



SEARCH

The National Consortium for Justice Information and Statistics

The Benefits of Using the Justice Information Exchange Model (JIEM) to Capture Privacy Requirements

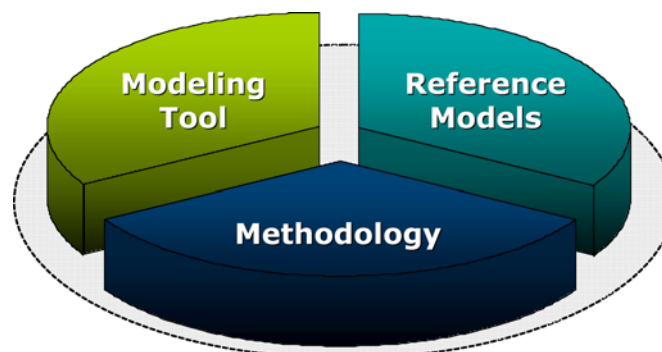
By Scott Came

Director, Systems and Technology
SEARCH

SEARCH, with the advice and consent of the Justice Information Exchange Model (JIEM) practitioner steering committee, plans to enhance the **JIEM conceptual framework** and **JIEM software tool** to allow JIEM users to capture privacy requirements in the same manner as they capture other information exchange requirements in JIEM. The purpose of this *Technical Brief* is to identify the benefits of this approach.

Background on JIEM

The **JIEM methodology**, developed by SEARCH with funding from the Bureau of Justice Assistance, U.S. Department of Justice, provides a structured framework for capturing the essential requirements of information exchange. For each exchange, JIEM identifies **who** is involved (what agencies/organizations), **why** the exchange is taking place (business process), **when** it takes place (business events and conditions), and **what** information is being exchanged. JIEM also includes **reference models**, which are the end-product of research to identify common or typical exchange requirements across jurisdictions, and which allow users to incorporate best practices into their own local requirements.



JIEM has been used by more than 100 jurisdictions over the past decade and has an active user base of several hundred practitioner and industry users.

More information about JIEM, see <http://www.search.org/programs/info/jiem.asp>.

Background on Privacy

As justice and public safety organizations exchange information, it is essential that they ensure proper protection of privacy and civil liberties. Several key documents from the Global Justice Information Sharing Initiative and Federal partners have emphasized the importance of information privacy. Most recently, the President's National Strategy for Information Sharing stated:

Protecting the rights of Americans is a core facet of our information sharing efforts. While we must zealously protect our Nation from the real and continuing threat of terrorist attacks, we must just as zealously protect the information privacy rights and other legal rights of Americans. With proper planning we can have both enhanced privacy protections and increased information sharing—and in fact, we must achieve this balance at all levels of government, in order to maintain the trust of the American people.

As the strategy indicates, proper planning—including identification of protected information and documentation of privacy policy rules—is a key step to protecting privacy while meeting the growing needs to share information.

In response to these concerns, the Global Information Quality and Privacy Working Group and the Global Security Working Group formed the Technical Privacy Task Team, which has developed a framework for capturing privacy policy rules.

Proposed Approach to Privacy Requirements Capture in JIEM

SEARCH has completed a preliminary design of an approach to capture privacy requirements in JIEM, and is planning to implement this design in the JIEM conceptual framework and software in 2008. This design is in part a response to the Technical Privacy Task Team's recommendation that Global leadership and the justice community should "evaluate [the] feasibility of augmenting the SEARCH JIEM Tool to define policy constraints for common information exchanges." The design also follows the Technical Privacy Task Team's conceptual framework.

The design proposes to enhance the JIEM conceptual framework as follows:

- Each exchange in JIEM will have one or more privacy policy rules associated with it.
- Each policy rule will include user and data categories, allowable actions, conditions, business purposes, and obligations that express the policy.

For example, a JIEM user may decide to define a person query in JIEM. As with the current JIEM framework, the user would define these elements, which form the *context* of this exchange:

- **agencies** (e.g., law enforcement, probation, courts)
- **events** (tip or lead), and
- **business processes** (investigation).

The user might also define the *content* of the exchange:

- the **query parameters** (e.g., driver's license number), and
- **expected results** (e.g., rap sheet, wants and warrants, etc.).

In addition, using the new privacy rule elements, the user might specify the *privacy requirements* of this exchange, as follows:

- Only sworn law enforcement officers (**user category**)
- are able to view (**allowable action**)
- personally identifiable information (**data category**)
- if their agency has signed a memorandum of understanding (**condition**),
- if the query is part of an authorized law enforcement investigation (**business purpose**), and
- if the agency discards all query results upon closure of the investigation (**obligation**).

Use of the privacy requirements capture features will be optional; that is, JIEM users will still be able to document information exchanges without capturing privacy requirements, if that makes sense for their project or situation. However, the JIEM conceptual framework will encourage users to consider privacy requirements at the proper place and time, and will provide easy-to-use support (via the Tool) for capturing those requirements.

SEARCH intends to follow the guidance of the Global Federated Identity and Privilege Management (GFIPM) initiative regarding the definition of user categories, as appropriate. This is still an open area of investigation.

Benefits of Capturing Privacy Requirements in JIEM

Enhancing the JIEM conceptual framework and software to include the capture of privacy requirements will result in the following benefits to the JIEM user community and the justice community overall:

- **Increased alignment of privacy and exchange requirements.** Maintaining privacy requirements in the same model as other information exchange requirements will improve consistency of requirements. Users will more easily and accurately reflect changes to requirements (and keep them aligned) if they are side by side, so to speak, in the same model and tool.
- **Increased attention to privacy.** The addition of privacy requirements to an existing information exchange requirements model involves less work than documenting

privacy requirements “from scratch.” The user-friendly JIEM application will also allow requirements capture with less writing and effort. Less effort means a greater likelihood that jurisdictions will give proper attention to the important subject of privacy.

- **Increased conformance to guidelines.** The JIEM software, through step-by-step “wizard” screens and similar interface capabilities, will help enforce the concepts of Global frameworks and guidelines as users document their requirements.
- **Increased consistency and reuse across jurisdictions.** A key factor in the ability to reuse requirements across jurisdictions is the consistency of terminology and structure in those requirements. The JIEM framework and software will enforce a high level of uniformity in how users define requirements (e.g., using standardized concepts like “data category,” “user category,” and so on). A standardized set of concepts used consistently across requirements models will dramatically improve the usability of models in other jurisdictions. This in turn will increase attention nationally to privacy issues.
- **Development of reference models representing national best practices.** Beyond sharing requirements models directly between jurisdictions, as envisioned in the previous paragraph, the capture of privacy requirements in JIEM will allow SEARCH to build (or expand existing) “reference models” that represent national best practices across a large number of jurisdictions. SEARCH will closely monitor users’ adoption of the privacy requirements capture functionality in JIEM, and will conduct research (as funding is available) to identify these best practices.
- **Cost savings from policy reuse.** Through both reference models and direct sharing between jurisdictions, the sharing of policy rules will reduce the cost of protecting privacy by allowing practitioners to “reuse and tweak” the work of others, versus having to re-think rules in every case. Just as with general information exchange requirements, many policy requirements will be very similar across jurisdictions, and the JIEM software will allow users to tweak these rules where necessary while directly reusing those parts that are the same.
- **Better ability to generate implementation artifacts.** The JIEM software will save requirements into an open, standards-based XML structure that can be transformed into “downstream” artifacts (such as eXtensible Access Control Markup Language (XACML)) that speed the implementation and deployment of policy rules at runtime. SEARCH does not intend to implement such transformations in the initial release of the JIEM-privacy functionality, but it will be relatively easy to do so in the future by leveraging the open “pluggable” nature of the Eclipse tools platform on which JIEM is built.

Direct questions about this *Technical Brief* to jiem@search.org.

This project was supported by Cooperative Agreement #2006-MU-BX-K006 by the U.S. Department of Justice Bureau of Justice Assistance. Points of view or opinions contained in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Francis X. Aumand II
Chairman

Ronald P. Hawley
Executive Director

Kelly J. Harris
Deputy Executive Director

SEARCH

7311 Greenhaven Drive, Suite 145 • Sacramento, CA 95831
(916) 392-2550 • (916) 392-8440 (fax) • www.search.org