Using Technology Principles to Create a Trustworthy Justice Information Sharing System.

Brett Gerke
(brett.gerke@oacp.org)

The Ohio Association of Chiefs of Police
6277 Riverside Drive, Suite 2N
Dublin, Ohio 43017
Phone: +1.614.761.0330
http://docs.olleisn.org

Share the power to protect.

OLLEISN™
Ohio Local Law Enforcement Information Sharing Network

Please do not quote or cite without permission of the authors.

This document was prepared under a grant from the U.S. Department of Homeland Security's (DHS's) State and Local Government Coordination and Preparedness (SLGCP) office. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. DHS or SLGCP.

Table of Contents

Acknowledgements

Parts of this paper were originally published as “Human Error, Trust and Trustworthiness”, Co-authored with my academic advisor, educator, and mentor, David Landsbergen, PhD. It was presented at the first annual Battelle Policy Days 1/22/2006, At The Ohio State University John Glenn School of Public Affairs.

Brett Gerke

Introduction

Historically, law enforcement officers would rely on their own instincts and knowledge, or make inquiries to a busy, faceless dispatcher and wait for answers. Today, these questions are being answered directly, using information technology. The responses to these questions are quicker, richer, and more accurate than ever before. Law enforcement personnel rely on the trustworthiness of their technology. It is the responsibility of the technologist to assure that these answers are accurate, rich, and responsive. It is also the responsibility of the technologist to assure availability of these systems anytime, anywhere and assure the accuracy and timeliness of the information. When an information system is trustworthy, it will be used, and relied upon by law enforcement personnel. By its very nature, it will become better. This paper will discuss the challenges and lessons learned by a law enforcement information sharing system developed by the state of Ohio (USA) and how the challenges were overcome in a manner that promoted trustworthiness in the information sharing system.

To date, the Ohio Local Law Enforcement Information Sharing Network (OLLEISN) is the most successful statewide law enforcement information sharing system in the United States. It continues to set the bar for other states to match. Much of the system's success can be attributed to how technology, operations and governance were used to accomplish the single goal of trustworthy information sharing.

Trustworthy Information Systems

One of the hallmarks of good policy is that it finds a pragmatic way to get agreement on what steps need to be taken next even in cases where there are ideological opponents. The Trustworthy Information System Model principles and the derived operating rules may provide a way to reconcile the interests of protecting private information and using information systems more intensely. A worthwhile goal for both interests would be the creation of strong systems that have high quality information. Both interests would benefit from information systems that make it clear where the information came from, how it has been used, who has "touched" that information and, for a person with the right credentials, track and audit any of these information flows.

Three Basic Operating Principles in Trustworthy Information Systems

Trustworthy Information Systems are "information systems that have integrity and have the capacity to produce reliable and authentic information and records"[1]. The three key operating principles are: integrity, reliability and authenticity. "Integrity" refers to the security of information -protection of the information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification. "Reliable" means that the information system can be trusted and that it has performed and will perform as expected. "Authentic" means that not only is there an appropriate level of "integrity" and "reliability", but that the system does have the information that is claimed to be there. This authenticity can be verified by a user through the tracking and auditing of the system through documentation of operating procedures and historical records of the transactions that have taken place. "Authenticity" could even mean that a user could track, or "drill down" summary information that is currently displayed on a computer screen all the way back to when and how that basic elemental information was first collected.

One good analogy in law that may actually be written into the business rules of

[1] Committee, O.E.R., *Ohio Trustworthy Information Systems Handbook,* 2001: Columbus, Ohio. P.63

how a computer operates is the “chain of custody” in documenting how evidence reached a courtroom or the foundation that must be laid before information can be introduced into court as evidence. Depending on the needs of the case, it may be necessary for a jury to hear the whole life cycle of that evidence to insure that the information being presented really is the information that it is claimed to be. The jury may hear from the person who originally collected the evidence, or from each person who had custody or possession as the custody was transferred from one person to the next; and it could even hear testimony from the person who conducted any analysis on that information or the person who retained custody of that information just before it was brought into the court room. These individuals may be asked to explain why that evidence is authentic, why it could not have been tampered with or what particular steps were taken to collect or analyze that information. While we certainly cannot expect all personal information to meet the same rigorous evidentiary tests in a court of law, some information may in fact have a long audit trail that needs to have some level of transparency in order for someone to trace the flows of information.

Operating Rules Derived from Principles

Several operating rules can be derived from these three principles: [2]

Clear definitions of information are necessary to be sure of the true origin, context, or content of the information. Without this information it becomes very difficult to know and understand what the information means and how useful it can be. The definitions of these data are also known as ‘metadata’.

When applied to describing the content and use of “documents”, metadata can contain many forms of information about the data: the source or author of the described dataset, how it should be accessed, what security controls are on that information and its limitations. Another very important type of data about data is the links or relationship among the data. In the case of Trustworthy Information Systems, specific metadata about personal information records could include information on:

1. Who has viewed this record?

2. Did they make changes to the record?

3. If changes were made, what did they change and when did they change it?

4. Who has access to this record now?

5. What is the history of ownership and / or possession of the data over its life?

6. What is the name of the information system in which this information now resides?

7. Where in that system does the information reside?

8. What is the list of the information systems in which this information resides?

9. What errors or corrections were made?

10. What kinds of reports or analyses utilized this information?

11. What kinds of information systems was this information sent to?

12. Who initially created the data that went into the creation of this information?

A second operating rule involves the “ownership” of that information. Information ownership must be established and rules governing that ownership (and possession)

[2] It is important to remember that there is a distinction between sharing information about a system as distinct from the personal information itself.

be made explicit. With ownership comes responsibility and assigning ownership is a very important way to make sure that high quality is maintained. If the responsibility for maintaining a piece of information is assigned to everyone, no one will take responsibility when an error is found. Ownership, however, is not something that is avoided. Organizations and individuals often insist on having ownership rights and ultimate responsibility for data. If individuals or organizations are politically or managerially responsible, ownership of information would be one way to minimize political and managerial risk.

With ownership comes the responsibility that information is complete both as to the content itself and the metadata that informs its use. Different information and different users will have different needs and this will dictate when information is complete. Practically speaking, it may not be possible to be fully complete, and if so, it must be clear what is missing and where it can be found.

The Privacy Act already requires that "there must be no personal data record-keeping systems whose existence is a secret from the general public." While this statutory right already exists, practically speaking, most persons do not know of an easy way to learn about what systems are out there and what information they are collecting. In the same way that the Electronic Freedom of Information Act took advantage of advancements of information technology to make it easier for persons to access government information already made available, new privacy rules could use new technologies to make it easier to know what information is being collected about them.

Once information about these information systems are made more available, it becomes much easier for individuals or organizations to track and audit uses of the information. Clearly, not everyone will have access to all information since information publicly available about security details would compromise the information system and disseminating personal private information to the public would compromise an individual's privacy. Individuals and organizations would have different levels of authorization for different uses and needs.

When information is disseminated to other individuals or organizations, the dissemination rules and decisions made must be auditable and traceable. It is not always possible to receive the data from the source, but it is highly desirable to be able to trace that information back to a source, through the long linked "chains of custody" as information changes possession or there is added value. The paper now turns to OLLEISN, a current effort now in operation that applies the Ohio Trustworthy Information Systems Model to a law enforcement information-sharing network in Ohio.

OLLEISN: Real-world Case Study Where Trustworthy Principles Were Applied

"**Recommendation:** Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge." [3]

This recommendation from the 9/11 Commission in 2004 helped set the stage for law enforcement information sharing in the state of Ohio. Using funding provided under the Law Enforcement Terrorist Prevention Program, LETPP, the Ohio Local Law Enforcement Information Sharing Network, OLLEISN, was created as a statewide, voluntary, information sharing system initially targeting all local law enforcement agencies in Ohio. The OLLEISN project follows the principles for information systems used for homeland security as set forth by President George W. Bush[4]:

1. Balance information requirements with citizens' privacy

2. View the deferral, state and local governments as one entity

3. Capture information at the source

4. Create databases of record, which will be a trusted source of information

5. Continually evolve the systems to stay ahead of terrorists' ability to exploit our systems.

OLLEISN specifically addresses four needs of local law enforcement:

1. Prepare for and improve the ability to respond to emergencies, including terrorist attacks

2. Prevent and protect the homeland from terrorist attacks and acts of crime

3. Produce comprehensive and practical approaches and solutions to combating threats

4. Increase officer / deputy safety

Strategically, OLLEISN is able to share information with all justice information systems, nationally including (horizontally) law enforcement, courts, corrections and rehabilitation, probation, and (vertically) regional and national organizations such as the Federal Bureau of Investigation.

The OLLEISN technical development staff established a set of guiding principles for the development and implementation of the project. These guiding principles were intended to reflect the technical team's support of the overall project's guiding principles as well as establish a guideline for best practices and trustworthiness. The Ohio Trustworthy Information Systems model was very influential in the building of OLLEISN. It confirmed some things that OLLEISN was already doing and suggested some new ideas. The Project Guiding Principles are:

1. Maintaining local law enforcement agency control of OLLEISN through governance mechanisms that include open participation and comment upon systems.

2. Voluntary Participation was necessary to gain ownership by the contributing agencies. This was deemed critical for the project and the work entailed.

3. Policy of "Give to Receive" or "Pay to "Play". If an agency wants to

[3] The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2004, U.S. Government Accountability Office, Section 13.3, *Unity of Efforts in Sharing Information*

[4] The National Strategy for Homeland Security, July 2002, U.S. Department of Homeland Security, pp 55 – 58, *Information Sharing and Systems*

access information it must also provide information. This creates ownership in the system and increases the quality of the information. It also encourages law enforcement agencies to participate and share information and, in so doing, encourage common standards and practices.

4. Agency System Independence or Interchangeability. The use of OLLEISN does not depend on purchasing or owning a particular hardware, software or communications protocol.

5. The originating local law enforcement agency maintains data ownership by policy. This derives from the necessity that agencies maintain control. Since OLLEISN is only a repository of the agency's data, the agency would still be responsible for the quality of the data in OLLEISN.

All information in the OLLEISN system belongs to, and is under control of, the originating agency. This puts the responsibility for accuracy, legitimacy, and propriety, and timeliness of the information in the hands of the system of record. Errors are bubbled up to the originating agency for disposition. This system of "trust yet verify" adds to the strength of the overall system.

From these Project Guidance Principles, the project team derived a set of technology principles including building open systems, use of XML as a document metadata standard, extensive use of information systems for auditing and logging and specific provisions for tracing information flows. [5]

Open Systems

OLLEISN is an open system. According to X/Open, a standard setting body for open systems, open systems can be defined as "computers and communications environments based on de facto and formal interface standards."[6] They openly describe how things are done. The act of publishing these standards means that there can be no proprietary restrictions on using the data. In addition to providing a very powerful error correction mechanism, the open systems approach promotes competition and reduces or eliminates many costs in buying software and hardware. Open systems result in portable and more interoperable systems. This concept is the basis for the "open source" movement and explains why software like Linux and Red Hat are offering a viable business model to the proprietary approach where the standards on how information is handled and processed are not public (e.g., Microsoft's ownership of its computer code).

OLLEISN utilizes the W3C (World Wide Web Consortium) standardized web services including SOAP (Simple Object Access Protocol) and XML (eXtensable Markup Language). The principles of 'open system' are further assured by publishing all design and development documents on a web site for the developer community to review and comment. The OLLEISN project also runs a discussion web site to complete the feedback loop. These sites are open to the public. In the design, development and implementation process, the OLLEISN team has made specific requests for review and feedback from the vendor community as well as the IJIS institute, a private industry working group based in Washington, D.C.[7]

[5] The complete list of items include: 1) Common Components; 2) National and Industry-Standard Protocols and Open Systems Technology; 3) Security Standards and Best Business Practices for Security; 4) Robust Management Features for Access Control and Auditing; 5) Robust Operational Features for Error Handling, Debugging, and System Testing; 6) Scalable Environment; 7) Data Standards; 8) System Performance; and 9) Query Flexibility.

[6] Tam, Patrick Y. K. Chau; Kar Yan. 1997. Factors Affecting the Adoption of Open Systems: An Exploratory Study. *MIS Quarterly* 21 (1):1 - 24.

[7] http://www.ijis.org

Using XML allows for, and promotes the use of, a reference model. The Department of Justice Services, The Bureau of Justice Assistance[8], and Georgia Tech developed such a reference model for use with all justice systems, nationally the Global Justice XML Data Model, GJXDM.[9] There were several rules used to guide the development and use of the XML data model.

1. The OLLEISN exchange model will be based on the GJXDM reference model. A minimum use of extensions to the GJXDM is the goal.

2. It is necessary to balance volume with completeness for traceability to context. This rule allows us to make decisions based on space required for the data, traceability and auditing of the records, and performance of the system.

3. Extensive use of attributes for super types is discouraged since all elements below inherit these attributes. This will allow tighter attribute designations for each individual data element.

4. The OLLEISN system will always track creator, expiration date (if any), and origination date of all information. This is to be built into the data model.

Metadata and XML

An advantage of XML is that it supports metadata as attributes. Metadata is commonly defined as 'Data about data'. OLLEISN uses definitions that are more descriptive:

- Data resource data – "data that is useful to understand how data can be used as a resource"[10]

- Or, according to Eliot Kimber "One way to distinguish metadata from content is to ask the question "If I remove this data, would my understanding of or ability to comprehend the content change? If the answer is no, it's metadata. Otherwise, it's content."[11]

The use of XML has some limitations that can be mitigated. The first problem is that the OLLEISN data model is an adaptation of the GJXDM; the design team of the OLLEISN project may have different ways of interpreting the GJXDM model than other design teams. However, if all state or local models are based on the same reference model, the number of variances is greatly reduced. One of the best ways to mitigate the risk of differences in the interpretation of the reference model is to have a complete law enforcement exchange model based the GJXDM that others can adopt. Information Exchange Package Documentation (IEPD) of exchange models (including the OLLEISN exchange model) are currently available on the IEPD clearinghouse.[12]

Robust Management Features for Access Control and Auditing

Access to the OLLEISN system is controlled by hardware, firmware and software systems. Each law enforcement agency is connected to the OLLEISN central system through a Virtual Private Network Connection, VPN. The VPN provides a dedicated, secure 'tunnel' through the

[8] A Division of the U.S. Department of Justice

[9] http://it.ojp.gov/jxdm

[10] XML In Data Management, Peter Aiken and M. David Allen, Elsevier Inc. (Morgan Kaufmann Pub.), June 7, 2004, pp. 7, ISBN: 0-12-045599-4 Metadata was formally ISO 11179. "The data that makes data sets more useable by users."

[11] System Architecture with XML, Berthold, Daum and Udo Merten, Elsevier Inc. (Morgan Kaufamnn, Pub.), June 25, 2002, pp 74, ISBN: 1-55860-745-5

[12] http://www.it.ojp.gov/iepd/

Internet with assured encryption of all data from endpoint to endpoint. The Internet connection is also secured by ‘secure HTTP’, HTTPS. Once in the OLLEISN system, three forms of credentials are authenticated. The user’s login ID, Password and the ORI of the agency must match and permission for access existing in a Lightweight Directory Access Protocol server (LDAP). Only then is the user allowed to access the information contained in the system. Every query is logged for auditing purposes and is available upon request by any of the participating law enforcement agencies. Audit logs are retained for one year.

Traceability of data over time is critical to the system. By the time justice information is consolidated to the federal level, the detailed knowledge about a crime incident is minimal at best. Crime statistics at the federal level holds little more than a classification of a crime and the number of occurrences of that crime in a geographic area. Information about the people involved, the address where the incident occurred is not valued, and therefore ‘lost’.

Information could be lost at each handoff. It is therefore, the responsibility of each level to retain the capability to trace the information held at that level to that information’s origin. To facilitate this process, the OLLEISN system requires that all uploaded information have ‘origination tags’. These are XML tagged fields used to trace the information to the system of record. One of the two fields identifies the reporting organization, using the agency identifier, ORI number. The second field identifies the ‘unique key’ from the system of record. These two fields, when used together, allows a tie back to the system of record.

It is critical to each handoff point to have a complete set of information from each level below. Incomplete information can introduce errors in statistics derived and other inferences based upon the information. It is also the responsibility of each level to maximize the coverage of the information it intakes. Each agency accessing OLLEISN data is highly encouraged to extend the ‘origination tags’ to identify their own system.

Equally important as complete coverage is the overall accuracy of the data at each handoff point. Just as completeness of information, inaccuracy of data can introduce errors as statistics and inferences are based on this data. It is the responsibility of each participating agency to assure the accuracy of the data it is storing and providing to the next level.

Policy enforcement of Trustworthiness Principles

By Policy, all information in the OLLEISN system belongs to and is under control of the originating agency. This puts the responsibility for accuracy, legitimacy, and propriety, and timeliness of the information in the hands of the system of record. Extensive filters and business rules in the OLLEISN system helps assure the data is of the best possible quality. All errors found are bubbled up to the originating agency for disposition. This system of ‘trust yet verify’ adds to the strength of the overall system.

Conclusion

It is important for all participants in information sharing to rely on the trustworthiness of the systems and the information these systems contain. It is even more important when these systems are being used in mission critical systems such as those used by law enforcement. Law enforcement personnel only use what they can trust. Their computer information systems must have 'integrity and have the capacity to produce reliable and authentic information and records'. In short, it must be as trustworthy as their sidearm or ballistics vest.

References

Human Error, Trust and Trustworthiness, David Landsbergen, PhD and Brett Gerke, (Presented and Published, Battelle Policy Days 1/22/2006), The Ohio State University John Glenn School of Public Affairs

Committee, (Ohio Electronic Records Committee) O.E.R., *Ohio Trustworthy Information Systems Handbook.* 2001: Columbus, Ohio.

The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2004, U.S. Government Accountability Office, Section 13.3, *Unity of Efforts in Sharing Information*

The National Strategy for Homeland Security, July 2002, U.S. Department of Homeland Security, pp 55 – 58, *Information Sharing and Systems*

XML In Data Management, Peter Aiken and M. David Allen, Elsevier Inc. (Morgan Kaufmann Pub.), June 7, 2004, pp. 7, ISBN: 0-12-045599-4 Metadata was formally ISO 11179. "The data that makes data sets more useable by users."

System Architecture with XML, Berthold, Daum and Udo Merten, Elsevier Inc. (Morgan Kaufamnn, Pub.), June 25, 2002, pp 74, ISBN: 1-55860-745-5

Tam, Patrick Y. K. Chau; Kar Yan. 1997. Factors Affecting the Adoption of Open Systems: An Exploratory Study. *MIS Quarterly* 21 (1):1 - 24.

Transparent Accountable Data Mining: New Strategies for Privacy Protection, Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Chris Hanson, James Hendler, Lalana Kagal, Deborah L. McGinness, Gerald Jay Sussman, K. Krasnow Waterman, MIT CSAIL Technical report – 2006 – 007, On the Web at http://www.w3.org/2006/01/tami-privacy-strategies-aaai.pdf