Institute
Kensington, California

Mr. Steven Correll
National Law Enforcement Telecommunication System
Phoenix, Arizona

Mr. Cabell Cropper
National Criminal Justice Association
Washington, DC

Mr. John Greacen
Greacen Associates, LLC
Santa Fe, New Mexico

Mr. John Jersernik
Illinois State Police
Joliet, Illinois

Ms. Rhonda Jones
National Institute of Justice
Washington, DC

Ms. Kate Lubanovic
Sysinct
McLean, Virginia

Mr. Patrick McCreary
Bureau of Justice Assistance
Washington, DC

Ms. Jeanette Plante
Executive Office for United States Attorneys
Washington, DC

Mr. Michael Ramage
Florida Department of Law Enforcement
Tallahassee, Florida

Ms. Donna Rinehart
Institute for Intergovernmental Research
Tallahassee, Florida

Ms. Cindy Southworth
National Network to End Domestic Violence Fund
Washington, DC

Ms. Martha Steketee
National Center for State Courts
Arlington, Virginia

Ms. Mary Gay Whitmer
National Association of State Chief Information Officers
Lexington, Kentucky

Global Privacy and Information Quality Working Group 2004

In December 2003, the GESC held a focused strategic planning session to forecast activities for the upcoming year. At this meeting, the GESC developed a "wish list" of activities for all the working groups, including GPIQWG. Chairman Cabell presented this list to the attendees, requesting that they prioritize the items by considering importance, feasibility/locus of control (i.e., is the task within GPIQWG purview?), and adherence to and alignment with the GPIQWG *Vision*[1] and *Mission*[2] *Statements*.

The following tasks were considered:

1. *Policy Paper* – due April 2004.
2. *Sourcebook* – due October 2004.
3. Global privacy summit – late 2004.
4. Privacy best practices case study.
5. Development of data quality minimum standards.
   a. Auditing standards.
   b. Certificate of accuracy for data entry to registries.
6. Collection of privacy policies for statewide Criminal Justice Information Services (CJIS) entities.
7. Review of compendium of privacy legislation/resources.
8. Document research for relevant privacy case law.
9. Enlistment of GPIQWG as outreach resource for justice community.
10. Support of the development of training.
11. Monitoring of the progress of privacy certificates.

In order of priority, tasks 1, 2, 5 (via a scoping paper) and 3 were determined as of the highest importance and relevance to group members. Tear-sheet notes on several of these items are included in *Appendix A*. The remaining majority of the meeting was devoted to tasks 1 and 2.

Privacy and Information Quality Policy Development for the Justice Decision Maker

As determined at previous Working Group meetings, the first of two deliverables due to the Global Advisory Committee (GAC) is a brief informational policy paper for decision makers explaining essential privacy policies and the systematic steps to pursuing a policy. Per input from the GPIQWG, Michael Ramage, Esquire, Florida Department of Law Enforcement Counsel, crafted the privacy policy paper, reviewed and refined the

[1] ***GPIQWG Vision Statement***: To accomplish justice information sharing that promotes the administration of justice and public protection by: 1) Preserving the integrity and quality of information; 2) Facilitating sharing of appropriate and relevant information; 3) Protecting individuals from consequences of inappropriate gathering, use, and release of information; and 4) Permitting appropriate oversight.

[2] ***GPIQWG Mission Statement***: To advance the adoption of privacy and information quality policies by justice systems participants that promote the responsible collection, handling, management, review, and sharing of (personal) information about individuals.

piece with assistance from a Working Group task team, and released the polished draft prior to this meeting for discussion[3] in Williamsburg.

Suggestions, questions, and discussion included the following:

General Comments

⇒ ***Purpose:***
Keep in mind the desired outcome: This paper should inspire an agency head to 1) read the material and 2) take action – assign staff to refine, develop, and/or appreciate the necessity of privacy policies. To that end, encouraging the reading of the material is the first step (see "Tone and Language," following).

⇒ ***Approach – Integrating Privacy Policies Into the Larger Global Picture:***
Privacy is the fourth wheel on the Global car. In addition to the other tools/substantive areas the Global group is addressing? e.g., data issues (Global Extensible Markup Language [XML] Justice Data Model [Global JXDM]), Web services, architecture, security? an integral component ("the fourth wheel") of justice-related information sharing is "privacy." All components are necessary.

⇒ ***Tone and Language*:**
The language is somewhat stilted and bureaucratic for the purpose of the document (an advocacy piece). The ideas are all correct and in the right order, but this piece needs to be "a grabber." Suggestion: Dedicate an editor to incorporate punchier language, a style that "leaps off the paper" and inspires top people to say, "This is what we need to do; now find a way to do it." The format suggestion (see "Format," following) is a complementary critique.

⇒ ***Format:***
Two options:
1) Brochure look and feel – substantive in content, but "flashy" and easy-to-read (e.g., bullets, pull-quotes)
2) Monograph format – while more interesting than an unformatted piece, this approach retains some of the formality, lending an air of gravitas.

⇒ ***Audience:***
Question: Are we writing to a "single-agency" audience (i.e., promoting developing ***intra-agency*** privacy policies) or promulgating "multiple agency"/***interagency*** (e.g., statewide, regional) privacy policy development? This question needs resolution.

Specific Sections

Participants proffered feedback on particular sections or portions of sections including:

[3] Due to weather conditions, Mr. Ramage was delayed in his arrival. Paper I revision suggestions were documented, and a subsequent conference call was arranged between Mr. Ramage, GPIQWG leaders, select members, and Global staff in the pursuit of refining the privacy policy paper.

⇒ ***Executive Summary:***
Suggestions included:

- Changing the title to "Highlights."
- Inserting language enumerating "what this paper is designed to do."
- Revising treatment of the Fair Information Practices (FIP) principles.
  - Six versus eight FIPs listed.
  - Although consensus upheld the importance of including FIPs as a historical reference within the body of the paper, they should *not* be listed in the Highlights section.
- Further defining "personally identifiable information."
- Striking a more optimistic tone.

Several Working Group members volunteered to rework the "Highlights" language.

⇒ ***Introduction:***
To counter potentially aversive reactions to privacy challenges raised by this document (i.e., several participants noted that if faced solely with caveats, an executive might decide that information sharing is simply too risky), it was suggested that the Introduction stress the need for justice-related information sharing. This point does not need extensive treatment (most agree this is a foregone conclusion), but some mention of the fact ". . . that the justice community has been moving that way for some time – and has hastened efforts in the post-9/11 environment – sets a good stage. 'There is a lot of benefit to sharing information, and good things are happening, but there are pitfalls.'"

⇒ ***Case Study Examples:***
- Currently, all the scenarios are "negative." Participants suggested including a "positive" example: "how a privacy policy has *worked*."
- Include a data quality example.
- The last example (corrections) is not especially concerned with a justice issue and, perhaps, should be deleted.
- There is no need to use citable examples; scenarios can be "based-on" in nature.
- Several Working Group members volunteered to refresh this section.

⇒ ***Questions: "You should be concerned if…" Section:***

Questions four and five should be reworked to be made stronger, more relevant (flesh out), and less ambiguous to answer.

Missing/Underemphasized Sections

⇒ ***Information Quality***
It was suggested that either "information quality" should be removed from the paper's title and treated in a separate effort or language should be added to

address the concept in greater detail. One participant noted, "Getting the ***right*** (read: accurate) data, to the right person, at the right place, at the right time is the difference between a justice system and an ***in***justice system."

⇒ ***Balancing Act: Individual Privacy v. Public Safety***
Language should be added noting the increasingly complex demands of balancing the protection of individuals' privacy versus the pursuit of public safety (e.g., employers' need-to-know/right-to-know about backgrounds of potential child care worker or bus drivers).

⇒ ***Memorandums of Understanding/Privacy Policy Negotiations***
If it is determined the audience for Paper I is multiagency in nature, a section concerning this issue is necessary.

As noted above, several issues were in need of resolution to direct the ultimate revision of Paper I. GPIQWG participants agreed to leave these determinations to the discretion of Working Group leaders and principal authors Mr. Ramage and Mr. Alan Carlson, Executive Director, Justice Management Institute.

Vetting and Distribution:

Attendees discussed an external vetting strategy. Resolution: Once Paper I is accepted by the GAC (requiring a formal recommendation by Chairman Cropper or his proxy and sustaining GAC vote), the document will be reviewed by the wider justice community following the paradigm established by the Global Security Working Group (GSWG) for the *Applying Security Practices to Justice Information Sharing*[4] document:

- Review-request letters are sent to each GAC representative (formatted for members' respective signatures) for use as cover in distributing the paper within their constituency.

- Review-request letters are sent to targeted recipients (e.g., international agencies).

- Reviewers provide feedback to Global staff, who coordinate revision of the document according to Working Group direction.

Steven E. Correll, Executive Director, National Law Enforcement Telecommunication System and GSWG chair, outlined the process and answered review and distribution questions. The GSWG resource, produced in both hard copy and CD formats, has been widely distributed at justice-related conferences and trainings. The privacy policy paper will employ these methods, as well as exploring utilization of the DOJ-sponsored National Criminal Justice Reference Service (NCJRS).[5]

[4] Available at http://it.ojp.gov/documents/asp/.
[5] More information on NCJRS is available at http://www.ncjrs.org.

Privacy and Information Quality Policy Developer's Sourcebook

Mr. Ramage led the *Sourcebook* development discussion. As previously noted, this will be a practical tool akin to the GSWG *Applying Security Practices* CD. A chief component will be a resource section, and in that regard, members' assistance will be solicited to provide these materials in all forms – documents, Web sites, contact information, excerpts of materials. Prior to the meeting, Mr. Ramage developed a fairly extensive, annotated Table of Contents *(Appendix B)*, which was distributed electronically in advance of the meeting. GPIQWG members discussed the outline and accepted assignments to flesh out the various sections. A deadline of October 2004 was set for initial *Sourcebook* presentation to the GAC.

"Use Limitation" Principle

Privacy policy development in a variety of disciplines, including justice, has strong roots in the commercially developed eight FIP principles. One of these—the Use Limitation Principle[6]—can raise challenges when applied to justice data, particularly law enforcement information. (One attendee noted: "You would almost need to be a mind-reader. Law enforcement routinely collects information for one purpose and then realizes that they need to use it for another. . . .")

To address this complexity, GPIQWG Chair Jeanette Plante proposed tackling the "law enforcement exception" to the Use Limitation FIP question. "There is no one-size-fits all, but we can provide some core considerations for those who have to make those decisions." To that end, she suggested:

- Exploring law enforcement FIPs.
- Defining the "law enforcement exception" (or developing questions to assist agencies in self-determining their own definition).
- Discussing with whom law enforcement can share.

Due to time constraints, a more extensive discussion was shelved until a later date. It was determined that Global staff would set up a conference call for interested parties to discuss this issue further after the final revision of Paper I is completed.

Next Steps, Next Meetings

- Conference call to discuss Paper I revision suggestions with Mr. Ramage
  - Time Frame: ASAP
  - Participants: Chairman Cropper, Vice Chairman Plante, Mr. Ramage, Mr. Carlson, and Global staff

[6] To "limit use and disclosure of information to the purposes stated in the purpose specification, and implement realistic and workable information-retention obligations."

- Additional considerations: GPIQWG members with Paper I assignments should submit materials to drinehart@iir.com by **no later** than Monday, March 29, 2004.

- *Policy Paper* presentation to the GAC
  - Time Frame: Spring 2004 GAC meeting
    - April 21-22, 2004

- Conference call to discuss law enforcement exception to the "Use Limitation Principle"
  - Time Frame: After spring GAC meeting
  - Participants: Any interested GPIQWG member

- *Sourcebook* assignments **due**
  - Time Frame: Monday, May 3, 2004

- GPIQWG meeting
  - Time Frame: Friday, May 21, 2004 (tentative)
  - Place: Phoenix, Arizona (tentative)
  - Additional information: Respond to Paper I issues raised by the GAC; continue development of Paper II

- GPIQWG meeting
  - Time Frame: September 2004 (tentative)
  - Place: Albuquerque, New Mexico (tentative)
  - Additional information: Preparation for Paper II presentation at fall 2004 GAC meeting; discussion of information quality scoping paper

Chairman Cropper reviewed the next steps and next meetings for his Working Group members. Paper I and Paper II assignments were delegated. A Global staff-generated e-mail, to follow in the near future, will confirm these assignments and provide additional details. With no further business, Chairman Cropper and Vice Chairman Plante thanked attendees for their participation. The GPIQWG meeting was adjourned.

Appendix A

The following is the Global Executive Steering Committee's "Wish List" of tasks for the GPIQWG and additional notes.

1. ***Privacy Policy Paper* – due April 2004.** *(See body of Meeting Summary.)*

2. ***Privacy Policy Sourcebook* – due October 2004.** *(See body of Meeting Summary.)*

3. **Global Privacy Summit – late 2004.**
   a. **Existing Events.**
      i. Who else is sponsoring privacy conferences? What is their focus?
         1. e.g., International Association of Privacy Professionals
      ii. Infiltrate those agendas tailored to justice constituencies, request time on a program and/or specific GPIQWG Workshop/training event. To support those events, the following could be used:
         1. Papers I and II
         2. Speaker's bureau
         3. Media kit
         4. Canned presentations
      iii. To the "wider world" it shows that the justice community IS doing something about privacy concerns.
   b. **Future Event - Global Symposium.**
      i. Hold workshops/training per Global issues of emphasis/tools developed (e.g., Security Workshop, Global JXDM Workshop).
      ii. Possibly tack onto other established, like-minded event (i.e., the SEARCH Symposium).

4. **Privacy best practices case study.**
   a. Issue: How to find jurisdictions for case studies?
   b. Language: Use "promising practices" instead of "best practices."
   c. Explore the development of privacy policies/processes in examples such as:
      i. MATRIX
      ii. CriMNet/Minnesota – Multiple Jurisdiction Network Organization (MJNO)
      iii. Denver
      iv. Open records versus closed records
      v. States – National Crime Prevention and Privacy Compact Council

5. **Develop data quality minimum standards.**
   a. Auditing standards.
   b. Certificate of accuracy for data entry to registries.
      i. Issues related to "data quality":
         1. Retention
         2. Access
         3. Law enforcement experience with aggregating data – consistency across jurisdictions

4. Common methodology for criminal justice entities versus discipline-specific methodologies
5. Identification examples
6. Data correction/redaction
7. Linking inaccurate data
    a. NCTC compliance with requirements

ii. The task and above issues are to be handled by a **Scoping Paper** examining components of:
1. Auditing
2. Data privacy mechanisms – are they working?
3. Descriptions of new development of data automation and techniques to share and protect data

6. **Collect privacy policies for statewide CJIS entities.**
RE: Repository of Privacy Policies/Legislation/Case Studies
a. A primary issue will be finding an institutional home for such a resource.
b. Include this information in the Paper II/*Sourcebook*.
c. Suggested resources:
i. Family Resource Centers
ii. Family Violence Prevention Fund
iii. National Clearinghouse for Science, Technology, and the Law – Stetson University College of Law
iv. The Center for Democracy and Technology
v. Robert Ellis Smith (author), Privacyjournal.net
vi. National Association of State Chief Information Officers online library
vii. Legal Action Center
viii. HIPAA Academy.Net

7. **Review compendium of privacy legislation/resources.** *(See 6. Collect privacy policies for statewide CJIS entities, above.)*

8. **Research documents about relevant privacy case law.** *(See 6. Collect privacy policies for statewide CJIS entities, above.)*

9. **Enlist GPIQWG as outreach resource for justice community.** *(See 3. Global privacy summit, above.)*

10. **Support the development of training.** *(See 3. Global Privacy Summit, above.)*

11. **Monitor progress of privacy certificates.** (Mr. McCreary will explore work under way in this area to better guide the Working Group members in complementary efforts, if applicable.)

Appendix B

PRIVACY POLICY SOURCEBOOK
Table of Contents

Draft I

I. PURPOSE OF THIS SOURCEBOOK
- Quick summary and overview

II. ACKNOWLEDGEMENTS

III. MESSAGE FROM THE CHAIR

IV. EXECUTIVE SUMMARY

V. INTRODUCTION – Why privacy policies are important and needed

- Enumerates scope of the discussion (i.e., related to "personally identifiable information" generated by, collected, utilized, shared, or disseminated by an agency)
- Defines "personally identifiable justice information"[7]
- Identifies individuals who may have personal privacy interests affected by justice information systems[8]
- Ties into the OJP "Public Attitudes" Survey
  - That is, most of public are "privacy pragmatists" who will support technological change but will require explanation of its value that will offset generally held privacy concerns
- Reinforces "dangers" from *Privacy and Information Quality Policy Development for the Justice Decision Maker* document ("Paper I")
- Stresses key reason an agency should be concerned with privacy policies, such as:
  - Privacy concerns surface regularly in the media and among policymakers
  - "If you do it on your own initiative, you are in control of how policies are developed" versus "if you fail to move, others (e.g., Congress, state legislatures, or state chief privacy officers) may do it for you" and impose limitations or restrictions in a manner that makes information management more complex

---

[7] Information within the justice system that is linked to an individual at the time of release or through analysis can be linked to an individual. Access to personally identifiable information is what generates privacy issues. Examples of personally identifiable information include:
- Law enforcement: police reports, arrests, warrants, personally identifiable or traceable neighborhood/city/county/state crime data, and GIS data;
- Jail: inmate information, pretrial information (scheduling, release);
- Prosecution: indictment/charging document;
- Courts: pleadings, motions, hearing transcripts, trial exhibits, dispositions, judge/attorney/juror information, bond information, protection orders;
- Corrections: inmate information, classification information, gang affiliation;
- Probation/parole: term of probation/parole, sex offender status, violent offender status;
- Victims services: treatment providers, contact information;
- Traditional criminal history record information: some or all compiled information available pursuant to state law; and
- Justice system employee: policies, employee evaluations, employment histories, medical evaluations.

[8] Including victims, witnesses, jurors, law enforcement officers, justice staff, plaintiffs, respondents, attorneys, judges, defendants, offenders, families and associates of these persons, and anyone else who comes in contact with the justice process.

- As states initiate privacy review, an agency's efforts can serve as a model; at a minimum, they can insulate the agency against criticism by anticipating issues and having a corresponding privacy policy in place
- State activity is growing (e.g. Arkansas HB 2247 and New Hampshire HB 64, both of which moved to create commissions to establish privacy standards on information housed in criminal justice system)
- Technology offering greater efficiency and the ability to address fraud may? if privacy concerns are not addressed? run aground because of privacy fears (e.g., Texas SB 945 "driver license biometric" failure)

VI. A FOUNDATION FOR POLICY DEVELOPMENT

- **Subsection A: Restatement of NCJA *Privacy Guideline*,[9] Chapter 3**
  The justice system has a set of unique characteristics that must be taken into account when developing privacy policy. Unlike the commercial sector (in which the Fair Information Practices were developed), criminal justice agencies have a very important goal: protection of society. The right to privacy must be balanced with the need to carry out the administration of justice and its prime goal: protection of society. The way in which a justice agency uses personal information in the administration of justice is vital to the protection of society and can result in life-or-death situations. In addition, there is a need for the public to access personal information where it directly relates to the integrity and effectiveness of the justice system process.
- **Subsection B: Fair Information Practices (FIPs)**
  Introduction and overview
- **Subsection C: The National Situation**
  - No unified approach because no preemptive Federal law
  - Numerous "special topic" Federal laws
    - Summary in Appendix, will briefly address:
      - Gramm-Leach-Bliley Act
      - Children's Online Privacy Act of 1998 (COPPA)
      - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
      - Fair Credit Reporting Act (including 2003 revision)
      - Driver's Privacy Protection Act
      - Family Educational Rights and Privacy Act of 1974 (FERPA)
      - Video Privacy Protection Act
  - Observation: State laws vary greatly and require independent research
    - Referral to "Compilation of State and Federal Privacy Laws" (Appendix)
  - Warning: growing integration of criminal justice information systems may result in existing policies and statutes proving inadequate in handling issues generated by modern information practices
    - Resource: *Privacy Schmrivacy*, pp. 15-16

VII. INITIAL DEVELOPMENT STEPS

1. Getting Started

a. Obtain leadership commitment within the organization
   i. Demonstrable by assignment to formulate a plan or develop policies
b. Obtain commitment from the senior policymakers over the agency
   i. Governor, legislative leaders, chief judge, highest-level policymakers

[9] Located at http://www.ncja.org/pdf/privacyguideline.pdf.

c. Form a good working team, to include the key players identified in **Paper I**
d. "Information steward," empowered within the agency, to head effort
e. Realize FIPs are a framework for continued efforts but know they will need to be modified and adjusted to the individual mission and information practices of an organization
    i. See next section on FIPs
f. Keys to success:
    i. Develop policy as though an agency's harshest critics will be reviewing and evaluating
    ii. Make the development effort one that involves all affected interests in the agency
    iii. Make the policy easy-to-read and understandable
    iv. Use the FIPs as a framework for the effort
    v. Promote the policy with those within the agency
    vi. Promote the policy with key stakeholders and other interested parties
        1. Policymakers
        2. Those with whom information is exchanged
        3. The media
        4. The public
    vii. Update the policy as needed to remain current with changes in agency information practices
    viii. Hold those "responsible parties," as identified by the policy, accountable for "training, explaining, and sustaining"

2. Study the Process Before Beginning It

a. Review NCJA *Privacy Guideline,* particularly Chapter 6
    i. **Review and understand the FIPs**
        1. Reminder: keep FIPs in the context of criminal justice functions. To that end, modify as necessary/appropriate
    ii. Focus particularly on the ***Purpose Specification Principle*****,** since it promotes an interagency review, re: <u>why</u> personally identifiable information is being collected.
        1. This serves as the keystone for further implementation of FIPs
        2. This principle was developed in commercial context and does not easily conform to all efforts of public criminal justice agencies
            a. It may need to be modified to meet the agency's mission and purpose
            b. It may need to include the option to use previously collected information when a new purpose is added to an agency's mission or efforts if other FIP concerns are appropriately addressed

3. Development Process

a. Begin by implementing a process-data and information element analysis
    i. Map the flow of personally identifiable information within the agency
    ii. Assess the sensitivity of personally identifiable information within the agency
    iii. Assess the information "in context" with how the agency handles it (i.e., the context may change even *within the agency*: information may have a certain purpose in one function of an agency but has another purpose in another function. In such cases, a "one-size-fits-all" approach may not be appropriate.)
    iv. Establish a "baseline" policy approach: under state law, are most agency records and information considered "public" or "confidential"? The state "baseline" will define from which perspective a privacy policy will be developed.

v. Ensure all other statutory restrictions affecting an agency's information have been identified
    1. Legal issues
    2. Consistency with overriding legislation

b. Utilize the NCJA "Policy Template" materials, *Privacy Guideline,* Chapter 6
    i. Developing a Purpose Statement
    ii. Determining the Scope of the Agency Policy
    iii. Determining How Information Is Verified, Maintained, and Corrected
    iv. Determining Who Gets Access
    v. Deciding What Information Can Be Accessed and By Whom
    vi. Determining the Method(s) of Access
c. Consider the agency's mission and purposes when creating privacy policy

4. Additional Considerations

a. **Biometrics:** Agency use of biometrics produces personally identifiable information. Such information should be included within the scope of an agency's privacy policy.
b. **Situation Considerations:** Information collected may be such that it can be utilized and shared in some contexts, but not in others.
    i. For example, the Florida Public Assistance Fraud (PAF) Investigative Unit was merged into the Florida Department of Law Enforcement (FDLE). Information available to a PAF investigator is not available to FDLE Special Agents for general investigative use. An internal "wall" between personnel within the same agency (and their allowed uses of information) is required to avoid violating the use limitations re: information provided to PAF investigators from other agencies.
c. **Coordinated Privacy Policy:** If your agency shares personally identifiable information with other agencies, a coordinated privacy approach will be required
    i. NCJA *Privacy Guideline,* Chapter 7, may be of assistance
    ii. Use of Interagency Memorandum of Understanding may be a mechanism to establish basic privacy protections and policies
    iii. Information sharing between states and/or Federal government can complicate the issue
        1. The respective jurisdictions' laws and rules may affect the ability to share, use, or secondarily disseminate information
            a. For example, an individual state's interpretation of Driver's Privacy Protection Act and "dissemination log" requirement
d. **The Internet:** If an agency maintains an Internet presence, special privacy policy considerations must be reviewed in the context
    i. Dedicated Internet section follows later in *Sourcebook*

5. Post-Policy Development Tasks

a. Consider an external policy review and evaluation, even as policy is being developed
    i. Ensure thoroughness
b. Train and educate!
    i. Agency leaders, managers, information workers, and other staffers
    ii. New-employee orientation
    iii. Hold accountable – discipline when violators are identified
c. Public Relations
    i. Make development efforts known; these efforts are "good news," and the public, media, and chief policymakers should be made aware
d. Lead by example
    i. Make basic privacy policies and protections a requirement for information sharing

VIII. IF YOUR AGENCY MAINTAINS AN INTERNET PRESENCE

- It is a good practice to develop an "Internet privacy statement"
- Organization for Economic Coordination and Development (OECD) Privacy Generator
  - Available to assist development of an appropriate statement
  - Prompts inquiries of pertinent issues that should be contained in an Internet privacy statement
    - Sample in *Appendix*, following

IX. APPENDIX AND TOOLS

(Following is an example of the type of "tool" to include in the Handbook [assuming permission to use is obtained], to be housed within the Appendix.)

United States Council for International Business' Information Policy Committee and Working Group of Privacy and Transborder Data Flows "PRIVACY DIAGNOSTIC"

The following checklist ("Diagnostic") may assist team efforts in compiling and organizing essential information.

WHAT IS INCLUDED IN THE DIAGNOSTIC?

? What is personally identifiable information?
? How is it collected?
? Who should be involved in its collection?
? Who controls it?
? How and where is it stored?
? Why collect it?
? How is it used?
? Will it be transferred or shared?
? Are there currently standards regarding personally identifiable information?
? Do redress mechanisms currently exist?
? What are Privacy Principles?
? What are International Principles?

How would a company approach the question of whether it needs privacy guidelines?

Personally Identifiable Information - What is it?
? E.U. Directive Definition
? OECD Definition
? Is an actual identity (name) required or are personal characteristics sufficient?
? Are "cookies" used in the collection process?

How is personally identifiable information collected from EXTERNAL SOURCES?
? Web sites
? Purchased Databases/customer lists
? Census/directories/public information
? Proprietary databases/customer lists
? Telemarketing activities
? Promotion: redemption, other name-gathering techniques
? Sales force-generated information
? Referrals
? Third party advertisers/Web hosts
? Warranty/customer service information
? Investor relations contacts/share-related information
? Customer transactions
? Potential customer inquiries

? Supplier/partner/service provider information
? Collation of information from various sources
? Data warehousing
? Data mining
? Customer profiling

How is personally identifiable information collected from INTERNAL SOURCES?

? HR – employment-related
? Employment application/other paperwork
? Employment physical
? Pension/retirement information
? Financial information
? Expense reports, travel
? Flexible spending
? Mortgages
? Relocation assistance
? Insurance-related information
? Medical – personal/family
? Personal – beneficiaries/partners
? Child care
? Conflicts of interest/influence disclosures
? Telecommuters (also external)
? Labor/Union
? General administrative and security
? Background checks
? Computer/phone/mail logs
? System Administrator Access
? Computer monitoring
? Video/surveillance/general security
? Third-party collection (from or on behalf of)
? Government-required reporting
? Workers compensation
? Charities
? PACS/Lobbying
? Independent contractors/partners
? Shared databases
? Outsourced functions
? Joint development

Who needs to be involved in collecting the above information and in the corporate decision-making process?

? Management
? Legal – M&A
? Marketing
? Finance
? Labor – Union/Worker representatives
? Investor relations/PR
? Policy/government affairs
? Relevant third-party providers/independent contractors
? Techies
? System administrator
? Web designers
? Communications
? Network
? Security

Who controls the information once collected?

? Is the information shared between the departments?
? Is the information shared with third parties?
? If the information was collected by an "agent," what record of the information do they retain?
? If third party-generated information, is it licensed? Co-owned?
? Is the information subject to external restriction?
? Does the controller audit the accuracy of the information?
? Is the information government compliance?

How and where is the information stored?

? Centralized
? Distributed
? Geographic location(s)
? Is the storage location different from the collection location?

What is the purpose for collecting the information?

? Was a primary purpose for the collection disclosed?
? Would a primary purpose be reasonably imputed - delivery, warranty?
? Were any other purposes for the collection of information disclosed?

How is the information used?

? Is the information used for the purpose(s) it was collected?
? Is the information used for other purposes?
? Will the purpose (or character) of the information change?

Transfer/sharing of the information

? Within the company?
? Within the same state, province, country?
? Within third parties?
? Within the same state, province, country?
? Is the information available on a computer network?
? Is the information available on a LAN (local area network)?
? Is the information available on a WAN (wide area network)/VPN (virtual private network)?
? Is the information available within the same state, province, country?
? Will the sharing/transfer of information generate fees/income?
? Is the sharing/transfer of information pursuant to agreement or contract?
? Were the subjects of the information aware of the potential for this sharing/transfer?
? Is this sharing/transfer the result of compliance with or compulsion by government?
? What is the medium for transmission of the information?
? Is the confidentiality of the information protected during transmission?

Are there existing standards, guidelines, regulations which apply to the collection, control or transfer of the information?

? Regulations/legislation/required record-keeping
? Federal/agency
? State/agency
? International
? Industry/sector practices, standards, norms
? Formalized self-, coregulation
? Company guideline/practice
? Association guideline/practice (ITI, DMA)
? Third party (FASB)
? Adhered to principles (ICC, COE, OECD)
? Sectoral issues
? Information across sectors with different standards
? Collection
? Use
? Reuse

? Accuracy
? Confidentiality
? Sectoral stratification (continuum of privacy: vaccine information to highly personal info)

Do redress mechanisms currently exist?
? How are they enforced?
? Are they effective?
? How are they publicized or communicated?
? Has the company experienced privacy policy-related problems?

Privacy Principles: Mostly sourced from OECD Guidelines.
? Limitations on the collection of information
? Scope needed to accomplish end sought
? Knowledge/disclosure of what information collected
? Consent to collection where practicable - has been read to mean some form of opt-out provision is needed
? Data quality
? Relevant
? Accurate
? Specified purpose
? Why is the information being collected?
? Specify the use at the time of collection
? Compatible subsequent uses with stated purpose of collection
? Use limitation - for purpose specified
? Security - safeguard the information
? Open - accessible policy and information
? Individual participation
? Right-to-check information
? Right-to-have information corrected
? Accountability of data comptroller
? Is the concept of a data comptroller still viable with the Internet?
? Data controller may be remote from data collector, user, or other parties.

International Principles:
? Avoid developing practices that would create obstacles to international free flow of ideas
? Consider transborder implications
? Uninterrupted, secure, free flow of data
? Do not impose restrictions on countries which substantially comply

This Diagnostic was created for the benefit of the business community, and you may copy and disseminate the Diagnostic with the following legend and version/date information:

> *The **USCIB Privacy Diagnostic v.1.0 (3/98)** is a tool for companies to use in evaluating information collection practices and developing privacy guidelines. If you have specific questions on the Diagnostic, please send e-mail inquiries to: info@uscib.org with "Diagnostic" in the subject header. Current versions of the Privacy Diagnostic may be found at http://www.uscib.org.*

United States Council for International Business
1212 Avenue of the Americas
New York, NY 10036