Privacy Technology Focus Group

Executive Summary

IJIS Institute

PRIVACY TECHNOLOGY FOCUS GROUP
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 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. Participants then formed three working teams and 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 recommendations for their selected topics, presented in chart format at the conclusion of this briefing document. Additionally, detailed working team reports and recommendations are contained in the full *Privacy Technology Focus Group Report* and include adaptation of architectural frameworks, specific technologies, methodologies, and business practices.

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 groups 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.

- 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 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.

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?	
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.	
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.	
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*.

Working Team Three
Personal Safety and Protection
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

Recommendations	The working group concluded that recommendations from the preceding three working team reports address this issue.

About Global