

**USING TECHNOLOGY TO
IMPROVE PRIVACY
PROTECTION IN JUSTICE
INFORMATION SYSTEMS**



IJIS Institute

SECURITY AND PRIVACY WHITE PAPER

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following individual and his sponsoring company for authoring this document:

Dr. Alan Harbitter

Harbitter Consulting Group

The IJIS Institute would like to thank the following individuals and their sponsoring companies for their dedication and input to this document:

Chuck Georgo, *Committee Chair*

Nowhere To Hide

Jim Cabral, *Committee Vice-Chair, Security*

MTG Management Consultants

Susan Laniewski, *Committee Vice-Chair, Privacy*

SAL Consulting, LLC

Jim Harris

National Center for State Courts

Rob Kribs

Analysts International

Tom Sandbach

Justice Technology Consulting

Bob Sudlow

JISP Liaison

Beverly Allen

Booz Allen Hamilton

Robert Slaski

Open Networks

Tom Carlson

Tom Carlson Consulting

Joe Mierwa

Patriot Data Solutions Group

The IJIS Institute would also like to thank the U.S. Department of Justice (DOJ) Office of Justice Programs (OJP) Bureau of Justice Assistance (BJA) and the members of the Global Security Working Group (GSWG) for their comments and feedback.

This project was supported by Grant No. 2008-DD-BX-K009 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

TABLE OF CONTENTS

Acknowledgements	i
Table of Contents	ii
List of Figures	ii
List of Tables.....	ii
Section 1. Introduction	1
Section 2. The Fair Information Principles (FIPs) Provides a Good Framework	3
Section 3. Cryptographic Hash Functions Can Help with the Use Limitation Principle.....	5
Section 4. Global Work on Automating Privacy Policy	7
Standardized Languages for Privacy Rules.....	7
Centralization and Standardization of IT Security Services.....	7
Web Services Platforms	Error! Bookmark not defined.
Section 5. It's All About Trust	10
About the IJIS Institute.....	11

LIST OF FIGURES

Figure 1 -The one-way Cryptographic Hash can be used to hide PII.....	6
Figure 2 - Example database.....	6
Figure 3 - Database incorporating hashing.....	6
Figure 4 - Global-developed privacy technology framework.....	9

LIST OF TABLES

Table 1 - Fair Information Principles	4
---	---

SECTION 1. INTRODUCTION

The protection of individual privacy can be a significant concern in integrated justice information systems. So significant that, in some cases, the inappropriate handling of privacy issues has resulted in the downfall of planned or operational systems.

Until very recently, technologists have barely engaged in the discussion of privacy issues. This paper introduces the problem and describes existing and emerging technological tools that address privacy.

As justice information and databases are integrated, linked, and fused on larger scales than ever before, concerns for privacy have taken center stage. Identity theft has become a frequent and widespread crime. Mishandling of privacy information in public and private sector applications has grabbed the headlines all too often and increased the concern of private citizens that sensitive personally identifiable information (PII)¹ isn't being adequately protected.

At federal, state and local levels, privacy issues have caused the failure of information systems that could potentially have improved the safety of our nation. Two well-publicized examples are the Federal Total Information Awareness (TIA) program² and the Florida Multistate Anti-Terrorism Information Exchange (MATRIX) program.³ In both situations, significant effort, money, and time were expended on what seemed to be good, proactive law enforcement, but without

enough focus on significant privacy issues. Both programs were cancelled as a result.

It would be naive to believe that privacy challenges can be addressed solely with technology. However, until very recently, technologists have barely engaged in the discussion of privacy issues. Privacy requirements have been driven largely by those coming from legal backgrounds. However, even when there is a very good privacy policy governing the operation of information systems, there are few technology controls in place to assure that policy will be adhered to.

Often privacy policy is so complex that even those charged with the manual enforcement of privacy have difficulty understanding the rules and restrictions. For example, privacy requirements differ in different jurisdictions and domains; state rules may be more stringent than federal ones, and privacy rules for juveniles are more stringent than they are for adults. All of this has contributed to public lack of trust in the government's ability to protect PII and the situation where systems that can improve law enforcement either cannot be built or can only be built with severe operating constraints.

¹ PII is often considered to be any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.

²http://en.wikipedia.org/wiki/Total_Information_Awareness

³<http://en.wikipedia.org/wiki/MATRIX>

Technologists need to take a more active role in the design and implementation of information systems to explicitly address privacy and associated policies.

Over the latter 1990s and early into this millennium, it became common wisdom that information security mechanisms had to be built into an information system and not considered an afterthought. Today, the same holds true for privacy mechanisms. While implementing privacy policy with technology is still new ground, there are new tools emerging and old tools to draw on.

This paper begins with a quick review of the Fair Information Practices (FIPS)⁴ to set a baseline for discussion. Then two efforts to use technology to address privacy concerns are overviewed as an example of the potential for improving information systems and increasing public confidence.

“While implementing privacy policy with technology is still new ground, there are new tools emerging and old tools to draw on.”

⁴http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles

SECTION 2. THE FAIR INFORMATION PRINCIPLES (FIPS) PROVIDES A GOOD FRAMEWORK

Privacy advocates have developed the Fair Information Principles (FIPs) as a high-level guideline for building and operating information systems that protect privacy. While these guidelines generally apply to all information systems, they are particularly applicable to those in the justice community and have been used as the basis for many of the recommendations of the Global Privacy and Information Quality working group⁵. The FIPs identify eight principles that provide guidance for developing information systems that honor individual privacy rights. Those principles are listed in Table 1.

Technologists tend to focus on the fifth principle – implementing security mechanisms that are targeted at preventing unauthorized use or exposure of PII. This is certainly an important principle and there have been numerous, well-publicized events where this principle was not upheld.⁶ The result was exposure of very sensitive PII in a potentially damaging way, so improvements are needed in implementing principle five.

However, the principles getting the least attention from technologists, yet are

extremely important, are the limitation principles, two and four. Many of the objections of privacy special interest groups focus on whether data should be collected in the first place, and if it is collected, how it is used (or potentially abused) once it is available for processing.

Privacy special interest groups are particularly concerned about the temptation to “data mine” PII for purposes not stated in the information system’s original Purpose Specification (principle 1) and in ways that would violate privacy.⁷

At a minimum, there should be technological mechanisms in place that restrict the type of information that is collected and limit the use of that information to the Purpose Specification. Ideally, there would be technological mechanisms to support adherence to all eight FIPs.

⁵ *The Global Privacy and Information Quality Working Group is a subcommittee of the Global Justice Information Sharing Initiative – a Federal Advisory Committee (FAC) that advises the U.S. Attorney General. Many of the products of this working group such as “Privacy and Information Quality Policy Development for the Decision Maker” (http://it.ojp.gov/documents/200411_global_privacy_document.pdf) are based on the FIPs.*

⁶ *For example, the Department of Veteran Affairs learned in August 2006 that a computer was missing from a subcontractor that provides software support to the Pittsburgh and Philadelphia VA Medical Centers. The computer contained insurance claim data for approximately 16,000 patients treated in these two facilities or their community clinics.*

⁷ *There is a humorous and well circulated video at www.aclu.org/pizza/ that illustrates the nature of this concern by acting out a fictional scenario in which personal medical and financial information is inappropriately shared and abused in an attempt to tailor services to a consumer.*

Fair Information Principle	Description
1. Purpose Specification	Define agency purposes for information to help ensure agency uses of information are appropriate.
2. Collection Limitation	Limit the collection of personal information to that required for the purposes intended.
3. Data Quality	Ensure data accuracy—misrepresenting PII is a violation of privacy
4. Use Limitation	Ensure appropriate limits on agency use of personal information.
5. Security Safeguards	Maintain effective security over personal information so that it not accessed by unauthorized parties for unauthorized purposes.
6. Openness	Promote a general policy of openness about agency practices and policies regarding personal information so that the subjects of the data can understand how information is used.
7. Individual Participation	Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency.
8. Accountability	Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies.

Table 1 – Fair Information Principles

SECTION 3. CRYPTOGRAPHIC HASH FUNCTIONS CAN HELP WITH THE USE LIMITATION PRINCIPLE

One technological approach to ensuring that information is only used consistently with the Purpose Specification is to cryptographically transform it through use of a one-way hash. A cryptographic hash is an irreversible function that scrambles the value of a piece of information and produces a unique substitute value.⁸ For instance the hash of the social security number (SSN) and birth date “123-45-6789 January 1, 1980” might be “Di*hrGJ#sdfc321pFYUg.” The hashing process is illustrated in Figure 1. The original SSN cannot be determined from the hash value – even by the party that performed the hash.

As an example of applying hashing to protect privacy, consider a hypothetical and extremely simplified information system. Suppose that this system is designed with the Purpose Specification of determining whether someone with a specific SSN is a known associate of a radical group. Figure 2 illustrates a simple database to support this function. This database can be queried by SSN and the required function fulfilled. However, this database might also be used for other functions such as determining the name of someone with a specific SSN or data mining all the names and SSNs of people who are known associates of a radical group. While these functions may be useful for investigative purposes, they are not consistent with the Purpose Specification and would

likely violate the privacy policy statement for the system.

In Figure 3, the SSN is replaced with a hashed SSN. If an investigator would like to determine whether or not someone with a SSN of “123-45-6789” was an associate, s/he would first hash 123-45-6789 (or the system software would do it) and search for “djwie012p4058” in the database. Referring to Figure 3, that query would produce an affirmative response and the name “John Public”. However, the hashed database could not be used to generally link individual names and SSNs, nor could it be used to data mine the SSNs of those who were associates.

The selective hashing of PII is a basic technology tool that can be effectively used in supporting the Use Limitation principle. It is being considered for the design of a national database will support the REAL ID information system. The Department of Homeland Security (DHS) REAL ID program⁹ requires, among other things, that if an individual holds a state-issued REAL ID identification card, the card is unique across the country. Privacy concerns and potential implementation costs have made REAL ID a controversial program. Although the future of this program is still a matter for debate, our point is that there are technology tools that can be leveraged in programs such as REAL ID to address privacy.

⁸ As with the use of any cryptographic function, care must be taken to select a specific hash algorithm that meets the needs of its intended use. For example, the algorithm should comply with applicable regulations and the resulting hash code should be of sufficient length to maximize the probability of a truly unique hash for differing inputs.

⁹ http://www.dhs.gov/xprevprot/programs/gc_1200062053842.shtm

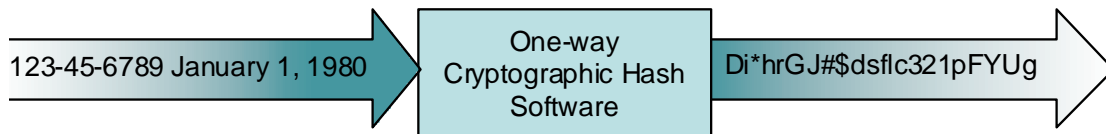


Figure 1 –The one-way Cryptographic Hash can be used to hide PII.

SSN	Name	Radical Associate?
123-45-6789	John Public	Yes
987-65-4321	Mary Citizen	No
555-55-5555	Jane Doe	Yes
101-01-0101	William Average	Yes
112-35-8133	Tom Anybody	No

Figure 2 – Example database

Hashed SSN	Name	Radical Associate?
djwie012p4058	John Public	Yes
Vjr093240^G	Mary Citizen	No
&^(IU66g5q	Jane Doe	Yes
49gh4000)0))6	William Average	Yes
Fj4903r0^NY02	Tom Anybody	No

Figure 3 - Database incorporating hashing

SECTION 4. GLOBAL WORK ON AUTOMATING PRIVACY POLICY

The Global Security Working Group (GSWG) is a subcommittee of the Global Justice Information Sharing Initiative (Global). Global serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration of initiatives. As stated on their web site, the mission of the GSWG is to, “enable the trusted sharing of justice information by recommending best practices for security guidelines, technologies, and procedures”. The GSWG, of late, has been developing the Global Privacy Policy Technical Framework.¹⁰ A central goal of the framework is to convert a written privacy policy to a machine-readable form so that an information system could assist in enforcing the policy.

There are a number of trends and new developments in information technology that make this concept a possibility. Among them:

Standardized Languages for Privacy Rules

There are now several existing and emerging standards for languages that can express privacy policy in a way that can be understood by computers. The eXtensible Access Control Markup Language (XACML) is an access control policy language implemented in XML and a processing model, describing how to interpret the policies. The XACML standard is managed by the OASIS standards organization (www.oasis-open.org/committees/xacml/). XACML is the standard preferred by the GSWG. There are other language standards available. The Enterprise Privacy Authorization Language (EPAL) is a formal language for writing

enterprise privacy policies to govern data handling practices in IT systems submitted by IBM to the World Wide Web Consortium (www.w3.org/Submission/2003/07/) for consideration. And finally, the Cascading Disclosure Control Language (CDCL), (www.wijiscommons.org/cdcl/) part of a research program being conducted by the State of Wisconsin, can be used to validate the logical basis of privacy policy. These tools support the expression of privacy policy statements such as “Only sworn officers conducting an investigation can access this information” in a formal syntax that could be processed by computer software.

Centralization and Standardization of IT Security Services

Legacy justice computer applications typically implement security on an application-by-application basis (e.g., access rights for criminal history information are defined and implemented within system A; access rights for case history information are defined and implemented independently within system B). With the advent of new software architectures such as web services,¹¹ IT security services, and, in particular, access control services, are implemented by central infrastructure utility software that can be accessed by all software applications. This type of architecture is better suited to layering on standardized privacy policy implementation software since all of the justice applications can be designed to filter information requests through common access control services.

¹⁰ http://it.ojp.gov/documents/Privacy_Report_Final_v_1_0_10-31-2007_with_cover.pdf

¹¹ http://en.wikipedia.org/wiki/Web_service

Off-the-shelf Products Provide Implementation Tools

Off-the-shelf software products are available to support the implementation of access policy in software. These tools implement software gates such as Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) that can interpret electronic versions of the privacy policy and permit or deny access to information based on that interpretation.

Figure 4 is adapted from the GSWG report summary¹² and illustrates the concept. At the center of this illustration is “the electronic policy statement” written, for example, in a language such as XACML or EPAL. This statement may need to reflect the policies of multiple jurisdictions. The PDP/PEP make determinations whether to permit or deny access to sensitive information based on the electronic policy.

The Global Privacy Policy Technical Framework is an aggressive and complex approach to implementing privacy policy. Implementing such a system requires first the conversion of the English language privacy policy to XACML, or another suitable, formal language. It requires information to be tagged to reflect its categorization for privacy purposes. It also requires users to be identifiable in terms of roles that are meaningful in the context of a privacy policy. For example, if information access is to be limited to “sworn officers”, a user must be identifiable as a sworn officer.

The framework is primarily targeted at two of the FIPS, Principle 4, “Ensure appropriate limits on agency use of personal information,” and Principle 5, “maintain effective security over personal information so that it not accessed by unauthorized parties for unauthorized purposes”. However, a machine-readable privacy policy is a powerful tool that can be used more generally for privacy protection in computer systems.

The GSWG is currently working on an implementation pilot to test feasibility in the real world. There is interest in other parts of the federal government in the idea of converting privacy policy to machine-readable form. For instance, DHS has a project in progress and has converted a few key policy documents into a structured language of their own design.

¹² http://it.ojp.gov/documents/Privacy_policy_flyer.pdf

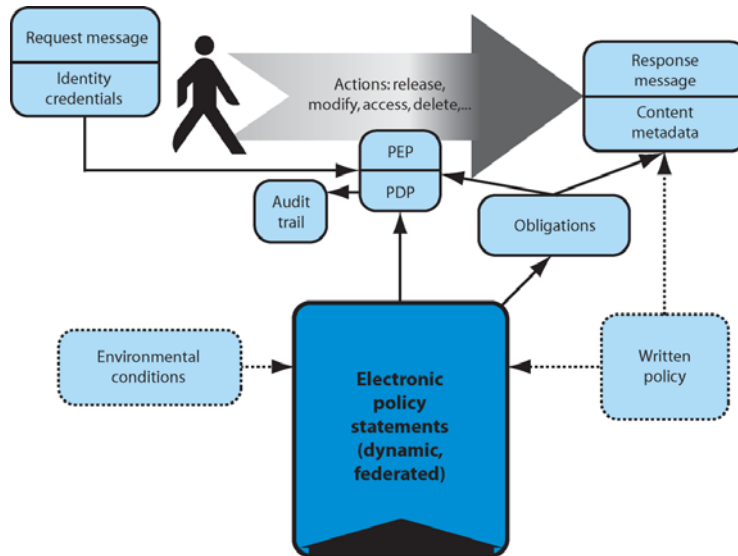


Figure 4 – Global-developed privacy technology framework

SECTION 5. IT'S ALL ABOUT TRUST

How far should we go to use technology to ensure that privacy policy is enforced? Far enough to engender confidence that personal privacy will not be abused by authorized or unauthorized users of the subject information system. Establishing that level of trust with the public-at-large, privacy special interest groups, the media, and oversight agencies is a lot easier when explicit steps have been taken to include technology in the system that addresses privacy.

The necessary groundwork for privacy is the development of a privacy policy and impact assessment by information system owners¹³. This foundational work should engage all system stakeholders. Specifically, the technology team should have involvement because such work builds understanding of privacy issues and concerns. From there, system designers and implementers need to creatively integrate technology in the system design and operation to enforce privacy policy, minimize the chance that the basic privacy tenets of the system can be violated, and build trust that the resultant system will improve the safety and security of its constituents, not diminish it.

¹³ See the Global Privacy and Information Quality Working Group's website at <http://it.ojp.gov/default.aspx?area=globalJustice&page=1151> for guidance on developing privacy policy and conducting privacy impact assessments.

ABOUT THE IJIS INSTITUTE

The [IJIS Institute](#), a 501(c)(3) nonprofit corporation, represents industry's leading companies who collaborate with local, state, tribal, and federal agencies to provide technical assistance, training, and support services for information exchange and technology initiatives. Serving as the voice of industry, the IJIS Institute unites the private and public sectors to improve mission-critical information sharing for those who protect and serve our communities.

The IJIS Institute was founded in 2001 as a result of the [U.S. Department of Justice's](#) interest in raising private sector participation in the advancement of national initiatives affecting justice and public safety, and more recently homeland security. Today, the IJIS Institute represents the [leading companies](#) serving these and other related sectors. The IJIS Institute provides assistance to government agencies by bringing industry to the table in a constructive role, and continuing to drive toward achieving high regard for the companies that are dedicated to helping the public sector find high value solutions. The IJIS Institute is funded through a combination of federal grants, industry contributions, and partnership agreements.

The IJIS Institute does its valuable work through the contributions of its member companies. The IJIS Institute thanks Alan Harbitter and the Security and Privacy Advisory Committee for their work on this document.

The IJIS Institute also thanks the many companies who have joined as members that contribute to the work of the Institute and share in the commitment to improving justice, public safety, and homeland security information sharing.

[Abstractian Group, The](#)
[Accelerated Information Management](#)
[Accenture](#)
[ACS State and Local Solutions](#)
[Advanced Justice Systems](#)
[Advanced Technology Systems \(ATS\)](#)
[AmCad Court Case Management, LLC](#)
[Amicus Group, The](#)
[Analysts International](#)
[Appriss, Inc.](#)
[ARC Consulting](#)
[Archer Group, The](#)
[BAE Systems](#)
[Bask Enterprises](#)
[BIO-key International, Inc.](#)
[BlueStreak Connect](#)
[Booz Allen Hamilton](#)
[BruckEdwards, Inc.](#)
[Cisco Systems, Inc.](#)
[Citizant](#)
[CivicUS](#)
[Cody Systems](#)
[CommSys Incorporated](#)
[Computer Projects of Illinois, Inc.](#)
[Core Technology Corporation](#)
[CourtView Justice Solutions](#)
[Data 911](#)
[Datamaxx Applied Technologies, Inc.](#)
[Deloitte Consulting](#)
[Development Services Group](#)
[DigitalBridge](#)
[Dykema Gossett PLLC](#)
[Eadie Consulting](#)

[eCorridor Inc.](#)
[Emergitech](#)
[ESRI](#)
[FATPOT Technologies, Inc.](#)
[FDM Software](#)
[FedSolutions, Inc.](#)
[Harbitter Consulting Group](#)
[Hitech Systems, Inc.](#)
[Holt, Sheets & Associates](#)
[HRInterop, LLC](#)
[Hunter Research](#)
[i2 Inc.](#)
[IBM](#)
[Intellitech Corporation](#)
[Interacx](#)
[Intergraph Public Safety](#)
[InterImage](#)
[Interop-Solutions, Inc.](#)
[iNovate Solutions](#)
[InTime Solutions, Inc.](#)
[IxReveal, Inc.](#)
[Justice Data Group](#)
[Justice Served](#)
[Justice Systems, Inc.](#)
[Knowledge Computing Corp.](#)
[Marquis Software Development, Inc.](#)
[Memex, Inc.](#)
[Metastorm, Inc.](#)
[Metatomix](#)
[Microsoft Corporation](#)
[Motorola](#)
[MTG Management Consultants, LLC](#)
[New Dawn Technologies](#)
[Niche Technology](#)
[Nixle](#)
[Nortel Government Solutions](#)
[NOWHERETOHide.ORG](#)
[Nuance Communications](#)
[The Omega Group](#)
[Online Business Systems](#)
[Open Networks](#)
[Optimum Technology](#)
[Oracle Public Sector](#)

[Pamet Systems, Inc.](#)
[Patriot Data Solutions Group \(PDSG\)](#)
[PCSS, Inc.](#)
[PNL Associates, LLC](#)
[Presynct Technologies, Inc.](#)
[PST Technologies](#)
[PSTG Consulting, Inc.](#)
[Public Safety Consulting, Inc.](#)
[Raytheon Company](#)
[RCC Consultants, Inc.](#)
[Readiness Resource Group Inc.](#)
[SAL Consulting LLC](#)
[SMART Public Safety Software](#)
[Spillman Technologies](#)
[SPSS Inc.](#)
[SRA International, Inc.](#)
[Sypherlink, Inc.](#)
[Syscon Justice Systems, Ltd.](#)
[Tetrus Consulting Group](#)
[Tiburon](#)
[Tom Carlson Consulting](#)
[Total Computer Group](#)
[TriTech Software Systems](#)
[Trusted Federal Systems, Inc.](#)
[Unisys](#)
[URLIntegration](#)
[VANTOS, Inc.](#)
[Versaterm Corporation](#)
[VisionAIR](#)
[Visiphor Corporation](#)
[Vortx](#)
[Waterhole Software](#)
[Whys Solutions, LLC](#)
[xFact](#)
[Yellow House Associates, LLC](#)