Information
and Privacy
Commissioner of
Ontario

Privacy Design Principles for an Integrated Justice System – Working Paper

Ann Cavoukian, Ph.D.
Commissioner
April 5, 2000

The Privacy Design Principles for Integrated Justice were prepared in a joint effort by the Office of the Ontario Information and Privacy Commissioner and the United States Department of Justice, Office of Justice Programs. A special thanks to the drafters of this document, Ann Cavoukian, Information and Privacy Commissioner, Brian Beamish, Director, Policy & Compliance Branch, and Michael Gurski, Policy & Technology Officer, Ontario, Canada, and Paul Kendall, General Counsel, and Anne Gardner, Attorney-Advisor, Office of Justice Programs, U.S. Department of Justice, Washington, D.C.

Information and Privacy Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Introduction

The justice system constantly balances the interests of protecting society and protecting the privacy of individuals. Personal information is collected and used by justice system agencies within a framework intended to:

- identify and apprehend offenders,
- adjudicate guilt or innocence of adult or juvenile offenders at trial,
- manage and resolve domestic and family legal issues,
- settle civil disputes,
- manage pre-trial activities,
- manage post conviction and post judgment activities,
- support the rehabilitation of the offender and restoration to victims,
- address repercussions to victims' and offenders' families,
- manage external risks, and
- maintain the integrity of the justice process.

Effectively managing personal information collected and used in the justice process by justice agencies needs to be a goal of any integrated justice information system. That goal can be accomplished through applying privacy design principles.

Purpose

This paper outlines a set of Privacy Design Principles, or policies, that would apply to the design and implementation of an integrated justice system. An integrated justice system includes the criminal[(1)] justice process, as well as civil court records, juvenile justice information, and probate proceedings. Increasingly, integrated justice systems also interact with information systems of affiliated agencies, such as heath, welfare, and transportation. Although this initial discussion of the principles focuses on the criminal justice process, many of the principles are suitable and applicable to civil, juvenile, and family court records in the context of an integrated justice system architecture. Issues such as public access and treatment of juvenile records will be specifically addressed in future guidelines.

This working paper is intended to spark informed debate in two areas. The first centers on the Privacy Design Principles and their applicability at various points within the justice system. The second area of debate centers on how technology can be used to implement the design principle policy. In this area, the paper describes 'technology design principles' to help a Technology Design Architect implement the Privacy Design Principles.

Background

Key players in justice systems around the world, from law enforcement, to prosecution and defense, through the courts and correctional institutions, to probation and parole services, are at various stages in using today's technology to integrate their systems' information and information management processes.

Current information systems in the justice sphere range from predominantly paper driven to highly automated and interactive systems. Despite the increasing use of information technology, however, in many state, local, and tribal jurisdictions, duplication of effort, delays in information transmittal, barriers to accessing information, as well as scheduling and case management bottlenecks are common. Many of these problems are the result of implementing individual technology solutions without integrating these solutions across the justice enterprise. Today's technologies, applied in an integrated fashion, hold the promise of reduced paper work, quick information capturing, broad transmittal and access capabilities, improved information quality, and reduced long-term costs. In the justice system, information technology also promises to help the effective administration of justice through the enhanced ability to collect, access and use information, including personal information. In addition to efficiency, managing privacy must be a component of any information technology system in the justice sphere. Information technology, to paraphrase Alan Greenspan, "is a perceived threat to privacy."[2]

A technology system that spans law enforcement, the courts, and corrections, as well as other justice components is an example of an enterprise-wide technology. Enterprise-wide information technology architectures, due to their complexity, require an enterprise-wide framework.[3] The 'architecture' is the underlying structure and protocols that determine specifications of how the technology is built and how information can be stored and accessed by various members of the justice system. The enterprise-wide framework is a tool that allows the necessary analysis from various perspectives, such as conceptual and designer views, to take place prior to committing to the resources to implement information technology.

An integrated justice system needs to address privacy within the enterprise-wide framework to manage privacy effectively. By addressing privacy directly within the framework at the planning stages, the resulting technology has the best chance of being privacy compliant. Otherwise, the result is having to manage unintended effects regarding privacy produced by new technology; and technology can have extensive unintended effects.[4]

Unintended effects have the immediate downside of diverting limited available intellectual capital and financial resources from the goal of implementing and using an integrated justice system to addressing policy and making technology changes retroactively. Given that privacy continues to grow as a public issue, unaddressed privacy concerns will likely absorb an increasing amount of limited resources in a combination of issues management and hasty coding changes.

For example, mismanaging the use of privacy policy in releasing personal information before trial could jeopardize the right to a fair trial (e.g. release of address or family affiliation). Likewise, using inaccurate information that misidentifies a person as an accused or suspected criminal would have potentially vast repercussions in an integrated justice system. The problem compounds when the system itself has difficulty authenticating or correcting information: garbage in, gospel out.

Privacy design principles should be considered at the design and development stages of any enterprise-wide architecture. Used in this way, the principles are the first steps to ensuring that the personal privacy of the suspected, accused, convicted, and acquitted, as well as victims, witnesses, and their families are managed effectively by the justice system. In other words, the system should operate without unintended effects to individual privacy that could hamper the effective carriage of justice.

The second step to guard against unintended effects is to conduct a privacy impact assessment. In short, the impact assessment acts as a litmus test from the conceptual through to the implementation stage of an integrated justice system. The privacy impact assessment ensures that the agreed upon privacy design principles are applied effectively. While outside the scope of this document, a model Justice System Privacy Impact Assessment for state, local and tribal governments is under development and will be available as a companion document to the Design Principles in the near future. Examples of Privacy Impact Assessments can be found on the Internet at:

http://www.gov.on.ca/MBS/english/fip/pia/pianew.html

http://ipc.developersedge.com/privacy_impact/welcome.htm

http://www.oipcbc.org/publications/pia/piam.html

http://www.austlii.edu.au/au/other/plpr/vol3/vol3No04/v03n04a.html

A History of Privacy Codes

The following history is provided to inform the discussion surrounding the development of privacy design principles and technology design principles that best address state, local, and tribal justice systems. The basis for privacy design principles worldwide is the Organization for Economic Cooperation and Development's (OECD) Fair Information Practices (FIPs), developed in the 1960's and '70's to address technology implications at the time. The FIPs were codified in the OECD guidelines in 1980 (see Appendix A). Despite advances in technology, the FIPs remain universally recognized as a solid foundation from which to build everything from privacy legislation to self-regulated privacy standards for the private sector.

Fair Information Practices[5] place restrictions on the collection, use and disclosure of personal information, and can be summarized as follows:

- limiting the collection and use of personal
- information for the purposes intended,
- ensuring data accuracy,
- establishing security safeguards,
- being open about the practices and policies regarding personal data,
- allowing individuals access to their personal data and the ability to have it corrected, and
- identifying persons to be accountable for adhering to these principles.

These principles, with some modification, form the basis for the proposed privacy design principles for an integrated justice information technology system.

Subsequent to the OECD Guidelines the European Union (EU) released its Data Protection Directive in 1995.(6) Under the Directive, data subjects are granted a number of important rights and may appeal to independent national authorities if they consider their rights are not being respected. These rights include:

- **information** from subsequent data users about where the data originated (where such information is available), the identity of the organization processing data about them and the purposes of such processing
- a **right of access** to personal data relating to him/her
- a **right of rectification** of personal data that is shown to be inaccurate, and
- the **right to opt out** of allowing their data to be used in certain circumstances (for example, for direct marketing purposes, without providing any specific reason).

For cases where data is transferred to non-EU countries, the Directive includes provisions to prevent the EU rules from being circumvented. The basic rule is that the data should only be transferred to a non-EU country if it will be adequately protected there, although a practical system of exemptions and special conditions also applies (such as for data where the subject has given consent or which is necessary for performance of a contract with the person concerned, to defend legal claims or to protect vital interests (e.g. health) of the person concerned).

In Canada, the Federal Government is in the process of passing legislation based on the Canadian Standards Association (CSA) Model codes. These codes have clear parallels with the OECD Guidelines and the EU Data Protection Directive. The CSA Model codes include:

Accountability

institutions are accountable for personal information they collect and shall designate an individual(s) to be accountable for compliance with this principle

Identifying Purposes

purpose of collection must be clear and done at or before time of collection

Consent

individual has to give consent to collection, use, disclosure of personal information

Limiting Collection

collect only information required for the identified purpose and information shall be collected by fair and lawful means

Limiting Use, Disclosure, Retention

consent of individual required for other purposes

Accuracy

keep as accurate and up-to-date as necessary for identified purpose

Safeguards

protection and security required appropriate to the sensitivity of the information

Openness

policies and information about the management of personal information should be readily available

Individual Access

> upon request, an individual shall be informed of the existence, use and disclosure of her personal information and be given access to that information, the ability to challenge its accuracy and completeness and have it amended as appropriate

Challenging Compliance

> ability to challenge all practices in accord with the above principles to an accountable body in the organization.

United States Department of Commerce has been working to develop and implement International Safe Harbor Privacy Principles (see Appendix B). The few details available on the Safe Harbor Principles suggest that American companies are leaning closer to the European model, since they would need consumer consent to transfer data to the United States and would be required to post notice of how the data would be used. The agreement would require United States companies that collect and manipulate the personal data of European citizens to sign up to virtually the same strict data protection standards in force within the 15-nation EU. Companies that violate their stated practices would be guilty of "deceptive business practices," subject to prosecution by the Federal Trade Commission and individual States, as well as being publicly sanctioned. As of March 31, 2000, The Article 13 Committee, the EU body responsible for the implementation of the EU Data Protection Directive, has not accepted the proposed Safe Harbor Principles. The Committee is expected to draft a list of areas for improvement in the United States proposal, predominantly the matter of individual redress for privacy violations.

Other countries have developed legislation similar to that discussed above[7] or continue with self-regulation.

Unique Characteristics of an Integrated Justice System

Information, Relationships, and Protocols

Fair Information Practices are a good starting point for developing privacy design principles. However, the justice system has a set of unique characteristics that must be taken into account. For a start, the right to privacy must be balanced with the need to carry out the administration of justice and its prime goal: protection of society. In addition, for the key players within the justice system, there is a need to access personal information on the accused, witnesses, and victims where it directly relates to the integrity and effectiveness of the trial process. As well, privacy design principles should not be viewed as changing the balance or diminishing the value of fairness inherent in the justice system. In other words introducing privacy design principles cannot give unfair advantage or create an unfair disadvantage to any part of the justice system. Finally, without overly dramatizing the situation, the way in which a justice agency uses personal information in the administration of justice is vital to the protection of society and can result in life or death consequences.

For these reasons an integrated justice system must have privacy protocols that recognize and distinguish the different purposes of specific types of justice systems. As well, the privacy protocols must recognize the relationships a person has with those justice systems; not just the types of information gathered and the conditions under which the information[8] was gathered and entered into the system. For example, a convicted criminal's personal information would be dealt with differently than a witness' personal information. A further example is that personal information collected for investigation may differ from information collected and used in a case processing system.

In addition, different information sharing rules apply. Rules, or protocols, for sharing information within the criminal justice system (e.g., police, prosecutors, the courts and corrections) would differ from rules used to determine the disclosure of that information to parties outside the justice system. For example, the police and prosecutors must share more information between them than is publicly available regarding an arrest.

These examples, while pointing to the complexities of managing personal privacy in an integrated justice system, should not cause one to jettison the value of privacy design principles. These principles act as overarching guide posts in the development of technologies that blend the collection of information and responsible information management in an integrated justice system.

Legislative Context

Most information systems world-wide are required to work within some type of legislative framework. However, an integrated justice system in the United States has to work within a detailed patchwork and array of legislation and regulations. Some is federal legislation, such as the Crime Control and Safe Streets Act,[9] and other is state-specific legislation that requires greater and lesser degrees of control of personal information. There is also a body of case law that rules on privacy challenges by persons against various state and federal legislation and practices. In addition, different states and tribes have varying policies and law regarding the degree of privacy a person can expect if he or she has a relationship with the justice system. Therefore, the legal context needs to be mapped clearly for each integrated justice system technology project according to the laws governing the jurisdiction.[10]

The Privacy Design Principles for an Integrated Justice System

Privacy design principles need to be built into the technology architecture at the outset of the technology initiative. For privacy design principles to be useful, beyond general discussion and agreement in the planning stage, however, they need additional specificity. Responsibility falls to the key integration partners of each project to generate this specificity as they develop and implement their integrated justice technology project. To expedite the work of integrating the privacy design principles in an integrated justice project, three steps have been taken within this paper:

- The internationally accepted Fair Information Practices have been used as a base from which to develop Justice-specific Privacy Design Principles;
- We have introduced a set of Technology Design Principles that provide a first step for the 'technology design architect' to bring each Privacy Principle into an enterprise architecture;[11]
- We have developed a matrix that can be used to undertake the necessary analysis of the data controls for collection and use of personal information that needs to be articulated for the major components of a justice enterprise architecture.

1. Purpose Specification Principle

When personal data are collected in a justice system, the system's purpose[12] should be specified in writing, not later than at the time of data collection.[13] The subsequent use (see Principe 4) must be limited to the fulfilment of those stated purposes (or other compatible purposes[14] that are specified on each occasion of change of purpose). As well, the personal data collected should be pertinent to the stated purposes for which the information is to be used.

The purpose statements also need to address various third party and private sector partnerships or relationships where personal data is or will be disclosed.

For example,[15] each component of a justice system (law enforcement/investigative systems, prosecutorial systems, defense systems, court systems, correction systems, and probation and parole systems) would have a set of stated purposes for collecting information. These purposes need to be articulated and harmonized prior to the technology design and prior to the outset of data collection. With an integrated system, data can be easily re-used in the future. However, the purposes for collection, by each component of a justice system, should be relatively stable.

Generally the purpose statements should directly relate to the mandate of the relevant sector of the justice system. For example, the purpose of law enforcement agencies for collecting personal information is to investigate (suspected) criminal activity to bring suspects to trial, where the purpose of the court system is to process cases, provide accurate and complete information for judicial decisions, and produce dispositions for complete criminal history records. The purposes of these systems should be harmonized to provide a "privacy framework" governing collection, use, and re-use of personal information.

Technology Design Principle

Organizations must clearly identify and document the purposes for collecting personal information. Systems design must ensure the systems outcome is limited to the purposes for which the personal information was lawfully collected and disclosed. We must pay attention in the design stage in all instances where personal information is disclosed regularly to one or more parts of the justice system. We must also pay attention to build a technology that easily enforces access restrictions to personal information available to parties outside the justice system. Information can be available through two methods:

- Information released by a component of the justice system, e.g., for public safety,
- Requested by a third party, e.g., the media.

2. Collection Limitation Principle

There should be some limits[16] placed on the collection of personal data. Personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent[17] of the data subject. It is important to remember that the knowledge and consent rights of individuals will vary depending on their relationship (e.g. suspect, offender, victim, witness, juror, offender's family) to the justice system.

A test of relevance should also be applied (e.g., by an independent third party or as authorized in legislation) when collecting personal data on individuals without their knowledge or consent, or when the individual is not charged with a crime, i.e., under investigation, or when an investigative body is 'information gathering'.

This principle differentiates between the knowledge and consent rights of an offender, arrestee, the victim, witness, juror, offender's family, or victim's family. Special consideration must be made to limit collection of personal information on victims, witnesses, and jurors (e.g., to test their credibility). For suspects or accused persons, although broader, the collection limits should be set by the legislative framework and legal precedent. However, obtaining a person's consent to collect their personal information is generally not applicable during case[18] investigation or prosecution.

The "collector" of personal information varies. In the criminal justices system, the collector is generally law enforcement. In the civil justice system it is the court. In the criminal justice system, personal information is collected by the investigative arm on suspects and those associated with the suspects, including victims, witnesses, and family members. In addition, most parts of the justice system collect personal information on offenders and those convicted, if only as a result of the actions, utterances and changing condition of the convicted offender. As well, personal information is generated by the workings of the justice system itself as the offender moves through the various components of the justice system.

Technology Design Principle

The limits and special circumstances set out in the collection of personal information principle must be incorporated into the design of information systems to ensure that extraneous personal information is not collected. We must define extraneous information for each relationship an individual has with the justice system. Generally, information is extraneous unless it has relevance to the integrated justice system's purpose statements. This definition is critical, as technology has the ability to automatically search for information on a person in an ever increasing number of data bases.

3. Data Quality Principle

Personal information, to the extent necessary for stated purposes, should be accurate, complete, current and verified.[19] This normally assumes that the person has some means of accessing the information to ensure it is accurate and up to date.

However, in the justice system other methods are needed to ensure that the data held are accurate and up to date. Those methods can involve passive data analysis, including cross-referencing, that identifies anomalies, plus authorized human correction that could involve the data subject. Separate from privacy concerns, data management and record retention need to be addressed as part of data quality. Inaccurate personal information can have a devastating impact on the person and the integrity of proceedings within the justice system. The accountability for data quality lies with the system's information steward as further described in Principle 8.

Technology Design Principle

We must design the technology to ensure efficient data access and correction. As well, the technology requires a streamlined methodology for logging or tagging the access and correction of information, recording changes, by whom, when, and for what reason, to ensure accountability. Where a record of corrections is retained the inaccurate information should not be routinely disclosed within the justice system.

To ensure data quality the technology design must foster "data verifiability." This is the process of ensuring data is sought where missing and flagged or excluded where found inaccurate. This process of data verification also demands a technology design that tags data as confirmed and either accurate or inaccurate, or to be confirmed.

For example, the technology design must have standardized security routines that address how certain people access the data and what standard of proof is required to amend data. For instance, the types of questions that need to be asked are, does a victim have access to all the data in the file or just his/her statement? Does technology allow for redaction of non-victim data? If an error is found, who decides what the correct information should be? Is there an administrative process with a legal standard — preponderance of the evidence (more likely than not) - for amending the information?

Finally, the technology needs to support data standardization across various data systems.[20] This would support use of same or comparable terms, data entry fields, data definitions and data structures. For example, date fields need to be interoperable, and field edits and meta-data definitions need to be consistent.[21]

4. Use Limitation Principle

Personal data should not be used or disclosed for purposes other than those specified in accordance with Principle 1 except:

a) with the consent of the data subject,

b) by the authority of law, or

c) for the safety of the community, including victims and witnesses.

Generally, personal information should be retained as necessary, but its use must be limited to its original purpose for collection as outlined in Principle 1. Use limitation,[22] generally, is more applicable where information is disclosed outside the justice system where issues of safety, risk, and the right to know by victims are factors applied in the use limitation principle. Within the criminal justice system, with the purpose for collection stipulated in Principle 2, the use limitation principle is also applicable under exception b) by the authority of law, and in an integrated justice system, where various components' system "use purposes" have been harmonized.

A general pattern of the use of personal information suggests that within the justice system, use is determined by access authorization and by assuming the doctrine of "consistent use." Consistent use means that how the data is used or re-used stems directly from the stated purpose(s) for which the data was collected initially. Where information is not being handled under "consistent use" within an information system or between systems, notification and specific authorization would be warranted.

Outside the criminal justice system, use is increasingly limited as the audience migrates from victims to the public. Public access issues are complex and problematic. Policy guidelines addressing public access issues are being developed and will be provided in a separate document.

It is important to note that there are a growing number of "gatherers" who make a living from uncovering personal information about citizens from government databases. Often referred to as "bulk data," the sale of government databases to the private sector changes data's intended use and accessibility, thus dramatically increasing the likelihood of abuse. In addition, compilations of legal data prepared by the private sector may result in unintended consequences for citizens exercising their right to participate in the judicial system. For example, it is not uncommon for rental or housing associations to develop databases of persons who have filed an unlawful detainer claim. These legal actions are likely to be based on a valid claim by the renter or home owner, i.e., for lack of repair. The information in the database, however, follows an individual forever and may result in denial of housing.

A third area of concern is information sharing between "closed record" states and "open record" states, where the information not available to the public in the closed records state becomes publicly available once it is shared with the open record state. This type of availability has created a market for private information gatherers to use justice system access in one state to provide non-accessible information to parties in their home state.

These types of data gathering have privacy implications that need to be addressed up front in integrated justice systems. Managing the sale and access to justice information may be difficult given the legislative framework in some states. Ideally, the sale of information in bulk should be limited to recognized justice system purposes as enumerated in Principle 1, and contracts for the sale of bulk information should require compliance with privacy principles.

Through a privacy impact assessment, a justice system can be reviewed by the government for the impacts of information-handling practices. Ongoing reviews are necessary as future changes increase the ability to gather and use information and as market forces control these processes.

Technology Design Principle

Privacy policy should drive the design and development of technology, rather than technological capability dictating the formation of privacy policy. We cannot assume that personal information collected for one purpose should be used or shared for an unrelated purpose. Information systems must be designed to halt unauthorized uses of personal information. This involves authorization procedures for access to information, even within the justice system, that in turn involves a protocol for tracking who accesses information and for what purpose. The circumstances of additional use need to be recorded and attached to the record. As well, a record of data linkage needs to be created and attached to the record, allowing for the development of an audit trail and enabling a use assessment.

The technology design also needs to address issues of disclosure. There are occasions were historical data is appropriate for disclosure within the justice system (former aliases, addresses etc.), but perhaps not outside the justice system. The decision rests on whether the most recent data is an "update" or a "correction." This is an area where this technology design principle dovetails with the Data Quality design Principle 3.

Data matching and data mining, where personal identifiers have been stripped from the record, falls outside of this design principle.

5. Security Safeguards Principle

Reasonable security safeguards against risks[23] should protect personal data against loss or unauthorized access, destruction, use, modification or disclosure of data. These safeguards should be provided according to the sensitivity of the information and risks to all involved parties. This principle recognizes that personal information collected by the justice system is highly sensitive and a natural target for compromise. The adage of Robert Morris Sr., former Senior Scientist National Security Agency (NSA) should always be remembered in the design of the security architecture of an integrated justice system: never underestimate the time, expense, and effort someone will expend to break your technology.

An example of risk assessment and the application of security safeguards is federal regulation 28 CFR Part 20, dealing with criminal history information, and 28 CFR Part 23, dealing with law enforcement intelligence systems. These regulations, promulgated in the late 1970's, address specific security procedures for state and local justice information systems and requires the implementation of these procedures on systems that are funded in whole or in part with federal dollars from the Office of Justice Programs. OJP acknowledges the need to update 28 CFR Parts 20 and 23 to correspond to the capabilities of today's information technology. In revising the current regulations, it is important to note that security is an area that will be constantly driven by technology. Although security policy, like privacy policy, should not be based on specific technology, the implementation of security safeguards will necessarily be dependant upon current technological capabilities.

Technology Design Principle

Organizations need to conduct information classification reviews to determine the appropriate level of security to apply, taking into account certain types of personal information, as well as the auspices under which the information was collected. The level of security is dependent on the sensitivity of the information and its value to both authorized and unauthorized parties. As well, methods to record failed attempts to alter information, or attack the system need be set up.

Some of the current methods to maintain security include:

- Public Key Infrastructures
- Data encryption
- Access controls
- Remote access, two-way user authentication
- Log in and password management
- Monitoring records of access to information
- Risk Assessment

6. Openness Principle

There should be a general policy of openness[24] about developments, practices and policies with respect to the management of personal data (apart from the actual data). Openness includes public access to the management practices of the data, except where it directly relates to an investigation, a pending or open case, or involves safety concerns and other factors that a government determines as necessary exemptions. Barring these exceptions, the public should be able to establish the existence and nature of personal data (apart from the actual data), and the main purposes of the data's use, as well as the identity and office of the data controller responsible for that data.

In an investigation or prosecution of an offense, established precedent and evidentiary rules will determine the openness principle or exceptions to it.

The openness principle also requires clear communication to effected individuals where justice records are requested, sold or released to third parties. The public should be informed of when information is sold in bulk for commercial purposes.

This principle is necessary for accountability and to implement the 'purpose for collection' principle.

Technology Design Principle

A justice information technology system is not transparent in its information. It does not easily allow individuals to verify how their information is collected, used or disclosed, nor should the technology need to make its practices and policies open to the public. However, the information technology system must be designed to allow for some method of independent oversight, as the openness principle must be part of the technology for the purpose of accountability.

One way to accomplish the openness principle is through a proxy[25] who provides independent oversight. The system is designed to be transparent to the proxy and authorized system users: showing the types of transactions and linkages within the system, as well as the way in which personal information is collected, used, disclosed and retained. When appropriate, the technology must be able to provide to the proxy a full description of all the circumstances where an organization discloses an individual's personal information to third parties, both within and outside the justice system.

Information systems must be designed to allow all transactions (including, who made changes, when and for what purposes) made on an individual's file to be traced for accountability purposes (addressed in Principle 8). A history of transactions must be retained for audit purposes and to respond to complaints.

7. Individual Participation Principle

Given the unique environment of the justice system an individual, or an agent for an individual or for victims and witnesses, should have the right, except as it would compromise an investigation, case or court proceeding:

a) to obtain confirmation of whether or not the data collector has data relating to him,

b) to have communicated to him, data relating to him/her,

- 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/her;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial;

d) to challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed or amended; and

e) to provide an annotation to data where an organization decides not amend information as requested by an individual, or an agent for an individual or for victims and witnesses.

Technology Design Principle

An information management system must be designed to be able to provide an individual, or an agent for a requesting individual, copies of personal information without disrupting the on-going operation of the justice system.[26] An example of this would be a system's ability to gather, collate, and disclose required pre-trial information or to respond to Freedom of Information Act requests efficiently.

The information management system must be designed to provide efficient access for authorized use and approved releases of information in a form that is readily understandable and at the lowest cost possible to the individual.

An information management system must be able to amend or annotate personal information subject to disagreement over accuracy. The system must also have the capacity to notify third parties who have either provided incorrect information or who have received incorrect information in a timely manner (optimally in real time). Information systems must be designed so that all transactions (including, who made changes, when and for what purposes) made on an individual's record can be traced for accountability purposes (see Principle 8).

8. Accountability Principle

Accountability should be established within each information system to assure the development and compliance with procedures that give effect to the principles stated above. The accountable party (information steward), whether an individual or a body, must preserve the meaning and integrity of the other design principles and assess their effectiveness throughout the operation of the integrated system. Roles and responsibilities of the information steward should be established by the system's key partners at the development stages of an integrated justice information system.

The Accountability Principle is the "due process" mechanism of the eight design principles. An individual or his proxy should be able to challenge the system's compliance with the any one of the privacy design principles through administrative procedures designed, implemented, and enforced by the information steward. The information steward should assure that procedures are in place that guarantee a timely, fair response to inquiries.

Technology Design Principle

To effect the integrity and meaning of all the design principles, there must be a mechanism to ensure accountability within the system. This may be accomplished through a high level body or

individual acting as an "information steward": a designate accountable for the privacy of personal information in the design and development of the justice information technology system.

Accountability practices for which the information steward would be responsible include:

Ensuring all the above privacy design principles have been incorporated in the technology design from the conceptual and contextual stages, through implementation;

Ensuring information systems are capable of providing access to personal information on request and recording who has had access to the personal information and for what purpose;

Ensuring staff managing data are trained on privacy protection requirements as detailed;

Ensuring information systems are transparent and documented, so that individuals or a proxy can be informed about the collection, use and disclosure of their personal information within the context of the principles outlined above;

Establishing regular security and privacy compliance audits commensurate with the risks to the data subject or other individuals with a relationship to the justice system. This would involve using internal auditors, public oversight agencies and external independent auditors.

Ensuring that the above privacy design principles are providing the intended privacy protections through conducting regular privacy impact assessments;

Using the Privacy Design Principles

The Privacy Design Principles are intended to provide a framework for state, local, and tribal governments to use when forming their justice systems' privacy policy and identifying technology requirements. Recognizing and agreeing upon the privacy principles in this document is the first step to incorporating meaningful privacy protections into justice information systems. State, local, and tribal governments should also review and discuss any privacy law or regulation specifically applicable to their jurisdiction. Strategies for actual implementation of the Design Principles and privacy laws are discussed in the forthcoming Justice System Privacy Impact Assessment.

State, local, and tribal governments need to begin by exploring how the Privacy Design Principles can be incorporated into plans for new information systems and enterprise-wide architectures and how they can be applied to existing justice information systems. In beginning these discussions, it may be helpful to consider privacy principles in the context of two audiences:

> **internal**, meaning those agencies that make up the core of the justice system; law enforcement, prosecutors, defense counsel, pre-trial services personnel, judges, court administration, correctional facilities, probation and parole bodies and associated agencies;

external, meaning those players (e.g. charged or convicted offenders, witnesses, victims, public) that could have a relationship with the justice system, but are not an operational part of the system.

Each audience requires an identification of issues that need to be addressed within the Privacy Design Principles. It is important to note that the Privacy Design Principles work under the assumption that any collection of personal information by members of the justice system is warranted, legal and meets the test of reasonableness. For example, trawling[27] personal shopping information through loyalty cards for the purchase of large quantities of zip lock baggies, is reasonable if searching for specific suspected drug traffickers. It is unreasonable if there are no suspects and the trawling is only based on the assumption that any significant purchase of baggies is suspicious, subjecting citizens who blanch large amounts of vegetables to unreasonable invasions of privacy. It is also important to note that when considering the "internal" justice system audience, there is tendency to assume a free flow of all personal information of any one with a 'relationship' to the justice system. However, the application of the Design Principles should be geared to provide only the free flow of information that meets an internal agency's function or system purpose.

The implementation of the Privacy Design Principles through the Justice System Privacy Impact Assessment will require justice system agencies to map data flows within and between systems and to consider how the systems interact with the internal and external audiences. Consideration and discussion of the Design Principles in a broad policy context should be done by all agencies contemplating an integrated justice system before undertaking the details of the impact assessment.

Appendix A

Fair Information Practices

The Fair Information Practices can be summarized as follows:

1. Collection Limitation 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.

2. Data Quality 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 kept up-to-date.

3. Purpose Specification Principle

   The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

   Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 3 except:

   a) with the consent of the data subject; or

   b) by the authority of law.

5. Security Safeguards 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.

6. Openness Principle

   There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of 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.

7. Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, 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.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Appendix B

15 November 1999

DRAFT

INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES

ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Community. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Community to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions (the principles) under its statutory authority to foster, promote, and develop international commerce. The principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the principles must comply with the principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an organization joins a self regulatory privacy program that adheres to the principles, it qualifies for the safe harbor. Organizations may also qualify by developing their own self regulatory privacy policies provided that they conform with the principles. Where in complying with the principles, an organization relies in whole or in part on self regulation, its failure to comply with such self regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts.

Organizations subject to a statutory, regulatory, administrative or other body of law (or body of rules issued by national securities exchanges, registered securities associations, registered clearing agencies, or a Municipal Securities Rule-making Board) that effectively protects personal privacy may assure safe harbor benefits by self-certifying to the Department of Commerce or its nominee. In all instances, safe harbor benefits are assured from the date on which each organization wishing to qualify for the safe harbor self-certifies to the Department of Commerce or its nominee its adherence to the principles in accordance with the guidance set forth in the Frequently Asked Question on Self Certification.

Adherence to these principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations. Organizations may wish for practical or other reasons to apply the principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor. To qualify for the safe harbor, organizations are not obligated to apply these principles to personal information in manually processed filing systems. Organizations wishing to benefit from the safe harbor for receiving such information from the EU must apply the principles to any such information transferred after they enter the "safe harbor."

Organizations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.(1) Personal data and personal information are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure, where the organization is using or disclosing it for a purpose other than that for which it was originally collected or for a purpose which it was processed by the transferring organization. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon as is practicable, but in any event before the organization uses or discloses such information for a purpose other than that specified above.

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties, where such use or disclosure is incompatible with the purpose(s) for which it was originally collected, or subsequently authorized by the individual.(2) Where choice is offered concerning disclosures to third parties not subscribing to the safe harbor principles, not subject to the Directive or another adequacy finding, nor bound by written agreement to provide at least the same level

of protection as required by the principles, this fact must be made clear when individuals are invited to exercise their choice.

For sensitive information, (i.e. personal information specifying(3) medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual) they must be given affirmative or explicit (opt in) choice if the information is to be used for a purpose other than those for which it was originally collected or disclosed to any type of third party other than those already notified to the individual, or used or disclosed in a manner other than as subsequently authorized by the individual through the exercise of opt in choice. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

ONWARD TRANSFER: An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice (because a use is not incompatible with a purpose for which the data was originally collected or which was subsequently authorized by the individual) and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles. If the organization complies with these requirements, it shall not be held responsible when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY: Consistent with the principles, an organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed.

At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

1. Use of the principles in model contracts has not yet been agreed to by the EC.

2. The EC has general concerns about the choice principle because it believes it offers individuals substantially less control of their data in comparison to the situation in Europe. The EC also does not agree with deletion of the crossed out text. In the US view, that sentence goes beyond what is required by the Directive and for this reason should be deleted. The EC does not agree pointing to the Directive's requirement of informed consent. The US has taken the view that if the EC can demonstrate that the prevailing practice in each Member State is reflected by this sentence, we will include the sentence.

3. The EC would prefer for us to use "revealing" rather than "specifying." The USG concern is that revealing is not clear enough, because it allows so much in the way of inference. Given the 10th Circuit's case on the FCC's rules, it may also raise First Amendment issues. US industry has also argued strongly against "revealing."

Notes

1. The criminal justice process includes specialized courts, such as drug courts, juvenile courts, traffic courts, and probation courts, and also interfaces with family courts and probate courts.

2. Alan Greenspan, Remarks at the Conference on Privacy in the Information Age, Salt Lake City, Utah (March 1997) (http://www.federalreserve.gov/boarddocs/speeches/1997/19970307.htm).

3. See John A. Zachman, Enterprise Architecture: The Issue of the Century, (last modified June 1988) www.zifa.com John Zachman has developed a multi-perspective model critical for the successful design and implementation of an enterprise-wide information technology architecture. See Appendix A for a discussion of what is an enterprise technology architecture and the framework needed to manage implementation of an enterprise-wide technology.

4. See Niel Postman, Technopoly, (Vintage Books, New York, 1992) (explaining unintended effects of technologies).

5. http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM see Appendix A for full description.

6. For a more detailed description of the EU directives: <http://europa.eu.int/comm/dg15/en/media/dataprot/news/925.htm>

7.

8. Paul F. Kendall, Neal J. Swartz, Anne E. Gardner, Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: the Need for Principles of Responsible Use, 2ist Annual International Conference on Data Protection and Information Privacy, Hong Kong (Sept. 1999). The authors identify three types of adult related information: criminal history information, criminal intelligence information, and "'Supplemental Information:' A New Type of Information'."

9. See Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 1968 U.S.C.C.A.N. 237, as amended. See also 28 C.F.R. ' 23.1 (1999) (the Office of Justice Programs is authorized to promulgate policy standards to assure that criminal intelligence services funded by the Omnibus Crime Control and Safe Streets Act "are not utilized in violation of the privacy and constitutional rights of individuals.").

10. This paper includes a matrix that can be used to undertake the detailed analysis required for an integrated justice system technology project.

11. "Enterprise architecture" refers to the specifications of an information technology that spans multiple organizations and allows those organizations to share and use information in a seamless and transparent way: i.e., no "stove pipe" technologies.

12. The purposes for the criminal justice system are well established. They include: law enforcement, criminal investigation, public protection, and the justice process. For this principle, these purposes need to be specified to ensure that the resultant technology design fosters adherence to the principle.

13. The purpose statements should determine the technology specification.

14. A compatible purpose is one that matches or is in harmony with the original stated purpose. The underlying logic in this thought is that the re-use of personal information is restricted to original stated purposes or similar purpose statements that are required prior to re-use of data. This will be critical in situations where third parties wish to access or purchase justice information. This will also be critical to manage data use. For example, the privacy design principles need to address third parties' (ranging from strictly private sector to quasi-justice system) access and use of information. For example, third parties wishing to scan justice information to look for potential drug rehabilitation customers, or Equifax wishing to access court data. Use of the purpose principle is a way to have third parties contractually bound to how they can use the data.

15. An example of a purpose statement for a law enforcement body would be: The state police collect personal information in the pursuit of suspected offenders, for public safety and to bring offenders to trial.

16. Determining limits is a difficult task in the justice system. A test of necessity, i.e., what is necessary to collect, would need to be developed by state and local justice systems. This would involve stating and assessing 'why' a component of the justice system would need to collect i.e., 'know' that information.

17. Consent from victims prior to data collection needs to be addressed.

18. State and local justice systems need to define 'case' under various components of the justice system, i.e., probation case, corrections case.

19. Reliability of information is a key priority that needs to be designed into an integrated justice technology system. For example, raw investigative information, could be fraught with inaccuracies until verified or cross checked with other data.

20. This does not eliminate the need for case comments, or text boxes, as they are needed, e.g., for probation. However, free flowing text needs to be restricted as much as possible.

21. Court transcripts pose a challenge, as they can't be corrected. This could mean they should not be disclosed broadly.

22. However, use limitation also includes access limitation and levels of authority to access certain types of information within the justice system. Part of this can be developed using the need to know principle. Other parts can be developed through access and security protocols. For example, distinctions should be made for certain types of information (pre and post guilty information), who has access to that information, as well the types of access (e.g., read only).

23. Risk assessment is an integral part of this process. It needs to identify all the potential data users as well as intruders. It also need to include disaster recovery strategies.

24. Openness includes both the accessability to the data as well as transparency regarding the policies and procedures

25. A proxy function may be introduced in applying the privacy design principles to allow for the necessary accountability for an information technology system comprised of personal information, while taking into account that investigation and court proceedings could be compromised if an individual had access to their information. The nature of a proxy should be a point of discussion at the federal, state, local, and tribal levels. An option for a proxy is: a point of system-wide accountability and advocacy, with audit functions, to ensure the privacy design principles are functioning as intended and personal information is not being misused. In small jurisdictions, the proxy function may be provided by the state, or in a reciprocal arrangement with a neighboring jurisdiction. In any case, the proxy role needs to be developed by jurisdictions implementing automated justice systems. It should be noted that a proxy in this context is distinct from an agent who acts on behalf of an individual.

26. Decisions on release or non-release of personal information must be established in a protocol that is in accord with the openness principle.

27. Trawling is used here to describe the process of casting a wide net in the waters of information with the broad intent to catch 'something'.

Information and Privacy Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca