Global Justice Information Sharing Initiative

Privacy and Information Quality Working Group

Draft Meeting Summary

Denver, Colorado

July 20, 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 July 20, 2004, at the Adam's Mark Hotel in Denver, Colorado.

The Working Group convened primarily for the purpose of gathering members' input on integrated justice privacy and data quality policy, specifically toward the release of *Product II* (exact title to be determined), a more exhaustive, practical, "hands-on" companion tool to *Privacy and Information Quality Policy Development for the Justice Decision Maker* ("Paper I" or "Policy Paper"), the high-level overview document aimed at the justice executive.

Mr. Cabell Cropper, National Criminal Justice Association and GPIQWG chair, and Jeanette Plante, Esquire, Executive Office for United States Attorneys and GPIQWG vice chair, led the meeting and set forth the following agenda and key discussion points, all in the furtherance of and alignment with the GPIQWG *Vision*[1] and *Mission*[2] *Statements*:

- Chairman's Report: Other Privacy Efforts
- *Privacy and Information Quality Policy Development for the Justice Decision Maker*: Global Acceptance, Vetting, Next Steps
- Development of a Privacy Case Study
- Stressing the Economic Benefit of Developing Privacy and Information Quality Policies
- Targeted Issues: Defining –
  - Personally Identifiable Information
  - Law Enforcement Exception

[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 system participants that promote the responsible collection, handling, management, review, and sharing of (personal) information about individuals.

- Development of *Product II (considering questions of)*
  - Audience/User
  - Purpose/Goals
  - Tasks
  - Tools

- Next Steps, Next Meetings

Chairman Cropper invited participants to introduce themselves and share their areas of interest relating to privacy and information quality. The following individuals were in attendance:

Mr. Paco Aumand
Vermont Department of Public Safety
Waterbury, Vermont

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

Mr. Bruce Buckley
Institute for Intergovernmental Research
Tallahassee, Florida

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. Ken Gill
Bureau of Justice Assistance
Washington, DC

Ms. Barbara Hurst
Rhode Island Office of the Public Defender
Providence, Rhode Island

Mr. Eric Johnson
SEARCH – The National Consortium for Justice Information and Statistics
Sacramento, California

Ms. Rhonda Jones
National Institute of Justice
Washington, DC

Ms. Erin Kenneally
San Diego Supercomputer Center
La Jolla, California

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. Monique Schmidt
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

Mr. Carl Wicklund
American Probation and Parole Association
Lexington, Kentucky

Chairman's Report: Other Privacy Efforts

A number of complementary privacy activities (and initiatives that can benefit from GPIQWG work) occurred since the last Working Group meeting. Chairman Cropper gave members the opportunity to update their justice peers on these efforts.

Erin Kenneally, Esquire, San Diego Supercomputer Center (SDSC) and new GPIQWG member, recapped the June 15-16 Privacy Technologies Conference, held under the auspices of the BorderSafe[3] project. The conference focused on technology solutions for ensuring privacy and the integrity of information in the context of sharing justice data. More specifically, the event examined issues in designing, deploying, and using integrated data systems that are flexible and extensible enough to be useful for handling large quantities of information for periods of years or decades but which provide technical, procedural, and legal mechanisms to maintain citizens' privacy.

Mr. Paco Aumand, Vermont Department of Public Safety, new GPIQWG member, and chair of the Law Enforcement National Data Exchange (N-DEx) Legal/Privacy Focus Group, briefed the group on the N-DEx System, an incident- and event-based information sharing system for local, state, tribal, and federal law enforcement agencies that securely collects and processes crime data in support of investigations, crime analysis, law enforcement administration, strategic/tactical operations, and national security responsibilities.

The vision of the N-DEx System is to:

- Create a vital access point for nationwide information sharing—effectively linking existing and developing criminal justice information systems.
- Provide a nationally based, automated information sharing system capable of optimal analysis for strategic, operational, and tactical purposes.
- Enable local, state, tribal, and federal law enforcement to provide support to the nation's Homeland Security mission.
- Establish a national information exchange system that does not necessarily need to be "knowledge-driven."
- Design and implement an information sharing system that provides users with needed investigative, analytical, and managerial tools.

At the June 22-23, 2004, N-DEx Focus Group meetings, Mr. Aumand led the discussion regarding N-DEx privacy standards. The following are highlights of the discussion:

[3] The BorderSafe project, sponsored by the U.S. Department of Homeland Security, is a collaborative research effort of SDSC, the San Diego-based Automated Regional Justice Information System, the University of Arizona, and various law enforcement agencies in Southern California and Arizona. It leverages data from participating agencies to develop models and test beds for research and analysis on cross-jurisdictional data. More information is available at http://www.sdsc.edu/bordersafe/.

- The N-DEx System has the responsibility to establish a privacy policy due to information sharing. Use of privacy design principles is the standard way to operate and design N-DEx. Memorandums of understanding (MOUs) should be a starting point to define basic privacy principles.
- The use of Information Limitation Restrictions Principles was suggested as a source of information, as well as the Law Enforcement Fair Information Sharing Principles.
- A minimum standard for privacy policy was suggested, thereby assuring that all criminal justice agencies participating in the N-DEx System have a baseline standard. The minimum standard should be required in the MOU, as well as information quality standards.
- With whom you share information is an issue under the law. The N-DEx System should articulate the expectations in regard to use of information; secondary dissemination of information may be an issue.
- The necessity of a legal analysis was discussed due to the many laws affecting privacy and information sharing.
- The release of criminal history information is controlled at the state level, so input might also be controlled by the state. Privacy has to be managed at the input level.
- N-DEx will be a conduit for information. Accuracy of the information is the responsibility of the owner.

Mr. Aumand's group also discussed treatment of victim information ("want" versus "need" for access) and prototype MOUs. He complimented the work of the GPIQWG and stressed the importance of N-DEx leveraging Global's work in all applicable areas, including privacy. To that end, he noted, "We looked at this group's material, adopted and integrated the FIPs [Fair Information Practices], and are testing the structural recommendations." At this point, the federally required Privacy Impact Assessment (PIA) has not yet been submitted; this step must be done before N-DEx moves into the piloting phase.

Ms. Mary Gay Whitmer, National Association of State Chief Information Officers (NASCIO), informed the group that NASCIO's Privacy Committee (of which Chairman Cropper is a member) is compiling a listing of state governments' emerging technologies. Once this information has been gathered, the top 10-14 technologies will be systematically analyzed for privacy implications, as well as potential benefits. The resulting data will be provided to states on the "front-end," to help them make sound technology acquisitions.

Mr. Steve Correll, National Law Enforcement Telecommunication System (NLETS) and chair of the Global Security Working Group (GSWG), updated attendees on his group's recent efforts. The GSWG is refreshing its successful *Applying Security Practices to Justice Information Sharing*, Version 2.0, CD[4] with new white papers on hot topics (i.e., Web services and wireless security issues), purchasing questions and answers (concomitantly enhancing the Integrated Justice Information Systems Institute's *Pre-RFP*

[4] Located at http://it.ojp.gov/process_links.jsp?link_id=3781.

Tool-kit[5]), and the development of a security architecture. The GSWG has two committees under its purview: 1) Security Architecture Committee, whose mission is to develop a security framework to enhance interoperability and information sharing in support of the *National Criminal Intelligence Sharing Plan*,[6] and 2) Web Services Security Task Force, whose mission is to explore security issues particularly associated with the deployment of Web services and to discuss how to mitigate those risks.

Chairman Cropper lauded the "great, positive collaboration between the two working groups [GPIQWG and GSWG]" and stressed the continued need for cross-pollination, because "security is ***NOT*** privacy."

Privacy and Information Quality Policy Development for the Justice Decision Maker

At the last GPIQWG meeting, participants polished *Privacy and Information Quality Policy Development for the Justice Decision Maker* ("Paper I") for presentation to the Global Advisory Committee (GAC or "Committee"). To that end, at the April 21-22, 2004, GAC meeting, Chairman Cropper presented Paper I for formal Committee acceptance. GAC Vice Chair Gerry Wethington, NASCIO representative, moved that the GAC accept the paper as a Global deliverable, pending a 60-day vetting procedure. Mr. Correll seconded. The motion passed unanimously. An immediate resulting action item was that Global support staff distributed the paper for an "external" review process, utilizing Committee members as conduits into various justice communities (following the procedure set by the GSWG during the vetting of *Applying Security Practices to Justice Information Sharing*; this process mirrors the "internal vetting" that GPIQWG members conducted, in which Working Group members solicited feedback from three members of their respective constituencies).

The remaining questions for Working Group discussion at the Denver meeting were as follows: 1) Is more vetting necessary, and (if so) with whom? and 2) How can the document be best distributed?

Further Vetting

Attendees discussed comments received to date, both from GPIQWG member- and GAC member-generated vetting. The majority of feedback was complimentary, with few substantive changes. Working Group members were polled to verbally relay critiques (inclusion of "requiring an audit" was suggested) and asked to initiate any final reviews. Though the "official" vetting period was drawing to a close, responses continued to arrive, and attendees were told "by no means is it too late." Paper I reviews can be sent to drinehart@iir.com. The responses will be compiled, draft document revised accordingly, and final version made available electronically and in hard copy. Paper I will be an important component of *Product II* (perhaps in the appendices), as discussed later in the meeting. **The target completion date is the fall GAC meeting, to be held September 28-29 in Arlington, Virginia.**

[5] Available at http://www.ijis.org/procure/.
[6] Located at http://it.ojp.gov/topic.jsp?topic_id=93.

Distribution Strategy

Vice Chair Plante began this roundtable with the statement: "First we need to decide who we want to receive the product and then how do we get it to them." Attendees brainstormed a list of target recipients for Paper I (*Attachment A*).

Task: As a homework assignment, GPIQWG members should review *Attachment A* and suggest mechanisms (e.g., specific listservs, Web sites, trade or professional publications) for reaching those groups. Suggestions should be directed to drinehart@iir.com.

Additionally, staff will draft a standard press release for use by Working Group members, GAC representatives, and other suggested entities in the broadscale distribution of *Privacy and Information Quality Policy Development for the Justice Decision Maker.*

Developing a Privacy Case Study

Working Group members debated the utility of developing a privacy case study. To frame the discussion, Vice Chair Plante used a case study handout detailing Du Pont's move to an electronic records management system. She explained the parallels: "Like privacy, this illustrates moving from paper to electronic. It was a ***monumental business process change*** and required high-level champions, very similar to privacy policy development." She stressed that by developing a similar study in the privacy realm, the process could be "made real, [could] flesh out areas that are particular problems . . . and provide lessons learned."

If undertaken, a privacy case study will need to be based on **systematic process**, showing **logical decisions.** Such a resource could serve two functions: 1) inclusion in *Product II* (appendix) and 2) a valuable tool for integration in speaking notes and other outreach/educational instances when justice professionals can underscore the need for privacy policy development.

Attendees were asked: Should we do a privacy case study? And, if so, "who do we do it on?" Several approaches were suggested:

- **Use the "Chicago experience."** This tact has obvious strengths:
  - Working Group member Mr. Bob Boehmer has been integrally involved in the project, and his insights are an invaluable resource.
  - The example is *on point:* it plays out in the justice arena.
  - Chicago is addressing privacy ***and*** information quality policy development.
  - The approach relies on planning and ingenuity, not a huge allocation of resources (a comforting fact to those facing policy developments).
  - Documentation already exists.
  - It is *actually being done*—as simplistic as this sounds, a function of *Product II* will be to provide assurance that this is the right thing to do, and it *can be done.*

- Mr. Carl Wicklund, American Probation and Parole Association, suggested **following a particular type of case** (suggestion: domestic violence) **through the entire "stream" of the justice system.**
  - This can illustrate how a wide variety of information can be used and misused.
  - By following the case through the justice system (from arrest forward, examining issues like the different privacy implications of the various types of information exchanges and potential breaches), the illustration becomes "inclusive . . . people can see themselves in it."
  - Perhaps use vignettes.
  - This approach could prove an effective marketing tool to small, local agencies.
  - This approach, "making the fairytale real," could be combined with an interactive component (such as worksheet) in *Product II*, so that readers review the example and then map their processes to the exemplar.
    - SEARCH's Justice Information Exchange Model (JIEM) tool is an important resource to include in this section.
  - Many attendees applauded this suggestion.

- **Reference a variety of models/case studies**
  - MATRIX—Denver has failed examples; cautionary tales are as valuable as success stories.

Considering limitations of time and resources, the following was determined: **GPIQWG members unanimously agreed to the utility of the Working Group developing a privacy case study; the first will study Chicago's experience.** Because *Product II* is envisioned as a living document, additional approaches (such as Mr. Wicklund's) can be added. **As a next step, Vice Chair Plante will lead a conference call with select members to outline the development of the case study and determine who has the necessary documents. She volunteered to complete the initial drafting.**

Stressing the Economic Benefit of Developing Privacy and Information Quality Policies

GPIQWG members discussed the impact of money (or threat of fiduciary censure) on "promoting" privacy policy development. Or, put another way: "No one does anything until they feel pain. To engender buy-in from a high-level champion, you need to show the possibility for pain." Members explored how to craft a *Product II* section that highlights both the costs of **not** having a privacy and information quality policy ("the stick") and the benefits to developing such policies ("the carrot").

The following is a listing of "the sticks":

- Political fallout
- Actual harm (e.g., domestic violence)
- Expense of how private information is currently handled in your organization (dedicated fax lines, hand carrying documents)
- Inability to exchange information
- Lawsuits
- Costs of discovery
- Inadvertent/inappropriate sharing of information
- Inaccuracies resulting in the need for duplication of efforts or manpower hours to correct data

The following is a listing of "the carrots"—points that demonstrate the value of allocating resources to develop and implement privacy and information quality policies:

- Increased information quality (timely and accurate)
- Better decisions based on better data
- Increased information exchange
- Agencies that engage in systematic data analyses and privacy policy development are much more attractive candidates for acceptance into information sharing consortiums
- **The right thing to do**

While attendees agreed that the economic factor is an important leverage to policy development—especially in providing universally understood justification (i.e., money) for the allocation of resources (e.g., staff)—quantification of "carrots" is problematic, especially considering the existence of both tangible and intangible benefits. Participants' statements, such as "a cost/benefit analysis is impossible" and "there is really no way to do an accurate return on investment," underscore this difficulty. **An approach may be to include both motivational/aspirational language (especially the universally agreed-upon "It's the right thing to do") and exemplars of "sticks" (i.e., "It's going to cost you money if you don't do it, and here are some examples . . . .").** Mr. Aumand suggested including portions of this language (in bullet form) in an expanded "what's in it for me" section.

To frame the issue for further member input, Chairman Cropper wrote the following on a tear sheet:

Benefits
- Privacy policy (access)
- Information quality

Economic
- Quantitative benefits
- Nonquantitative benefits

Task: GPIQWG members are requested to submit information relative to this section (i.e., real-life examples of "carrots" and "sticks"—both quantitatively

and qualitatively defined, suggested language to flesh out this section, and other pertinent ideas and material) to drinehart@iir.com.

Targeted Issues:
Defining "Personally Identifiable Information" and the Law Enforcement Exception to the Use Limitation Principle

Personally Identifiable Information (PII)

In the *Product II* draft produced by Michael Ramage, Esquire, Florida Department of Law Enforcement, PII is defined as follows: "'Personally identifiable information' within the justice system is generally recognized as information that can be reasonably linked to a known individual at the time of its review or dissemination, or subsequently linked to a known person by reason of analysis or comparison of the information."[7]

Working Group members debated the need to expand and/or modify this definition to include issues of **context, linking of data, amount of information** (i.e., the fact the PII can be one piece of data or multiple elements), **"thinking outside the box"** (i.e., "Just because you don't have a name doesn't mean you don't have PII"), and the **leveraging of other accepted definitions of PII**.

---

[7] Examples of personally identifiable information include, but are not limited to:

- Law enforcement: police reports, arrests, warrants, personally identifiable or traceable neighborhood/city/county/state crime data, and GIS data
- Jail: inmate information, inmate medical records, and pretrial information (scheduling and release)
- Prosecution: indictment/charging documents and victim and witness identification materials
- Courts: pleadings, motions, hearing transcripts, trial exhibits, dispositions, judge/attorney/juror information, bond information, or protection orders
- Corrections: inmate information, inmate medical information, classification information, gang affiliation, religious affiliation
- Probation/parole: term of probation/parole, sex offender status, violent offender status, employer information, residence information, or family member information
- Victims services: treatment providers, contact information, or counseling referrals
- Traditional criminal history record information: some or all compiled information available pursuant to state law
- Criminal intelligence information related to individuals
- Justice system employee: policies, employee evaluations, employment histories, medical evaluations, family information, residential information, banking or insurance information related to employees
- Other types of information related to 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
- More predictable types of information such as one's residence address, telephone number, e-mail addresses, birth date, credit card information, social security number, and information used to validate access to computer services, such as mother's maiden name or home town

Resolution and Task (voluntarily undertaken by Mr. Alan Carlson, Justice Management Institute): The definition contained in draft *Product II* should be supplemented and presented in the spirit of the following: "While there is no single definition of PII, core concepts include . . . ." Concepts to be integrated are:

- **PII can be one or more pieces of data.**
- **Context and the linking of information are essential considerations.**
  - **Regarding PII: Your agency is responsible for data under its control, including linking with other information.**
- **Consult PII as defined and enumerated by the Health Insurance Portability and Accountability Act (HIPAA) and work being done by NASCIO.**

Again, understanding *Product II* will be a living document, two additional tasks relative to PII were tabled for later discussion:

1) Defining of "Event Information"
2) Mapping PII to the Global Justice XML Data Model (Global JXDM[8]) metadata descriptors. This exercise can facilitate the assignment of specific rules governing use of PII in a justice data exchange; such rules will then automatically "flow throughout the entire model."

Law Enforcement Exception to the "*Use Limitation Principle*"

Privacy policy development in a variety of disciplines, including justice, has strong roots in the commercially developed eight Fair Information Practices Principles. One of these—the Use Limitation Principle[9]—can raise challenges when applied to justice data, particularly law enforcement information. Working Group discussion of this issue carried over from the last GPIQWG meeting.

Ultimately, it was determined the Law Enforcement Exception issue should be addressed in *Product II* as follows: (1) highlight the issue and describe the complexity, (2) provide examples of how other justice agencies have tackled the problem (e.g., Alaskan Statutes, provided as a handout at the meeting), and (3) underscore the need for each organization to determine and document *their own method* for handling law enforcement exceptions.

GPIQWG members that have additional suggestions for this section are encouraged to submit their ideas to drinehart@iir.com.

[8] For more information about the Global JXDM, please see http://www.it.ojp.gov/topic.jsp?topic_id=43.
[9] "Limit use and disclosure of information to the purposes stated in the purpose specification, and implement realistic and workable information-retention obligations."

Product II: Previously Titled
Privacy and Information Quality Policy Developer's Sourcebook

The last substantive agenda item was the continued development of *Product II* (exact title to be determined), an action book building on Paper I. As envisioned, this workbook will contain practical, hands-on materials (best practices, case studies, templates, and step-by-step outlines) to assist personnel assigned with the development of privacy and information quality policies. This action manual will be previewed at the fall GAC meeting, with completion slated for April 2005.

The development discussion was extensive[10] and focused on general determinations (such as the "goal of" and "audience for" the workbook) and rough development of the individual sections and tasks. Per resolution by Working Group members, the document will include:

Section I: Introduction, Chairman's Message

Section II: Tasks

- Defining Terminology
- Building the Project Team
- Developing and Writing the Business Case
- Holding Stakeholder Meetings
- Conducting a Workflow Analysis
- Analyzing Legal Requirements
- Determining/Developing Elements of the Policy
  - Privacy Policy
  - Information Quality Policy, Including Issues of:
    - Accuracy
    - Completeness
    - Currency
    - Reliability
    - Context/meaning
- Planning and Conducting Outreach
- Planning and Performing Policy Evaluation

Section III: Appendices and Tools

Task: Working Group leaders determined *Product II* refinement is best served by convening a *Product II* Task Team. This small group—to meet in the near future—will review participants' valuable suggestions, determine a development course of action, and report next steps and additional assignments back to the full Working Group.

[10] In the interest of containing this summary to a reasonable length, full discussion notes have been excised. Those wishing for the complete notes, in draft form, should send requests to drinehart@iir.com

Next Steps, Next Meetings

- *Product II* Task Team Meeting
  - Time Frame: ASAP—likely early to mid-August
  - Participants: Chairman Cropper, Vice Chairman Plante, Mr. Carlson, Mr. Boehmer, and Global staff

- *Product II* Table of Contents: Presentation to the GAC
  - Time Frame: Fall 2004 GAC meeting
    - September 28-29, 2004

- GPIQWG meeting
  - Time Frame: November 10, 2004
  - Place: Chicago, Illinois
  - Additional information: Respond to *Product II* issues raised by the GAC; continue development/review next draft of *Product II*; discuss vetting strategies; further explore issues of **MOUs, secondary usage**, **access rights**, and **defining "event information"** (vis-à-vis activities associated with the criminal justice system; as Mr. Aumand noted, "Privacy concerns that often arise with data arelinked with event information.")

Chairman Cropper reviewed the next steps and next meetings for his Working Group members. Assignments were delegated (as previously highlighted in this report). With no further business, GPIQWG Chairman Cropper and Vice Chairman Plante thanked attendees for their participation. The Working Group meeting was adjourned.

Appendix A

Task: Regarding distribution of Paper I: As a homework assignment, GPIQWG members should review the following and offer mechanisms (e.g., specific listservs, Web sites, and trade or professional publications) for reaching these specific groups and/or general constituencies (at both the state and federal levels). Suggestions should be directed to drinehart@iir.com.

- Chief information officers
- FBI APB
- Corrections
- Attorneys general
- Parole and probation
- State-level domestic violence coalitions
- Justice-interested state agency directors
  - Departments of motor vehicles
  - Education
  - Health care providers
  - Mental health
  - Human/social services
  - Housing
  - Departments of natural resources
- Law Enforcement
  - Prosecutors
  - State attorneys
- Privacy officers
- Privacy organizations
- State planning agencies
- Juvenile and family court judges
- Chief justices
- Child welfare agencies
- Mental health
- State legislatures
- Private sector/commercial/information
- Pretrial
- Jails
- Governors
- Defenders
- Civil liberties community
- Media
- Border patrol
- Victim advocates