United States
Department of Justice

Privacy Technology Focus Group

Final Report and Recommendations

IJIS Institute

About 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.

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.

September 19, 2006

Mr. Domingo S. Herraiz
Director
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice
810 Seventh Street, NW, Room 4427
Washington, DC 20531

Re: Privacy Technology Focus Group Report

Dear Mr. Herraiz:

It is with pleasure that the members of the Privacy Technology Steering Committee submit this report of the work accomplished by the Focus Group members during their summit in November 2005.

The Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), has supplied steady leadership in supporting the development of privacy policy for the justice community. This was the first time BJA assembled a select group to focus specifically on the technologies that can effectively support those policies.

We were well served by groundwork accomplished by our colleagues from the Global Justice Information Sharing Initiative (Global) in defining issues, recommending policies, and developing frameworks for application of those policies.

Steering Committee members were not only familiar with this foundation work; in many cases, we contributed to the efforts through our involvement in Global and IJIS Institute activities and in local and regional initiatives. It is from that perspective we tell you what a unique, rewarding, and productive experience it was to support the work of the participants in the Privacy Technology Focus Group.

Focus Group participants were selected for their impressive work in this field, solid accomplishments, and insight into the privacy policy issues and potential technology solutions. We counted on this background. An added bonus was the level of commitment the participants brought to the work. Not only did each of the participants spend weeks prior to the summit reading and considering volumes of reference works, but they also came to Phoenix prepared to move into action.

Finally, as a testament to the value, importance, and potential of the Focus Group effort, each of the participants committed their support and willingness to undertake any and all recommendations that BJA may select as the next steps to move this work forward.

We thank you for the opportunity to be part of this important collaboration, and we are equally committed to continue exploration of tangible options that leverage technology to support privacy policy.

Sincerely,

Focus Group Steering Committee

Paul Wormeli
Executive Director
IJIS Institute

Moira Rowley
Vice President
IJIS Institute Board

Paul Embley
Chair
Global XML Structure Task Force

Jeanette Plante
Director
Office of Records Management
U.S. Department of Justice

Cindy Southworth
Director of Technology
National Network to End Domestic Violence Fund

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The Privacy Technology Focus Group (Focus Group) Steering Committee thankfully acknowledges the commitment of the following people and organizations:

The Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), provided the vision and support to convene this inaugural effort to identify technology solutions supporting existing privacy policies and the insight to gather a group that included technologists, policy specialists, and active practitioners. Key to the success of this effort was funding, direction, and leadership from BJA. More information on BJA is available at http://www.ojp.usdoj.gov/BJA/.

The IJIS Institute was actively involved in the organization and support of this Focus Group and also provided private sector privacy and technology experts who contributed invaluable insight and advice to the group, en masse, and to individual teams. More information on the IJIS Institute is available at http://www.ijis.org.

The Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) has recommended much of the privacy policy practices that served as the foundation for the Focus Group's work. Additionally, a number of GAC and Global Privacy and Information Quality Working Group (GPIQWG) members served as participants in the Phoenix meeting. More information on the Global Initiative, GAC, and GPIQWG efforts is available at http://it.ojp.gov/global.

The Institute for Intergovernmental Research® (IIR) provided support throughout this process by coordinating the organizational activities of the Steering Committee, preparation for the Focus Group, and on-site support and by assembling these final recommendations. More information about IIR is available at http://www.iir.com.

Focus Group Participants – The dedication and diligence of each participant in the Privacy Technology Focus Group were phenomenal and *integral* to the success of the effort. Participants spent weeks in preparation for their participation. Once assembled in Phoenix, long days of on-site sessions often extended into the night. Participants' issues, identified in preliminary exercises, reflected thoughtful and well-considered analysis, and their collaborative efforts in the three working teams resulted in the tangible recommendations for action contained in this report. Participants were as follows (***Appendix A*** contains full contact information for participants):

* **Indicates Team Leader**
** **Indicates Steering Committee Member**
*** **Indicates Facilitator**
**** **Indicates Staff**

Brenda Abaya
Hawaii Criminal Justice Data Center
Department of the Attorney General
babaya@hcjdc.hawaii.gov

Joseph Alhadef
Oracle
Joseph.alhadeff@oracle.com

Glenn Archer
ChoicePoint Corporation
Glenn.archer@choicepoint.com

James Beshada
Department of Law and Public Safety
Division of the New Jersey State Police
L045beshadaj@gw.njsp.org

John Bliss
Entity Analytic Solutions
IBM
jblisslv@us.ibm.com

Robert Boehmer*
Institute for Public Safety Partnerships
University of Illinois at Chicago
rboehme@uic.edu

James Cabral
MTG Management Consultants
jcabral@mtgmc.com

JC Cannon
Microsoft Corporation
jccannon@mircrosoft.com

Maria Cardiellos*
Department of Law and Public Safety
State of New Jersey
Maria.cardiellos@lps.state.nj.us

Alan Carlson
Justice Management Institute
acarlson@jmijustice.org

Thomas Clarke
National Center for State Courts
tclarke@ncsc.dni.us

Steven Correll
Nlets—The International Justice and Public Safety Information Sharing Network
scorrell@nlets.org

Trelles D'Alemberte**
Insititute for Intergovernmental Research
tdalemberte@iir.com

John Doktor
Maricopa County Integrated Criminal Justice Information System
jdoktor@mail.maricopa.gov

Paul Embley**
Practitioner Resource Group
pembley@ghinternational.com

Kael Goodman
New York City Departments of Correction and Probation
Kael.goodman@doc.nyc.gov

Owen Greenspan
SEARCH—The National Consortium for Justice Information and Statistics
Owen.greenspan@SEARCH.org

Bob Greeves**
Bureau of Justice Assistance
United States Department of Justice
Robert.e.greeves@usdoj.gov

Jeff Harmon
MAXIMUS
jeffreyharmon@maximus.com

Kelly Harris*
SEARCH—The National Consortium for Justice Information and Statistics
Kelly.harris@search.org

Michael Haslip
Blaine Police Department
mhaslip@cityofblaine.com

Erin Kenneally
San Diego Supercomputer Center
University of California, San Diego
erin@sdsc.edu

Mike Lesko
Texas Department of Public Safety
Mike.lesko@txdps.state.tx.us

Mike Lettman
Wisconsin Department of Administration
Mike.Lettman@DOA.State.WI.US

Thomas MacLellan
National Governors Association
tmaclellan@nga.org

Jeanette Plante**
Office of Records Management Policy
United States Department of Justice
Jeanette.plante@usdoj.gov

Patsy Proctor
North Carolina Department of Correction
pproctor@doc.state.nc.us

Donna Rinehart****
Institute for Intergovernmental Research
drinehart@iir.com

Moira Rowley***
ACS
IJIS Institute Board
moira.rowley@acs-inc.com

Norma Jean Schaefer
Kansas Department of Health and Environment
njschaefer@kdhe.state.ks.us

Kate Silhol
Nlets—The International Justice and Public Safety Information Sharing Network
ksilhol@nlets.org

Roland Silva
Texas Department of Public Safety
Roland.silva@txdps.state.tx.us

Cindy Southworth**
National Network to End Domestic Violence Fund
cs@nnedv.org

Samantha Styles****
IJIS Institute
Samantha.styles@ijis.org

Carl Wicklund
American Probation and Parole Association
cwicklund@csg.org

Bud Yanak
BIO-key International
bud.yanak@bio-key.com

Paul Wormeli**
IJIS Institute
Paul.wormeli@ijis.org

FOREWORD

In the last four decades, a great deal has been discussed and written about the implementation of privacy protections in justice community information systems and data exchanges. A formidable body of work, much of it supported by the Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), has been developed to guide justice agencies in drafting, monitoring, and assessing privacy policies. Conspicuously absent from this work is an examination of the role of technology in supporting privacy policies and offering reasonable assurances that operational practices follow established laws and guidelines. In fact, there seems to be a common perception that technology, by its nature, compromises rather than protects personal privacy.

This is not an either/or consideration. It is true that technological advancements of the past decade have introduced fundamental changes in the ability of justice agencies to collect, use, share, and aggregate data. The capabilities introduced by these emerging technologies have significantly improved the ability of justice and public safety agencies to fulfill their mandates. This trend will not abate. However, those same technical advances have introduced real and immediate challenges to appropriately safeguarding privacy and personally identifiable information (PII).

While acknowledging that caveat, technology is not the enemy in this balancing act. In fact, it can be a primary enabler of protections in our "wired" world, if included in thoughtful privacy policy discussions and debates.

BJA recognized this, both the false dichotomy *of technology versus privacy*, and the real potential of currently available and emerging technologies to bridge the gap between existing privacy policies and the ability of justice agencies to effectively support and enforce them.

This recognition, combined with valuable and promising developments in justice-related technology, such as the DOJ's Global Justice Information Sharing Initiative (Global) Justice XML Data Model (Global JXDM), prompted BJA to convene the Privacy Technology Focus Group in Phoenix, Arizona, on November 1–3, 2005.

Invited Focus Group members are people actively involved in the development of privacy policy, the application of technology, and the role of both in the justice system. The level of commitment from all participants was clearly evidenced by their diligent research in preparation for the meeting and their unanimous commitment to further in-kind work on this topic.

The charter for this first Focus Group meeting was to provide BJA with specific recommendations for action that leverage technology in support of privacy policy. To that end, we submit this report for your consideration.

Bob Greeves
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Moira Rowley
Focus Group Facilitator
Vice President
IJIS Institute Board

EXECUTIVE SUMMARY

Background

For the first time, in November 2005, the Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), gathered a group of public and private sector specialists to focus specifically on privacy *technology* (as opposed to privacy policy). This Privacy Technology Focus Group (Focus Group) was chartered to examine the use and exchange of personally identifiable information (PII) in the context of justice information systems and in the dissemination and aggregation of justice and public safety data. The event was sponsored by BJA, in partnership with the DOJ's Global Justice Information Sharing Initiative (Global) and the IJIS Institute.

On November 1–3, 2005, after weeks of preparatory analysis, the carefully selected group of practitioners, policymakers, and technologists met in Phoenix, Arizona, to identify existing and emerging technologies to support justice-related privacy policies.

Focus Group members:

- Identified what they considered to be the most important issues in privacy policy and technology.
- Narrowed the focus to areas that could be adequately addressed in the given timeframe.
- Outlined tangible, targeted technology solutions.
- Developed specific recommendations for action.

Focus Areas and Recommendations

On-site, each of the Focus Group participants submitted five issues that he/she thought were critical to privacy policy and had the potential of being addressed by technology. The collected issues were categorized into a list of subjects. The participants, after forming three separate working teams, selected what they considered to be priority subjects from that list.

Working teams addressed the following subject matters:

- **Access and Authentication**
- **Data Aggregation and Dissemination**
- **Identity Theft**
- **Personal Safety and Protection**

Each working team produced a report and recommendations for their selected topics. Their conclusions are summarized in the following charts.

The teams' detailed recommendations for action are captured in the Focus Group full report and include adaptation of architectural frameworks, specific technologies, methodologies, and business practices.

Working Team One	
Access and Authentication	
Issue How do you foster an appropriate balance between *effective information sharing* and *privacy*? Specifically, what approaches are necessary to develop appropriate, interoperable, and adaptable business rules and technical standards to ensure that only authorized people have access to the information appropriate to their roles and privileges?	**Tab 4**
Recommendation 1	Develop standard elements/components for interoperability (suggested outline contained in report).
Recommendation 2	Commission appropriate ad hoc entity(ies) of public and private policy experts and/or technologists to define technical requirements associated with the Federated Identity (ID) Management and Service-Oriented Architecture (SOA).
Recommendation 3	Create an inventory of Federated ID Management technologies, and conduct a privacy-related architectural gap analysis to determine if additional technologies should be used.
Recommendation 4 *Related to #12*	Review and create, where needed, privacy metadata (e.g., reliability, sensitivity, use limitations, and personally identifiable information) in the Global JXDM.
Recommendation 5	Create a matrix defining roles and associated services to serve as a model to develop business rules and standards related to data content and messaging architectures.
Recommendation 6	Commission further work to properly identify supporting technologies related to Federated ID Management and SOA and their impact on privacy.
Recommendation 7	Appoint a cross-skilled team (policy/practitioners/technologists from public and private sectors) to evaluate and revise the Fair Information Principles (FIPs) as they relate to specific justice circumstances and technologies.

Working Team Two	
Data Aggregation and Dissemination	
Issue There is a sustained trend within the justice community to move away from "silo" models of information (e.g., disparate records and case management and emergency response systems) to integrated public safety operational and intelligence systems. As access to data becomes more and more ubiquitous, technologies must be implemented to ensure lawful access control and use and meaningful oversight, thereby ensuring compliance with privacy policies.	**Tab 5**
Recommendation 8	Prepare a policy paper on data anonymization and its value for privacy protection. **Note: Anonymization* is <u>not</u> synonymous with anonymous.**
Recommendation 9	Develop a strategic plan for use of anonymization in justice, public safety, and homeland security efforts to protect privacy while enhancing information sharing.
Recommendation 10	Request that the Global Justice Information Sharing Initiative support development of standards for audit functions.
Recommendation 11	Request that the National Institute of Justice conduct a research project on the maturity and applicability of immutable audit capabilities.
Recommendation 12 *Related to #4*	Assemble or use existing groups to identify privacy-related metadata and its links to business rules.
Recommendation 13	Determine mechanisms to ensure persistence of metadata throughout transfer, aggregation, and dissemination of data. Refer to the Global XML Structure Task Force (XSTF) to build into the Global JXDM.

* In this document, the term "data anonymization" refers to technology that converts clear text data into a nonhuman readable and irreversible form, including but not limited to preimage resistant hashes (e.g., one-way hashes) and encryption techniques in which the decryption key has been discarded. Data is considered anonymized even when conjoined with pointer or pedigree values that direct the user to the originating system, record, and value (e.g., supporting selective revelation) and when anonymized records can be associated, matched, and/or conjoined with other anonymized records.

Data anonymization enables the transfer of information across a boundary, such as between two departments within an agency or between two agencies, while reducing the risk of unintended disclosure, and in certain environments in a manner that enables evaluation and analytics post-anonymization.

Working Team Three	
Identify Theft	
Issue The pervasive and growing problem of identity theft manifests itself in myriad forms. Justice information is certainly as susceptible to identity theft as any other information, whether paper or electronic, internal or publicly available.	**Tab 6**
Recommendation 14	Identify best practices that ensure data quality is a priority throughout near-term and long-term business processes and technology solutions.
Recommendation 15	Establish a grant condition requiring applicants/grantees to address identity management in plans and outcomes for programs and systems development supported by national funding.
Recommendation 16	Through funding, training, and technical assistance, encourage local, county, state, and regional agencies to move towards foundational components, such as open data standards Global JXDM and National Information Exchange Model (NIEM) and baseline definition of identity data elements.
Recommendation 17	Through funding, training, and technical assistance, encourage local, county, state, and regional agencies to categorize data within existing and/or new systems.
Recommendation 18	Through funding, training, and technical assistance, encourage local, county, state, and regional agencies to develop and undertake projects related to strong authentication and identification of the user.
Recommendation 19	Develop enforceable policies and practices, such as audit logs, that appropriately respond to potential systems misuse.
Recommendation 20	Form a task force to evaluate how personally identifiable information (PII) ** is obtained or collected and should be treated.

** Personally Identifiable Information (PII) is defined in ***Appendix B—Glossary*** of the full *Privacy Technology Focus Group Report*.

<table>
<tr><th colspan="3">Working Team Three</th></tr>
<tr><td colspan="3">Personal Safety and Protection</td></tr>
<tr><td colspan="2">Issue
Information collected and disseminated by the justice system related to a person's safety or protection must also be safeguarded. For example:
❖ Location of a stalking victim
❖ Officials' home addresses, phone numbers, and other PII
❖ Identity of a rape victim
❖ Confidential information such as physical health or mental health</td><td>Tab 6</td></tr>
<tr><td>Recommendations</td><td colspan="2">The working group concluded that recommendations from the preceding three working team reports address this issue.</td></tr>
</table>

Common Issues—Important to All Topic Areas, Relevant to All Working Teams

Just as important as the working teams' separate recommendations are common elements expressed by all three teams as they analyzed realistic solutions to complex issues:

- Technology can support privacy policies to the extent that those policies are reliably and specifically expressed within technology frameworks.

- Interoperability is dependent upon consistency and open standards. *Standards* in the technological world can be (and often are) more detailed and structured than *policy* in the executive world.

- Within the justice community, there is currently a gap between technological capabilities and open standards to support the consistent explanation, dissemination, and implementation of privacy policy.

- While technologists may be of assistance in translating *policy* to *technology*, agency executives and information stewards must clearly articulate those policies and ensure they are adequately and accurately reflected in the application of technologies.

- Fair Information Principles (FIPs) are the backbone of most current privacy policy for the justice community. Each working team requested a review and refinement of the FIPs as they relate to specific justice circumstances and today's technology environment and capabilities.

- Universally understood, accepted, and supported privacy technology solutions depend on a commonly understood lexicon. A comprehensive glossary of related terms should be developed as a next step in this process. (Please see ***Appendix B*** for an abbreviated glossary of related terms.)

- Specific technology solutions may be constrained by local infrastructure; therefore, to avoid an all-or-nothing approach to solutions, it is important to look at a range of options rather than limit recommendations to only the most recent (and usually most effective) technological solutions.

- Use and refinement of the Global Justice XML Data Model (Global JXDM) to support privacy elements will play a key role in future work.

- Whenever possible, stakeholders and funding authorities should encourage and support the ability of each jurisdiction and information sharing community to acquire and employ the most effective technology solutions.

- Support comes in various forms, but in some measure, it is tied to local, state, tribal, and national initiatives and funding mechanisms. Ensuring currency of information and considerations of these groups will require close and continued coordination among policy bodies, funding authorities, technologists, practitioners, executive sponsors, and private sector partners.

- Determining appropriate access to and safeguarding against unauthorized use of data requires more, not less, information to ensure positive identification of persons and roles.

- Even the most effective privacy policy technology solutions will be subject to the inherent risks associated with human behavior. Good technology solutions work in tandem with sound business practices and vigilant monitoring.

Concluding Thoughts, Moving Forward

The ongoing commitment of the Privacy Technology Focus Group participants—from the Steering Committee members to the working team leaders to the invitees—cannot be overstated: all attendees expressed sincere interest in continuing this work and pledged to contribute future time and effort to further refine the recommendations in this report.

Participants look forward to the BJA's decisions and guidance about which of these recommendations warrant additional action and stand ready to support the work that BJA determines to be of most immediate value to the justice community.

The Bureau of Justice Assistance-Sponsored
Privacy Technology Focus Group
November 1-3, 2005 ♦ Phoenix, Arizona

FINAL REPORT AND RECOMMENDATIONS

Background

Because this was the first formal examination of privacy policy-related technology in justice information systems and exchanges, the Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), carefully identified the necessary skill sets and practitioner/industry experience to best support this work. The corresponding cast that comprised the Privacy Technology Focus Group (Focus Group) was constructed to include both professionals representing the technology and policy perspectives in the public and in the private sectors of the justice community. This combination of expertise and perspective was critical in fully understanding and evaluating the issues and in developing realistic and effective recommendations.

Focus Group participants were given clear charges regarding what to address during their sessions and what not to undertake. Attendees evaluated technology approaches and methods that can promote, ensure, and carry forward existing privacy policies and adapt to changes in those policies. It was not the work of this group to revisit, revise, or otherwise attempt to reshape underlying privacy policies.

Methodology

Many groups and persons within the justice community have, in the past decade, applied intense focus to privacy policy issues. Those efforts have produced an impressive body of work that guided the Focus Group. Prior to the Phoenix gathering, each participant reviewed, at a minimum, the following policy documents which provided the foundation for technological considerations:

Organization for Economic Cooperation and Development: *(OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

Justice Information Privacy Guideline: *Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*

DOJ's Global Justice Information Sharing Initiative: *Privacy Policy Development Guide*

DOJ's Global Justice Information Sharing Initiative: *Applying Security Practices to Justice Information Sharing*

Privacy and Civil Rights Policy Templates for Justice Information Systems

(Please see ***Appendix C*** for additional information about these resources, including access instructions.)

The above documents incorporate constructs from the Fair Information Principles (FIPs or Principles), which were first published by the U.S. Department of Health, Education and Welfare in 1973 and continue to serve as the basis for much of the current privacy policies in the United States' public and private sectors.

Focus Group participants spent their first day in Phoenix reviewing established privacy policy work. Because much of the existing policy in this area is based on the FIPs, participants reviewed the Principles in detail and discussed their relevance to the justice community.

Also during their first day on-site, each participant was asked to submit what he/she considered the top five justice-related privacy policy issues that can likely be addressed by technology. The individual issue cards were grouped into common subject matters.

Before adjournment on the first day, participants were divided into three working teams, each comprised of a combination of public and private sector participants with a range of technology, policy, and practical business experience. Working teams prioritized a single subject matter they felt well-equipped to carefully analyze and recommend corresponding specific actions. (One working team tackled two issues.)

The teams spent the next two days in separate drill-down sessions examining their chosen topics. Resulting reports and recommendations follow later in this document.

Privacy Technology Subject Matters Identified and Prioritized for Analysis

A practical consideration was narrowing the Focus Group scope to produce detailed analyses and recommendations. Issues submitted by individual participants were grouped into the following subject matters. (Please see ***Appendix D*** for a transcription of individual issue cards.) While all subject matters were considered important, a selection of four (*italicized and* ***bolded****, below)* were addressed within the timeframe of the Focus Group. (Issue cards for these four subject matters are not included in Appendix D because their content is subsumed in this report.)

Subject matter areas included:

- ***Access and Authentication***
- Automation of Flow and Processes/Data Mapping
- Compliance/Accountability

- Data Quality
- Data Ownership/Stewardship
- ***Data Aggregation and Dissemination***
- ***Identity Theft***
- Expungement/Retention
- Granular/Discrete Data
- Inherent Privacy Issues Associated With Technology
- Organizational Behavior
- Policy
- Privacy Policy/Technology Standards, Legacy Systems
- ***Personal Safety and Protection***
- Security
- Solutions
- Miscellaneous

WORKING TEAM REPORT AND RECOMMENDATIONS: TEAM ONE, "BLUE TEAM"

Subject Matter: **Access and Authentication**

Team Composition

Team Leader:	Robert Boehmer
Steering Committee Liaison:	Bob Greeves
Team Members:	Joseph Alhadeff James Beshada James Cabral Thomas Clarke Kael Goodman Owen Greenspan Erin Kenneally Mike Lesko Patsy Proctor
Staff:	Donna Rinehart

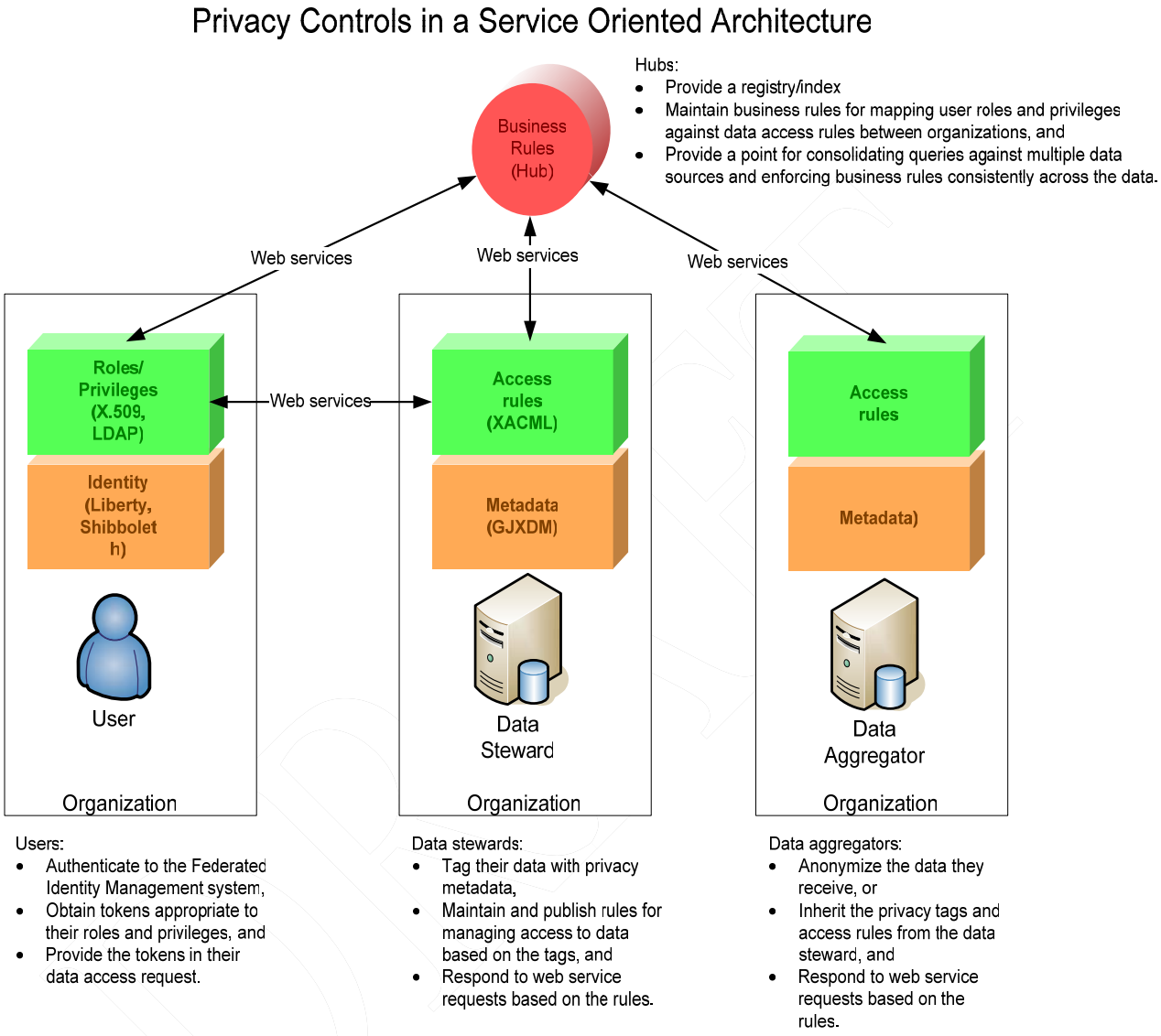
Working Team One	
Access and Authentication *See Exhibit 1: Privacy Controls in a Service-Oriented Architecture*	
Problem Statement	Organizations need to use and share justice-related information electronically to fulfill their mandates and obligations and to enhance their capacity to protect public safety. They must do this while also considering privacy interests of individuals in contact with the justice system. The introduction of new technologies has heightened the immediacy, scope, and complexity of privacy issues related to information access and sharing.
Issue	How do you foster an appropriate balance between effective information sharing and privacy? Specifically, what approaches are necessary to develop appropriate, interoperable, and adaptable business rules and technical standards to ensure that only authorized people have access to the information appropriate to their roles and privileges? What are the requirements of an interoperable and open standards-based framework to address the problem statement? Consideration should be given to: ❖ Identities (persons, organizations) o Creating, proofing, background checking, and credentialing • Leveraging existing efforts (e.g., FIPS 201) o Validating the credential o Revocation ❖ Establishing roles for and associating privileges with identities o Role definitions across the framework o Privilege management • Privilege delegation • Special access—Temporary access beyond provision of role(s) and privilege(s)

Working Team One	
Access and Authentication *See Exhibit 1: Privacy Controls in a Service-Oriented Architecture*	
Issue (continued)	❖ Access rules associated with the data o Control mechanisms, such as: • Role-based filtering mechanisms • Subject-based filtering mechanisms • Selective revelation o Levels of sensitivity of data o Metadata, such as: • Source of information • Quality of information • Purpose for which information was collected • Sensitivity of information ❖ Business rules for use and access o Requirements for interface and interoperability o Contingency rules (exceptions) o Need for documentation **Recommendation**: Considering the above outline, develop standard elements/components for interoperability.
Assumptions	We need technologists, users/practitioners, and policy people working together when requirements and system design are first considered and undertaken. Note that policy people may cross boundaries and must be defined for each organization.
Conclusions(s)	We need to pursue technologies that allow us to work in interoperable frameworks.

Working Team One	
Access and Authentication *See Exhibit 1: Privacy Controls in a Service-Oriented Architecture*	
Recommendation	**Identity Management and Architecture** **Recommendation**: Commission appropriate ad hoc entity(ies) of public and private policy experts and/or technologists to define technical requirements associated with the following two topics. 1. **Federated Identity Management** **Recommendation**: Create an inventory of Federated Identity (ID) Management technologies and conduct a privacy-related architectural gap analysis to determine if additional technologies should be used. Examine the following current technologies and strategic plans related to the future application, identify/assess potential privacy functionality by conducting a privacy impact assessment of those technologies. Technologies include, but are not limited to: ▪ WS-Security Profile ▪ ebXML Profile ▪ Liberty Alliance Profile ▪ Shibboleth Profile 2. **Service-Oriented Architecture (SOA)** SOA is the method of providing Web-based services. We believe the following recommendations respond to high-level requirements previously outlined: i.e., establishing roles for and associating privileges with identities; access rules associated with the data and business rules for use and access. **Recommendation**: Create appropriate privacy metadata (e.g., reliability, sensitivity, use limitations, and personally identifiable information) in the Global Justice XML Data Model (Global JXDM). **Recommendation**: Create a matrix defining roles and associated services to serve as a model to develop business rules and standards related to data content and messaging architectures.

Working Team One	
Access and Authentication *See Exhibit 1: Privacy Controls in a Service-Oriented Architecture*	
Recommendation	**Supporting Technologies** The above justice reference architecture relies on a number of supporting technologies and policies which will often be deployed at the system level and need to be considered for interoperation. **Recommendation**: We recommend that the BJA commission further work to properly identify these technologies and their impact on privacy.
Recommendation	**Governance and Policy** In light of technological advancements and the changing context of justice-related information sharing, the application of the Fair Information Principles (FIPs) must be reexamined, revised, and supplemented (as necessary) to address the current practices and potential use of information within the new justice environment. **Recommendation**: We recommend that BJA appoint a cross-skilled team of policy practitioners and technologists from the public and private sectors to reexamine, revise, and supplement (as necessary) the FIPs as they relate to new justice circumstances and technologies. Consideration must be given to technical as well as policy-oriented audiences.

Exhibit 1: Blue Team report on Access and Authentication—Illustration of the role and operation of Service-Oriented Architecture to support privacy policies.



WORKING TEAM REPORT AND RECOMMENDATIONS: TEAM TWO, "GREEN TEAM"

Subject Matter: **Data Aggregation and Dissemination**

Team Composition

Team Leader: Kelly Harris

Steering Committee Liaison: Paul Wormeli

Team Members: Brenda Abaya

Glenn Archer
John Bliss
Alan Carlson
Steven Correll
Jeff Harmon
Jeanette Plante
Norma Jean Schaeffer
Roland Silva

Staff: Samantha Styles

Working Team Two	
Data Aggregation and Dissemination	
Definition/Notes	Definition: **Data Aggregation**—Two or more data sets combined to create one data set Note: Data anonymization* is **not** anonymous data. This is a very important distinction, one that is widely misunderstood. That misunderstanding has legal and ethical implications and can hinder, rather than help efforts to support privacy policy.
Problem Statement	Data aggregation introduces difficulty in controlling use and access of data consistent with privacy and other business rules as the data moves through multiple systems and/or is aggregated with other data. *(This subject matter originally included the issue of data mining. The Working Team determined that the time frame did not permit adequate evaluation of data mining issues and technology solutions.)*
Issues	There is a sustained trend within the justice community to move away from "silo" models of information (e.g., disparate records and case management and emergency response systems) to integrated public safety operational and intelligence systems. In this networked, collaborative environment, the capability of local, state, regional, tribal, and federal governments to gather data from multiple sources through aggregation technologies serves important justice and public safety functions. As access to data becomes more and more ubiquitous, technologies must be implemented to ensure lawful access control, use, and meaningful oversight of the accessed data, thereby ensuring compliance with privacy policies.

* In this document, the term "data anonymization" refers to technology that converts clear text data into a nonhuman readable and irreversible form, including but not limited to preimage resistant hashes (e.g., one-way hashes) and encryption techniques in which the decryption key has been discarded. Data is considered anonymized even when conjoined with pointer or pedigree values that direct the user to the originating system, record, and value (e.g., supporting selective revelation) and when anonymized records can be associated, matched, and/or conjoined with other anonymized records.

Data anonymization enables the transfer of information across a boundary, such as between two departments within an agency or between two agencies, while reducing the risk of unintended disclosure, and in certain environments in a manner that enables evaluation and analytics post-anonymization.

Working Team Two	
Data Aggregation and Dissemination	
Assumptions	**The problem statement assumes that:** There is an ongoing concern that aggregated data can be inaccurate, and/or be used inappropriately, particularly data associated with specific individuals. **Problem and solutions assume that:** ❖ We are addressing information sharing and data exchange for justice, public safety, and homeland security. ❖ Data will continue to be federated or centralized and open-source or proprietary. **The proposed solutions assume that:** ❖ There will be adequate policy and law enforcement supporting lawful access and use of data/information. ❖ Source systems abide by applicable privacy statutes, rules, regulations, and policies. ❖ Business rules are documented and agreed upon by involved parties. ❖ When implemented, all participants have the responsibility to communicate the use restrictions and other constraints on the data.
Conclusion(s)	Justice, public safety, and homeland security agencies need the ability to carry restrictions, permissions, access (controls and integrity), and business rules about data as it is passed through multiple systems.

Working Team Two	
Data Aggregation and Dissemination	
Recommendation	**Anonymize (privacy enhanced) Data Sharing** Anonymizing data permits multiple parties to correlate data from multiple sources without revealing personally identifiable information until or unless appropriate. Anonymized data: ❖ Prevents exposure of data that does not match. ❖ Limits exposure of data that does match, based upon appropriate policy, rules, and regulations. **Recommendations**: We recommend that BJA take/support the following actions: ❖ Prepare a white paper on anonymization and its value for privacy protection. ❖ Develop a strategic plan for use of anonymization in justice, public safety, and homeland security agencies to protect privacy while enhancing information sharing. o The planning process should involve primary stakeholders. o The plan should have a clear mission and vision for the use of data. o The plan should include a candidate list for high-value demonstration projects.

Working Team Two	
Data Aggregation and Dissemination	
Recommendation	**Enhance Audit Capability** Enhanced audit capabilities can solve data integrity and responsibility issues. Information sharing and aggregation processes and practices should include an immutable audit trail that provides for continuous monitoring for system and/or policy violations. This type of audit capability: ❖ Detects and deters inappropriate use of system and data. ❖ Prevents changes to the audit data (alterations, deletions, and modifications to audit trail). ❖ Increases public trust, particularly in systems that lack transparency. ❖ Improves training by providing feedback on improper system/data use, even when it is unintended misuse. ❖ Provides input for policy development on appropriate use. ❖ Provides a mechanism to enforce policy and take remedial action. ❖ Can be used as an evidentiary tool. **Recommendations**: We recommend that BJA take/support the following actions: ❖ Global Information Sharing Initiative establishes a working group to develop standards for audit functions. ❖ National Institute of Justice (NIJ) conducts a research project on the maturity and applicability of immutable audit capabilities.

Working Team Two	
Data Aggregation and Dissemination	
Recommendation	**Communicate Privacy Business Rules** Privacy business rules can be communicated by linking the privacy-related metadata with each data element in all exchanges. The approach: ❖ Enables ongoing implementation of privacy rules. ❖ Allows traceability for each data element. ❖ Enables individual participation with the right to challenge and correct. **Recommendations:** We recommend that BJA take/support the following actions: ❖ Assemble or use existing groups to identify privacy-related metadata and its links to business rules. ❖ Determine mechanisms to ensure persistence of metadata throughout transfer, aggregation, and dissemination of data. Refer to the Global XML Structure Task Force (Global XSTF) to build into Global JXDM.

WORKING TEAM REPORT AND RECOMMENDATIONS: TEAM THREE, "RED TEAM"

Subject Matters: **Identity Theft**
Personal Safety and Protection

Team Composition

Team Leader: Maria Cardiellos

Steering Committee Liaison: Paul Embley

Team Members:
J. C. Cannon
John Doktor
Michael Haslip
Mike Lettman
Thomas MacLellan
Kate Silhol
Cindy Southworth
Carl Wickund
Bud Yanak

Staff: Trelles D'Alemberte

Working Team Three	
Identify Theft	
Problem Statement	Nationwide, the pervasive and growing problem of identity theft manifests itself in myriad forms. The justice system is not immune to being preyed upon by people wishing to abuse personally identifiable information (PII)* for purposes of identity theft. This team has prepared recommendations that take advantage of current systems and emerging technologies to address such challenges.
Issues	Entities need to protect stored and shared information. All data collected and disseminated could be used to intentionally, inadvertently, and/or carelessly cause identity theft. We need to be concerned with: ❖ Existing victims of ID theft. ❖ Prevention of future victims. The stakeholders at issue are: ❖ Users of data: ○ Practitioners and technologists within the justice community ○ Users external to the justice community (lawyers/bail bondsman) ❖ Subjects of data: ○ Defendants/suspects, etc. ○ Victim/witness, etc. ❖ Builders of data systems (external and internal).
Assumptions	The move from paper to electronic records and from stand-alone applications to networked information systems introduces new considerations about how justice-related information may be used as a tool for identity theft.
Conclusion(s)	There are specific practices, policies, and technologies that can support the protection of PII and detection/prevention and of inappropriate information use leading to identity theft.
Recommendation	**Recommendation**: We recommend forming a task force to evaluate how PII is and should be treated and how agencies exchange PII.

* PII is defined in the ***Appendix B—Glossary*** of this report.

Working Team Three	
Identify Theft	
Recommendation	**<u>Recommendation</u>:** Develop best practices that ensure data quality is a priority throughout near-term and long-term business processes and technology solutions, such as: ❖ Better validation, such as fingerprints (biometrics), should be associated to tie as many records together as possible. o Validate and verify the data against other data sources: • MVC • Vital statistics, etc. *Note: BJA should coordinate with the International Association of Chiefs of Police (IACP), Law Enforcement Information Technology Standards Council (LEITSC), and other groups working on complementary efforts regarding computer aided dispatch (CAD)/records management systems (RMS) data definitions.*

Working Team Three	
Identify Theft	
Recommendation	**<u>Recommendation</u>:** Establish a grant condition requiring applicants/grantees to address identity management in plans and outcomes for programs and systems development supported by national funding. *Note: Similar grant conditions can be established by funding authorities other than BJA.* Related notes and issues include: ❖ For the purposes of this recommendation, identity management focuses on the practitioner role and the assigned usage of available data today. ❖ Determinations of data accessibility (user role assignment) should first consider and review privacy information and then continue with the balance of data to determine appropriate level of sharing within and across agencies (i.e., privacy policy takes priority in rules sequencing). ❖ Federated Identity Management efforts should include the following considerations and assumptions: o Role definitions. o Stratification of the roles across the nation. o Roles must correlate with each other across states. o Data owner has the core responsibility of identifying the roles (issuing vs. receiving state/jurisdiction). o Linkage to local statute(s) and data.

Working Team Three	
Identify Theft	
Recommendation	**Recommendation:** Through funding, training, and technical assistance, encourage local, county, state, regional, and tribal regional agencies to move towards foundational components, such as: ❖ Open data standards (Global JXDM and NIEM). o Add privacy metadata properties to the Global JXDM to facilitate the ability to identify personally identifiable and private data at a more granular level. ❖ Baseline definition of ID data elements: o Service-Oriented Architecture. o Enterprise service bus. o Web services.
Recommendation	**Recommendation:** Through funding, training, and technical assistance, encourage local, county, state, regional, and tribal agencies to categorize data within existing and/or new systems with respect to: ❖ Customized response based on role. ❖ Record and field classification. ❖ Shared data in the context of objects (we should be breaking it down further). ❖ Filtered data based on classification (i.e., standardized rap sheet). *Note: By classification of data, the team refers to confidentiality, availability, and integrity of pertinent data.* ❖ Essential data versus provision of nonessential data. *Note: Existing systems should be enhanced with privacy protections.*

Working Team Three	
Identify Theft	
Recommendation	**Recommendation:** Through funding, training, and technical assistance, encourage local, county, state, regional, and tribal agencies to develop and undertake projects related to strong authentication and identification of the user (*justice practitioner vs. arrested individual vs. victim/witness*). Issues related to this recommendation include: ❖ Supporting biometric standards (i.e., National Institute for Standards and Technology (NIST)—Federal Information Processing Standard 201). ❖ Using multiple data sources to verify identity. ❖ Incorporating audit capabilities outlined in data aggregation recommendations. ❖ Ensuring that audit logs are detailed enough to determine who requested/accessed/used/misappropriated the information. ❖ Using consolidation and query tools for audit logs. ❖ Assigning alerts. ❖ Incorporating governance recommendations from Authorization/Access Control report.
Adjunct Considerations	❖ Ensure that policy is reflective of requirement need and technical capacity. ❖ Develop enforceable policies and practices that appropriately respond to potential systems misuse of the supporting technologies, such as audit logs.

Working Team Three	
Personal Safety and Protection	
Problem Statement	Similar to the challenge of identity theft, personal information collected and disseminated by the justice system related to safety or protection must also be protected. Some examples of this type of information include: ❖ Location of a stalking victim. ❖ Officials' home addresses, phone numbers, and other personally identifiable information. ❖ Identity of a rape victim. ❖ Confidential information such as physical health or mental health.
Issues	Issues that should be addressed by the appropriate resources include, but are not limited to: ❖ The legal right to have sex offender registries must be balanced with the impact to other parties, including family members of the offender. ❖ Current and prior victims use the justice system for non-law enforcement issues. It is hard to protect victim information unless they self-identify. ❖ Information can be misused by practitioners and/or accessed by those outside the system for nefarious purposes. ❖ Specific types of data, require special consideration: o Dispatch data. o Witness data. o Juvenile offenders. *Note: Many of the above issues are jurisdictional in nature.*
Assumptions	The move from paper to electronic records and from stand-alone applications to networked information systems introduces new considerations about how use and access to justice-related information may compromise the safety of persons who are the subjects of source and aggregated records.

Working Team Three	
Personal Safety and Protection	
Conclusion(s)	Justice-related data includes a plethora of PII which is widely available to internal and external access. Depending upon circumstances and context of request for and access to this information, it is possible that the dissemination will put vulnerable people at risk, compromising their personal safety. Cognizance of this risk is a first step toward addressing it. Solutions in this area require combined focus on policy, practice, technology, human behavior, and responsibility to safeguard sensitive information.
Recommendation	**Recommendation:** The working teams' recommendations set forth in the preceding three subject areas address this topic.

Concluding Thoughts, Moving Forward

The ongoing commitment of the Privacy Technology Focus Group participants, from the Steering Committee members, to the working team leaders, to the invitees, cannot be overstated: all attendees expressed sincere interest in continuing this work and pledged to contribute future time and effort to further refine the recommendations in this report.

Participants look forward to the BJA's decisions and guidance about which of these recommendations warrant additional action and stand ready to support the work that BJA determines to be of most immediate value to the justice community.

APPENDIX A: PRIVACY TECHNOLOGY FOCUS GROUP

ATTENDEE ROSTER

Brenda Abaya
Hawaii Criminal Justice Data Center
Department of the Attorney General
465 South King Street
Honolulu, HI 96813
babaya@hcjdc.hawaii.gov

Joseph Alhadef
Vice President Global Public Policy
Chief Policy Officer
Oracle
Suite 200
1015 15th Street, NW
Washington, DC 20005
Joseph.alhadeff@oracle.com
(202) 721-4816

Glenn Archer
ChoicePoint Corporation
Suite 450
1410 Spring Hill Road
McLean, VA 22102
Glenn.archer@choicepoint.com

James Beshada
Department of Law and Public Safety
Division of the State Police
P.O. Box 7068
Building #15
Trenton, NJ 08625-7068
L045beshadaj@gw.njsp.org
(609) 984-2398

John Bliss
Privacy Strategist
Entity Analytic Solutions, IBM
Suite A
6600 Bermuda Road
Las Vegas, NV 89119
jblisslv@us.ibm.com
(702) 853-4658

Robert Boehmer
Director
Institute for Public Safety Partnerships
University of Illinois at Chicago
Suite 230
921 West Van Buren Street
Chicago, IL 60607
rboehme@uic.edu
(312) 355-1753

James Cabral
MTG Management Consultants
Suite 2700
1111 Third Avenue
Seattle, WA 98101-3201
jcabral@mtgmc.com
(206) 442-5010

J. C. Cannon
Microsoft Corporation
One Microsoft Way
Redmond, WA 98009
jccannon@mircrosoft.com

Maria Cardiellos
Chief Information Officer
Department of Law and Public Safety
P.O. Box 081
Trenton, NJ 08628
Maria.cardiellos@lps.state.nj.us
(609) 984-2398

Alan Carlson
President
Justice Management Institute
821 Coventry Road
Kensington, CA 94707
acarlson@jmijustice.org
(415) 816-3341

Thomas Clarke
Chief Information Officer
National Center for State Courts
300 Newport Avenue
Williamsburg, VA 23185
tclarke@ncsc.dni.us
(757) 259-1870

Steve Correll
Executive Director
Nlets—The International Justice and Public Safety Information Sharing Network
Suite 160
2930 East Camelback Road
Phoenix, AZ 85016
scorrell@nlets.org
(602) 627-2710

Trelles D'Alemberte
Senior Research Associate
Institute for Intergovernmental Research
Suite 200
2050 Centre Pointe Boulevard
Tallahassee, FL 32301
tdalemberte@iir.com
(850) 385-0600, Ext. 295

John Doktor
Technical Director
Maricopa County Integrated Criminal Justice Information Systems
Suite 400
411 North Central Avenue
Phoenix, AZ 85004
jdoktor@mail.maricopa.gov
(602) 506-7906

Paul Embley
Practitioner Resource Group
G&H International Services
Post Office Box 1309
Frankfort, KY 40602
pembley@ghinternational.com
(202) 250-3498

Kael Goodman
Chief information Officer
Deputy Commissioner
New York City Departments of Correction and Probation
60 Hudson Street
New York, NY 10013
Kael.goodman@doc.nyc.gov

Owen Greenspan
Director
Law and Policy Program
SEARCH—The National Consortium for Justice Information and Statistics
6 Gramercy Court
Clifton Park, NY 12065
Owen.Greenspan@SEARCH.org
(518) 373-2260

Bob Greeves
Policy Advisor
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice
810 Seventh Street, NW, 4th Floor
Washington, DC 20531
(202) 305.9317
Robert.e.greeves@usdoj.gov

Jeff Harmon
Senior Consultant
MAXIMUS
P.O. Box 1175
Auburn, ME 04211-1175
jeffreyharmon@maximus.com
(207) 514-7505

Kelly Harris
Deputy Executive Director
SEARCH—The National Consortium for Justice Information and Statistics
Suite 145
7311 Greenhaven Drive
Sacramento, CA 95831
Kelly.harris@search.org
(916) 392-2550

Michael Haslip
Blaine Police Department
322 H Street
Blaine, WA 98230
mhaslip@cityofblaine.com
(360) 332-6769

Erin Kenneally
Cyber Forensics Analyst
San Diego Supercomputer Center
University of California
9500 Gilman Drive
La Jolla, CA 92093-0505
erin@sdsc.edu
(858) 822-0991

Mike Lesko
Deputy Administrator
Crime Records Service
Texas Department of Public Safety
5805 North Lamar Street
P.O. Box 4143
Austin, TX 78765-4143
Mike.lesko@txdps.state.tx.us
(512) 424-2524

Mike Lettman
Chief Information Security Officer
Chief Security Architect
Office of the Administrator
Wisconsin Department of Administration
101 East Wilson Street, 8th Floor
Madison, WI 53702
Mike.Lettman@DOA.State.WI.US
(608) 264-9786

Thomas MacLellan
Senior Policy Analyst
National Governors Association
Hall of States
444 North Capitol Street
Washington, DC 20001
tmaclellan@nga.org
(202) 624-5427

Jeanette Plante
Director
Office of Records Management Policy
U.S. Department of Justice
National Place Building
Suite 1070
1331 Pennsylvania Avenue, NW
Washington, DC 20530
Jeanette.plante@usdoj.gov
(202) 514-3528

Patsy Proctor
North Carolina Department of Correction
MSC-4217
Raleigh, NC 27699-4217
pproctor@doc.state.nc.us
(919) 716-3533

Donna Rinehart
Senior Research Associate
Institute for Intergovernmental Research
Suite 200
2050 Centre Pointe Boulevard
Tallahassee, FL 32301
drinehart@iir.com
(850) 385-0600, Ext. 285

Moira Rowley
Vice President, Justice Services
ACS
1733 Harrodsburg Road
Lexington, KY 75039
moira.rowley@acs-inc.com
(816) 361-0303

Norma Jean Schaefer
Information Security Officer
Kansas Department of Health and Environment
1000 SW Jackson Street
Topeka, KS 66612
njschaefer@kdhe.state.ks.us

Kate Silhol
Senior Software Engineer
Nlets—The International Justice and Public Safety Information Sharing Network
Suite 160
2930 East Camelback Road
Phoenix, AZ 85016
ksilhol@nlets.org
(602) 627-2716

Roland Silva
Justice II Coordinator
Texas Department of Public Safety
Crime Records Service
MSC: 0230
P.O. Box 4143
Austin, TX 78765
Roland.silva@txdps.state.tx.us
(512) 424-2991

Cindy Southworth
Director of Technology
National Network to End Domestic Violence Fund
Suite 303
660 Pennsylvania Ave, SE
Washington, DC 20003
cs@nnedv.org
(202) 543-5566

Samantha Styles
IJIS Institute
44983 Knoll Square
Ashburn, VA 20147
Samantha.styles@ijis.org
(703) 726-3697

Carl Wicklund
Executive Director
American Probation and Parole Association
P.O. Box 11910
Lexington, KY 40578-1910
cwicklund@csg.org
(859) 244-8216

Paul Wormeli
Executive Director
IJIS Institute
44983 Knoll Square
Ashburn, VA 20147
Paul.wormeli@ijis.org
(703) 726-3693

Bud Yanak
Vice President Marketing
BIO-key International
Allaire Corporate Center
3349 Highway 138
Building D, Suite A
Wall, NJ 07719
bud.yanak@bio-key.com
(732) 359-1113

APPENDIX B: PRIVACY TECHNOLOGY FOCUS GROUP REPORT

GLOSSARY OF TERMS AND DEFINITIONS

The following terms and definitions are provided as a reference and were originally appended in the U.S. Department of Justice's Global Justice Information Sharing Initiative *Privacy Policy Development Guide,* available at http://it.ojp.gov/global.

Not all of the terms listed were specifically discussed within this Focus Group report. However, they are terms relative to the subject of privacy and may contribute to an understanding of privacy-related issues.

A

Access
In respect to privacy, an individual's ability to view, modify, and contest the accuracy and completeness of personally identifiable information collected about him or her. Access is an element of the Organization for Economic Cooperation and Development's (OECD) Fair Information Principles (FIPs). See *Fair Information Principles (FIPs).*

Access Control
The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Accountability Principle
One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Cooperation and Development (OECD). According to this principle, a data controller should be accountable for complying with measures that give effect to the other 7 FIPs.

Administrative Vulnerability
Failure to observe administrative best practices, such as using a weak password or logging on to an account that has more user rights than the user requires to perform a specific task.

Anonymity
A condition in which an individual's true identity is unknown.

Anonymization
See *Data Anonymization*

Appropriate Security

An organization is required to take appropriate data security measures to protect personally identifiable information and prospect information. These measures must include physical security measures, such as doors and locks, as well as electronic security and managerial controls that limit the potential for unauthorized access or misuse by employees and contractors. The security measures necessary to protect information sufficiently will vary based on the risks presented to the individual by an organization's collection and use of the data. See *Prospect Information*.

Assuring the Accuracy of Information

In addition to providing individuals with the ability to correct factual inaccuracies in their personally identifiable or prospect information, an organization must also take reasonable steps to assure that the personally identifiable and prospect information that it collects is accurate, complete, and timely for the purposes for which it is used. See *Personally Identifiable Information* and *Prospect Information*.

Attack

A deliberate attempt to compromise the security of a computer system or deprive others of the use of the system.

Audit Trail

Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication

Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See *Biometrics* and *Credentials*.

Authentication of Identity

The process whereby an organization establishes that a party it is dealing with is:

- A previously known real-world entity in which case, it can associate transactions with an existing record in the relevant information system.

- A previously unknown real-world entity in which case, it may be appropriate to create a new record in the relevant information system and, perhaps, also to create an organizational identifier for that party.

Authorization
The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See *Authentication*.

B

Biometrics
Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of physiological biometrics include face, eye (retina or iris), finger (fingertip, thumb, finger length, or pattern), palm (print or topography), and hand geometry. Behavioral biometrics includes voiceprints and handwritten signatures.

C

Certificate
An encrypted file containing user or server identification information that is used to verify identity and to help establish a security-enhanced link.

Charter (Project Team)
A collection of the project team's written vision, mission, and values statements, as well as the stated goals and objectives. The charter serves as a reference and resource throughout the course of the project team's effort. The most critical feature of the charter is that it memorializes the planning efforts and agreements of the team members to achieve specific goals and, thus, serves as an historical record of team plans and efforts.

Collection Limitation Principle
One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Cooperation and Development (OECD). According to this principle, there should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Computer Security
The protection of information assets through the use of technology, processes, and training.

Confidentiality
Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See *Privacy*.

Cookie
A small data file that is stored on a user's local computer for record-keeping purposes that contains information about the user that is pertinent to a Web site, such as a user preference.

Credentials
Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Cryptography
The study or analysis of codes and encoding methods used to secure information. Cryptographic techniques can be used to enable and ensure confidentiality, data integrity, authentication (entity and data origin), and nonrepudiation. See *Nonrepudiation*.

D

Data
Inert symbols, signs, or measures.

Data Anonymization
In this Focus Group report, the term data anonymization refers to technology that converts clear text data into a nonhuman readable and irreversible form, including but not limited to preimage resistant hashes (e.g., one-way hashes) and encryption techniques in which the decryption key has been discarded. Data is considered anonymized even when conjoined with pointer or pedigree values that direct the user to the originating system, record, and value (e.g., supporting selective revelation) and when anonymized records can be associated, matched, and/or conjoined with other anonymized records.

Data anonymization enables the transfer of information across a boundary, such as between two departments within an agency or between two agencies, while reducing the risk of unintended disclosure, and in certain environments in a manner that enables evaluation and analytics post-anonymization.

Data Controller
A party who, according to domestic law, is competent to decide about the contents and use of personal data, regardless of whether or not such data is collected, stored, processed, or disseminated by that party or by an agent on its behalf.

Data Protection
Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Data Quality Principle
One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Cooperation and Development (OECD). According to this principle, personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and up to date.

Data Transfer
As a key principle of privacy, it is the movement of personally identifiable information between entities, such as a customer list being shared between two different companies.

Degaussing
A process of destroying computerized data by leaving the domains in random patterns with no preference to orientation, which then renders previous data unrecoverable.

Digital Certificate
A digitally signed statement that binds the identifying information of a user, computer, or service to a public/private key pair. A digital certificate is commonly used in the process of authentication and for securing information on networks. See *Authentication*.

Digital Signature
Data that binds a sender's identity to the information being sent. A digital signature may be bundled with any message, file, or other digitally encoded information or transmitted separately. Digital signatures are used in public key environments and provide nonrepudiation and integrity services. See *Nonrepudiation*.

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

Download
To transfer a copy of a file from a remote computer to a requesting computer by means of a modem or network.

E

Electronically Maintained
Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted
Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voice mail. See *Extranet*.

Enforcement
A privacy principle that provides mechanisms for assuring compliance with the Organization for Economic Cooperation and Development's (OECD) Fair Information Principles (FIPs), recourse for individuals affected by noncompliance, and consequences for noncompliant organizations. Methods for enforcement include a review by independent third parties.

Extranet
An extension of an organization's intranet used to facilitate communication with the organization's trusted partners. An extranet allows such trusted partners to gain limited access to the organization's internal data.

F

Fair Information Principles (FIPs)
The Fair Information Principles (FIPs) are contained within the Organization for Economic Cooperation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Filter
A pattern or mask through which data is passed to separate specified items. For instance, a filter used in e-mail or in retrieving newsgroup messages can allow users to automatically discard messages from designated users.

Firewall
A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

G

Goals (Project)
Project goals are the desired long-term end results that, if accomplished, will mean the team has achieved their mission. Goals provide a framework for more detailed levels of planning. Goals are more specific than mission statements but remain general enough to stimulate creativity and innovation.

H

Health Insurance Portability and Accountability Act (HIPAA)
A U.S. law that gives patients greater access to their own medical records and more control over how their personally identifiable information is used. The law also addresses the obligations of health-care providers and health plans to protect health information. In general, covered entities such as health plans, health-care clearinghouses, and health-care providers that conduct certain financial and administrative transactions electronically had until April 14, 2003, to comply with this act.

I

Identification
A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or may be a compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

Individually Identifiable Health Information (IIHI)
Information, including demographic information, which relates to the past, present, or future physical or mental health or condition of a member and can be used to identify the member.

Individual Participation Principle

One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Cooperation and Development (OECD). As stated in the FIPs, according to this principle, an individual should have the right:

a) To obtain from the data controller confirmation of whether or not the data controller has data relating to him;
b) To have communicated to him, data relating to him:
    - Within a reasonable time,
    - At a charge, if any, that is not excessive,
    - In a reasonable manner, and
    - In a form that is readily intelligible to him.
c) To be given reasons if a request made under subparagraphs a) and b) is denied, and to be able to challenge such denial; and
d) To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Individual Responsibility

Since a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Information

The use of data to extract meaning.

Information Disclosure

The exposure of information to individuals who normally would not have access to it.

Information Privacy

Information privacy is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.

Information Quality

The accuracy and validity of the actual values of the data, data structure, and database/data repository design. The elements of information quality are accuracy, completeness, currency, reliability, and context/meaning.

Invasion of Privacy

Invasion of privacy can be defined as intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See *Right to Privacy*.

K

Key
In encryption and digital signatures, a key is a value used in combination with an algorithm to encrypt or decrypt data.

L

Least Privilege Administration
A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform.

Logs
Logs are a necessary part of an adequate security system as they are needed to assure that data is properly tracked and only authorized individuals are getting access to the data.

M

Maintenance of Information
The maintenance of information applies to all forms of information storage. This would include electronic systems, like databases, and nonelectronic storage systems, like filing cabinets. To meet access requirements, an organization is not required to create new systems to maintain information or maintain information beyond a time when it no longer serves an organization's purpose.

Mission Statement
A succinct, comprehensive statement of purpose of an agency, program, subprogram, or project that is consistent with a vision statement. See *Vision Statement*.

N

Nonrepudiation
A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

O

Objectives (Project)
Objectives are specific and measurable targets for accomplishing goals, which are usually short term with a target time frame. In contrast to goals, objectives are specific, quantifiable, and time-bound statements of desired accomplishments or results. As such, objectives represent intermediate achievements necessary to achieve goals. See *Goals*.

Online Collection
A Web site or online service is deemed to collect personally identifiable information or prospect information online, even though that information may be immediately deleted and not maintained for further use by an organization.

Openness Principle
One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Cooperation and Development (OECD). According to this principle, there should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

P

Permission
Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permission must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data
Personal data refers to any personally identifiable information that relates to an identifiable individual (or data subject). See *Personally Identifiable Information*.

Personal Information
See *Personally Identifiable Information*.

Personally Identifiable Information
Personally identifiable information is one or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is sufficient to specify a unique individual.

The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual, including name; address; phone number; social security number; e-mail address; driver's license number; financial account or credit card number and associated PIN number; and Automated Integrated Fingerprint Identification System (AIFIS) identifier, booking, or detention system number.
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s), including geographic information system (GIS) locations, electronic bracelet monitoring information, etc.

Privacy

The term privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.

Other definitions of privacy include the capacity to be physically alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Compromise

A privacy compromise is a scenario in which an unauthorized individual, or group of individuals, is able to gain access to personally identifiable information about another individual.

Privacy Policy

A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection

This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Privacy Champion (or Sponsor)

The project champion or sponsor is a high-level individual within the organization who has been selected to drive the privacy policy development effort. The champion helps steer the development of the privacy policy, identifies and allocates the necessary resources (both human and other support), and oversees policy implementation. This person provides a strong voice for the team effort, particularly when there is competition for scarce resources, and provides the mechanism for efficient decision making when the project team leader or project manager does not have the authority to make decisions in selected areas.

Project Team

The project team is a multidisciplinary group of individuals, representing a broad array of perspectives, who collaborate on the development of the privacy policy. This team represents the core agencies that are entrusted with the protection of private information for justice information sharing. See *Stakeholder*.

Project Team Leader

A project team leader is someone who will direct and manage the privacy policy development project on a day-to-day basis. The project team leader should possess the following essential characteristics: organizational credibility, organizational authority, ability to build and manage coalitions, and ability to manage day-to-day tasks over an extended period of time.

Prospect Information

Prospect information is defined the exact same way as personally identifiable information except that it is submitted by an individual who is not the subject of the data and who is giving personally identifiable information about someone else. This personally identifiable information about someone else is considered prospect information.

Purpose Specification Principle

One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Cooperation and Development (OECD). According to this principle, the purposes for which personal data are collected should be specified no later than at the time of collection, and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes, and as are specified on each occasion of change of purpose.

R

Record

Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Repudiation
The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retrievable Information
Information is retrievable in the ordinary course of business if it can be retrieved by taking steps that are taken on a regular basis in the conduct of business with respect to that information or that an organization is capable of taking with the procedures it uses on a regular basis in the conduct of its business.

Information is not considered retrievable in the ordinary course of business if retrieval would impose an unreasonable burden or violate the legitimate rights of a person that is not the subject of the information. The unreasonableness of burden is balanced against the significance of the information's use.

Right to Privacy
The possible right to be let alone, in the absence of some reasonable public interest in a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

The right to privacy as a matter of constitutional law is understood to have begun with a pioneering law review article, "The Right to Privacy," in the *Harvard Law Review* in the 1890s, written by lawyers Samuel D. Warren and future Supreme Court Justice Louis D. Brandeis. See *Privacy*.

Role-Based Authorization
A type of authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

S

Safeguard
A safeguard is considered a technology, policy, or procedure that counters a threat or protects assets.

Secondary Data Uses
Uses of personally identifiable information for purposes other than those for which the information was originally collected. The Organization for Economic Cooperation and Development's (OECD) Fair Information Principles (FIPs) state that a person can provide personally identifiable information for a specific purpose without the fear that it may later be used for an unrelated purpose without that person's knowledge or consent.

Secure Sockets Layer (SSL)
A protocol that provides secure data communication through data encryption. This protocol enables authentication, integrity, and data privacy over networks through a combination of digital certificates, public-key cryptography, and bulk data encryption. This protocol does not provide authorization or nonrepudiation.

Security
Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes.

Computer and communications security efforts also have the goal of assuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Security Policy
A security policy is different from a privacy policy. A security policy alone may not adequately address the protection of personally identifiable information or the requirements of a privacy policy in their entirety. A security policy addresses information classification, protection, and periodic review to ensure that information is being stewarded in accordance with an organization's privacy policy. See *Privacy Policy*.

Security Safeguards Principle
One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Cooperation and Development (OECD). According to this principle, personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Stakeholder
A stakeholder is an agency or individual that is essential to the development and implementation of the privacy policy and who contributes to, but is not a member of, the project team. Stakeholders have interests in the outcome of the privacy policy and provide input (for example, focus groups, surveys, documents for public comment, or invited speakers at team meetings). See *Project Team*.

T

Transborder Flows of Personal Data
Movements of personal data across national borders. See *Fair Information Principles (FIPs)*.

U

Use
With respect to personally identifiable information, the sharing, employment, application, utilization, examination, or analysis of such information within the agency or organization that maintains the designated record set.

Use Limitation Principle
One of the eight Fair Information Principles (FIPs) developed by the Organization for Economic Cooperation and Development (OECD). According to this principle, personal data should not be disclosed, made available, or otherwise be used for purposes other than those specified in accordance with the Purpose Specification Principle, except with the consent of the data subject or by the authority of law. See *Purpose Specification Principle*.

V

Values Statement
The core principles and philosophies that describe how an agency conducts itself in carrying out its mission.

Virtual Private Network (VPN)
The extension of a private network that provides encapsulated, encrypted, and authenticated logical (not physical) links across shared or public networks. VPN connections typically provide remote access and router-to-router connections to private networks over the Internet.

Virus
A code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or data. See *Worm*.

Vision Statement
A compelling and conceptual image of the desired, successful outcome.

Vulnerability
Any weakness, administrative process, act, or physical exposure that makes a computer susceptible to exploitation by a threat.

W

Worm

A self-propagating malicious code that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such as consuming network or local system resources, possibly causing a denial-of-service attack.

Glossary of Cited Resources for Terms and Definitions

- "Data Anonymization" definition courtesy of subject-matter expert Mr. John Bliss, Privacy Strategist—Entity Analytic Solutions, IBM.
- Better Business Bureau, BBBOnLine Privacy Program, *Privacy Terms and Definitions*, www.bbbonline.org/privacy/help.pdf.
- University of Miami Ethics Programs, Privacy/Data Protection Project, Encyclopedia, Index, http://privacy.med.miami.edu/glossary/index.htm.
- Privacilla.org, *Privacy and Government*, Organization for Economic Cooperation and Development (OECD) Guidelines, www.privacilla.org /government/oecdguidelines.html.
- Organization for Economic Cooperation and Development (OECD), OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980, www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html.
- Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy," *Harvard Law Review* 4, 1890:193.
- Clarke, Roger. Privacy Introduction and Definitions, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, September 16, 1999, www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.
- Birnbaum, Adam. Blue Cross Blue Shield Association (BCBSA), Health Insurance Portability and Accountability Act (HIPAA), *Helpful HIPAA Terms and Definitions*, www.fepblue.org/privacyhipaa/privacyhipaadefined.html.
- Law.com, ALM Properties, Inc., *Law.com Dictionary,* http://dictionary.law.com/.

- Microsoft Corporation, *Microsoft Security Glossary*, October 29, 2002 (Revised May 20, 2005), www.microsoft.com/security/glossary.mspx.

APPENDIX C: PRIVACY TECHNOLOGY FOCUS GROUP

REFERENCE MATERIALS

Organization for Economic Cooperation and Development: ***(OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data***
(http://it.ojp.gov/documents/OECD_FIPs.pdf)
The eight Fair Information Principles (FIPs) contained within this OECD document were developed around commercial, not justice, transactions and the transborder exchange of information. However, they do provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems.

Justice Information Privacy Guideline: ***Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*** (http://www.ncja.org/pdf/privacyguideline.pdf)
The goal of this Bureau of Justice Assistance (BJA)-sponsored guideline, produced in partnership with the National Criminal Justice Association, is to provide assistance to justice leaders and practitioners who seek to balance public safety, public access, and privacy when developing privacy policies for their agencies' systems. This guideline was prepared through the collaboration of nearly 100 local, state, and tribal justice leaders, as well as academia, elected officials, the media, and the private sector.

Global Justice Information Sharing Initiative: ***Privacy Policy Development Guide***
(http://it.ojp.gov/documents/Privacy_Guide_Final.pdf)
The Guide is a practical, hands-on resource geared toward practitioners charged with developing or revising their agency's privacy policy. Using this document is the next logical step for those justice entities that are ready to move beyond awareness into the actual policy development process. While this manual may certainly be of interest to justice leaders, the target reader is the professional tasked with getting the job done. Appended to this Guide are two excellent stand-alone resources: 1) *Privacy and Information Quality Policy Development for the Justice Decision Maker*, a high-level overview booklet introducing the framework for a systematic consideration of privacy and information quality policy and practices within an executive's agency and 2) Glossary of Terms and Definitions. These resources were produced by the U.S. Department of Justice's Global Privacy and Information Quality Working Group, a component of the Global Initiative, with guidance and leadership from BJA.

Global Justice Information Sharing Initiative: ***Applying Security Practices to Justice Information Sharing*** (http://it.ojp.gov/documents/asp/)
This document contains background information, overviews of best practices, and guidelines for secure information sharing. Fifteen disciplines have been identified that span the important elements of information security architecture. Executives and managers should use this document as a resource in securing critical justice information systems and suggesting

ideas and best practices to consider in building their agency's information infrastructure. This resource was produced by the U.S. Department of Justice's Global Security Working Group, a component of the Global Initiative, with guidance and leadership from the BJA.

Privacy and Civil Rights Policy Templates for Justice Information Systems
(Please contact Focus Group participant Alan Carlson at acarlson@jmijustice.org for further information and/or copies of the Templates.)

These templates are designed to cover a range of computer-based justice information systems and can be used by entities that are developing or modifying an incident- or events-based records management system, a case management system, an integrated criminal justice information system (that supports the work of or is used by several agencies or courts), a criminal history record information system, or a criminal intelligence gathering system and/or entities that are creating or joining a justice information sharing network.

The policy templates are intended for systems that seek, receive, store, and make available information in support of criminal investigations, crime analysis, law enforcement, protection of public safety or health, or other matters handled through the justice system. The templates are also relevant to the administration of justice, strategic/tactical operations, and national security responsibilities.

APPENDIX D: PRIVACY TECHNOLOGY FOCUS GROUP

TOP PRIVACY TECHNOLOGY ISSUES SUBMITTED BY EACH PARTICIPANT

Given the depth of experience of participants, a valuable initial Focus Group activity was requesting that each attendee list on index cards his/her top five justice-related privacy policy issues that can be addressed by technology. The individual issue cards were then grouped into common subject matters, revealing both common themes and a diversity of ideas.

The Focus Group Planning Committee feels these cards represent a valuable resource and should be presented in this report. While they have been grouped into subject matters, they are otherwise reproduced in their original form. (Please note: The subject matters of ***Access and Authentication***, ***Data Aggregation and Dissemination***, ***Identity Theft***, and ***Personal Safety and Protection*** are not treated below since they are addressed fully in the Focus Group report.)

Subject: Automation of Flow and Processes/Data Mapping

- Information sharing format—electronic sharing—appropriate way to disseminate to different requestor types. For example, in raw format, the requestor can easily manipulate and share data as they see fit; in a fixed text format, it is much more difficult—public, criminal justice agencies, etc.
- Ability to specifically tag privacy (or not) of data and information in the exchange design, that is, privacy rules moving with the data.
- Have business products more adequately support standards, e.g., Global JXDM.
- Every property in the Global JXDM has metadata to describe source and quality. How can these be used to support the FIPs? What additional metadata would improve support for the FIPS?
- There is a quality issue in that we cannot accurately identify the information about a person without a biometric ID. These IDs are only available from law enforcement and do not flow with the data.

- Issue—Business rules stated in a way that translates into functional and technical requirements. Examples:
  - Expungement
  - Sealing
  - Audit trail
  - Record access
  - Juvenile
  - Conviction
  - Criminal history
  - Business rules to define large segments of process: arrest, investigation, prosecution, conviction

- Spam—How does one ensure that e-mail does not contain spyware for a phishing exploit that may steal their personally identifiable information (PII)?

- Automation of flows/process engineering from data mapping to network mapping to PIAs—All of these flow processes, revisions, and reengineering can be better supported by technology—the easier to do, the more likely it will be done.

Subject: <u>Compliance/Accountability</u>

- SOA—When information is made available as a service, as opposed to sending it in bulk/batch, technologies such as digital signatures, access lists, or identity management may be required.

- Automated process to assess compliance with privacy policy.

- Accountability and enforcement—How can technology enable us to monitor system use to detect and prevent abuse, raise confidence and trust levels, and improve likelihood system will be used and operated in a lawful manner?

- How to trace back to source of "leak" to hold person accountable when information sharing systems dilute "evidence" trail of inappropriate/illegal disclosure.

- What technologies are available to ensure accountability for compliance with privacy policies?

- Ensuring that data is encrypted from databases, applications, data transfers, data sharing, and backup procedures will provide "data stewards" and the public with a higher degree of confidence that the FIP guidelines of security and use are adhered to.

- Auditing a criminal history system to determine accuracy of the data. With data coming from multiple sources, is there a way to best audit to ensure accuracy?

- Digitized court records—There is a large move toward scanning/digitizing court records. This is generally accompanied by public access via the Internet. Technology needs to be used to suppress or redact personally sensitive information from public release yet be retained for proper judicial use.

- Challenge of data accessibility by questionable users/sources.
  - Potential resolution: Federated ID Management

- Control of access and disclosure through technology, the ability to provide access where, and only where needed and appropriate and allowing disclosure only in a lawful manner.

- Public access to court/public record information via electronic/Internet technology. Data collected through legacy processes may include information (not considered appropriate) and possibly even (private) information about victims, witnesses, etc., which may be released to potentially harmful individuals. (Data review and authentication of requestor would limit release of certain data.)

- Authenticating people accessing information—to ensure appropriate access and use. Do you put the blinds on the inside of the window or on the outside? Security is an inhibitor or facilitator of privacy.

- Data sharing access and controls.
  - Potential resolution: SOA with Web services

- Leveraging data access across systems with controls/security.
  - Potential resolution: SOA/Enterprise service bus usage within open architecture

- Countless legacy systems collect personally identifying information—Software filters should be developed to identify this information so that its access and dissemination can be tracked and monitored.

- Authorization—Use Lightweight Directory Access Protocol (LDAP), identity management, and role-based permissions to ensure privacy.

- Auditing/enforcement—Use logging and data mining to make sure data isn't being accessed for inappropriate purposes.

- Authenticating participants in the criminal justice system.

- Anonymization of personally identifiable information for privacy-enhanced information sharing. Because if data can be shared in an anonymized form with a materially similar result produced by clear text analysis, why should data be shared any other way?

- Immutable audit to enhance trust in information sharing systems and encourage U.S. citizen support and data contributions.

- Automation/mapping privacy best practices/guidelines (e.g., automating Java Metadating Interfacing (JMI's) Privacy Policy Templates). Privacy policy creation can be vastly improved by automation. Too often, those involved skip hard thinking and move to "cookie cutter" PIAs.

- Tethered data—Organizations are sharing data without recording what they shared with whom. Data cannot be kept current (or redacted, where necessary) from secondary sources. Supports openness principle.

Subject: <u>Data Quality</u>

- Taking into consideration new standards (e.g., Global JXDM) and improved electronic communications, improve accuracy of information by relying strictly upon original source information (from records systems maintained by an agency) and eliminate copies of aggregated data.

- Records management/data standards—agreed formats, use of data standards, including compatible classification methods accounting for nontraditional data—PIF in information fragments can be better captured, catalogued, and made searchable.

- 90% of criminal justice data in law enforcement agencies is nonarrest. Accuracy and content confidence is often suboptimal. Technologies are available to improve accuracy and avoid the errors of garbage in/gospel out.

- In order to improve overall data quality, ensure that information initially collected—then updated and amended—is as accurate, complete, and up to date as possible.

- Data quality is a big concern—How can we use technology to ensure that a record is associated with the correct person?

- Use of Global JXDM/NIEM standard and "reference documents" will decrease the rate of errors incurred during system-to-system data translation, thereby increasing accuracy.

- How do we determine we are collecting useful or nonessential information? What are the guidelines?

- Expunging criminal records is practically impossible, since data are sold or given to third parties. This also goes along with correcting incorrect data.

- Use of technology to indicate ***information quality,*** that is, how accurate, complete, and reliable is a piece of information in a justice system?

- Criminal history collected on an individual who has fraudulently identified himself can lead to loss of employment or other negative incidents to the law-abiding citizen. Use of biometric identification can help ensure proper identification of arrested persons and prevent future discrepancies.

- Quality—When data is wrong/bad, privacy can be impacted. Technologies such as input validation, data cleansing in a data warehouse (ETL), or maintaining of the source as it moves from location to location.

- Data warehousing has the potential to provide the justice community with a great source for querying by law enforcement. However, incorrect identifiers may lead to false arrest if data collected is not subject to strict validation and timeliness policies.

Subject: <u>Data Ownership/Stewardship</u>

- Ability to modify sensitivity level of data and update those that have it (involves ownership).

- Ownership of data—as it crosses systems—transactions are logged creating a "new" database of information that can be used for a new purpose (i.e., N-DEx—What new issues arise and how are they fixed?).

- Control of data usage after dissemination (ownership of data).

Subject: Expungement/Retention

- The ability to amend, update, change, delete (seal or expunge) data that moves beyond the originating system—How can technology track and audit and deal with that data?

- How do we force all agencies and companies to protect the display of personal information within when it is not needed? For example, all you need to see is the last four digits of a social security number on credit cards. How about reports?

- How can technology address the issues of sealing and expunging records? What about correcting inaccurate information that may have been sold or aggregated?

- How to deal with expungements and delayed sentences with technology and information sharing?

Subject: Granular/Discrete Data

- How can technology facilitate the "tagging" or data with the associate FIPs' information so it may be carried with the data through an integrated system?

- How to denote the sensitivity level of data at a granular level within a document/database?

- Hiding unique identifiers in the transactional databases, but leaving them useable.

Subject: Inherent Privacy Issues Associated With Technology

- Issues inherent with new technologies such as Radio Frequency Identification (RFID), which pose potential to conduct electronic surveillance without an individual knowing it. RFID implemented in store stock, clothing, vehicle cargo, etc.

- Understanding the interconnectedness and secondary effect of multiple technologies re: privacy.

- Service-Oriented Architecture (SOA).
  - Granular delivery of functions/data
  - Minimizes need to consolidate data

- Enterprise Service Bus.
  - Pub/sub
  - Web services gateway
  - Granular/auditable access to services in SOA

- How do we protect the transmission of personally identifiable information through wireless means?

- A move towards an SOA infrastructure puts registry or index information "out there." This causes many concerns. How do we mitigate these concerns?

Subject: Organizational Behavior

- Business partners unwillingness to share identifying information.

Subject: Policy

- Configurable models.
  - I.e., classification of common sharing scenarios as a platform upon which privacy policies can be embedded in technologies

- Trust authorities—Enhanced review and oversight. Sharing needs to be predicated on trust across organizations to the extent that technologies can help establish compatibility across enterprises and can provide audit and policy oversight, then trust will be enhanced and greater sharing can be accomplished. There needs to be oversight/auditability of the trust authority as well.

- How technology development and implementation can support evolving privacy standards and risks.
  - I.e., privacy is not static, but both affects and is informed by new technology capabilities

- Secondary use.

- Preference Management—How do we ensure that data is being processed in adherence with the owner's wishes?

- Who or what agency should be responsible for taking the lead on managing and monitoring the development of the technological and policy framework related to privacy policies and safeguards? Who should audit it? Who defines the technological or policy standards?

- How do you define and articulate the risks associated with privacy in the context of Criminal Justice Information Services (CJIS) technology? How do you educate policymakers on the importance of privacy and its direct relationship to technology?

- FIPs don't fully take into account either the capabilities or the problems of modern systems.

- Cannot get consistent privacy policies (or even definitions) for specific services across organizations.

- Privacy laws and practices in the U.S. are failing to keep pace with the North American-wide free flow of people post-NAFTA. Cultures and procedures need to change to allow technology to be leveraged to provide accurate information.

- The intelligence/information gathering push post-9/11 appears oftentimes at odds with both FIPs and with current system abilities to absorb and interpret that information.

- How can you possibly get Jane and Joe users (customers) to understand how their information is going to be used and why?—aside from saying, "We don't share this information?"

- Public agencies face liability for the release of wrong data and criticism for failure to release the right data at the right time. What kind of assurances can minimize their liability for releasing or not releasing data?

- Review FIPs in the context of ***current*** technology capabilities to determine whether they need to be modified or supplemented. Two areas that need to be addressed:
  - Aggregation of information, particularly ownership and control
  - Information passing end to end through multiple systems and owners

- Privacy becomes the new roadblock to information sharing for those who really don't want to share. Technology no longer can be called too hard, too expensive, so privacy gets stood up in its place.

- Regulatory compliance—Companies need to be able to ensure that accesses to data are being done in accordance with regulatory legislation and corporate policy.

- Data access control—How do companies ensure that employees are only accessing data that is appropriate to their role?

Subject: Privacy Policy/Technology Standards, Legacy Systems

- How do you use technology to apply privacy policies to legacy systems?

- N-DEx privacy concerns—While privacy policy for N-DEx has not yet been articulated, technology will need to be in place to foster the policy. Failure to ensure privacy will doom N-DEx.

- Identification of technology standards that may be used to support privacy requirements in integrated systems.

- Cannot implement privacy policies in consistent way using technical standards (many corollary issues).

- Cannot translate privacy policies into precise technical requirements (many corollary issues).

- Identification of standards related to the logging of the dissemination and/or use of personally identifiable data to facilitate auditing.

Subject: Security

- Current legacy systems are incapable of meeting FIPs' criteria and technology can be used to manage that data to bring it into standard.

- Security of transmission of sensitive data.
- Protecting case notes of all players in justice system.

- Build ***convenient***, accurate system for fast, easy, secure retrieval of information.

- Recognize that a system's security policy is not privacy policy, but with the right emphasis, security can help safeguard personally identifiable information.

Subject: Solutions

- Automated analysis (e.g., Entity Analytics) eliminates subjectivity.

- System usage analysis.
  - Tools to detect anomalies in system usage

- Global JXDM—Use it to enable exchange of privacy-related information, like level of privacy intended or proper context for use.

- Software applications that support policy analysis through information flow mapping—geared to:
  - Identifying privacy issue risk points in the flow and walking users through potential solutions
  - Identifying different privacy needs based on position in the information flow and surrounding context.

- What is the current state of technology? In other words, what are the risks, gaps, and needs? Strengths? What does a "good system" look like?

- Building privacy into System Development Life Cycle—beginning in concept phase:
  - Concept
  - Requirements definition
  - Design
  - Development and text
  - Deployment
  - Production and operation
  - Retirement

- Applications that allow for correction of information across multiple entities.

- The Global JXDM should be modified/altered/enhanced to include data elements specific to privacy needs and issues.

- When interfaced with other databases, emerging and developing technologies such as RFID and Distance Facial Recognition pose privacy risks

- Identifying information exchange packages that could be incorporated with other Information Exchange Packages (IEPs) that would overlap privacy on each exchange.

- Confidence-building/educational efforts re: use of technologies in information sharing context to inform proper expectations of privacy.

- Interactive Service Level Agreement (SLA) to facilitate preparation/completion of a Privacy Impact Assessment.

- Data elements in Global JXDM which are necessary to manage privacy.

- Data integration, in an enterprise environment, can lead to the release of private information collected by one agency and retrieved by another. The use of meta tagging to identify particular data elements as private/confidential can help prevent such incidents.

Subject: <u>Miscellaneous</u>

- Consistent implementation of standards between agencies at local, state, tribal, and federal levels.

- RFID and new technologies develop protocols to review and use of sensor-based, less obvious collection mechanisms. There can be physical tracking of things or people. As we go into more "aware" environments, we will have to deal with issues of tracking and purposes. RFID to identify persons with HIV in prison population for treatment and guard safety; could have function creep.

- How do we ensure that information made available is not stale? Record retention issues—Can technology help us track when to delete/archive data?

- Eliminating/reducing fraud
  - In original documents
  - In information transmission
  - In information storage/retrieval

- Lack of session state information when using Web services.