Washington TECHNOLOGY

Governors want new safeguards for criminal justice data

04/17/06
By Ethan Butterfield,

With technology rapidly outpacing policy, major improvements are needed at the state level to better protect sensitive criminal and civil justice information, according to a brief released today by the National Governors Association's Center for Best Practices.

The speed at which new justice information systems allow data to be shared, sold and analyzed has led to improved communications and awareness, according to the brief, "Protecting Privacy in Integrated Justice Systems."

But these new systems also have unintended consequences. For one, they can violate privacy protections by inadvertently revealing the identity of victims, witnesses, law enforcement and court personnel.

While justice records always have been public information to some degree, they also are big business, as such data is now a source of revenue for states. Last year, the sale of one state's driver's license records brought in between $30 million and $40 million, according to the brief.

There are roughly 227 million registered drivers in the United States, and states sell each record for 50 cents to $6, according to the brief. States also sell criminal history and tax records.

Illinois, Minnesota and Wisconsin are looking at ways to protect sensitive data. States can improve privacy protection by:

- Establishing a collaborative process to develop privacy policies for justice information sharing initiatives
- Identifying areas where justice information sharing initiatives put individuals' privacy protections at risk
- Conducting legal analyses of privacy laws and regulations that impact justice information sharing systems
- Defining statewide privacy principles to govern the operation of justice information sharing initiatives
- Developing privacy policies that protect information in different contextual settings
- Enforcing accountability and setting minimum security statewide standards for justice information sharing initiatives.

Contact: Thomas MacLellan, Policy Analyst
Social, Economic, and Workforce Programs
202/624-5427
April 12, 2006

Protecting Privacy in Integrated Justice Systems

Executive Summary

Major improvements in justice information sharing now allow criminal and civil justice records to be shared, synthesized, sold, and analyzed at speeds and with an ease not previously imagined. Unfortunately, in addition to many public safety benefits, these improvements can have unintended consequences as the sharing of information concerning victims, witnesses, law enforcement, court, and other justice personnel potentially exposes them to harm by violating privacy protections. States need now to address growing questions and concerns as the "practical obscurity" that served as the *de facto* privacy protection in a paper-based justice system has all but vanished in the face of statewide justice information sharing initiatives.

The full implications of improved justice information sharing are not yet known. The challenge is that state privacy policies have not kept pace with technological advances. The state laws, practices, and rules and regulations designed to protect privacy were mostly put in place when justice records and information were paper-based, housed in separate agencies and organizations, and not searchable electronically. The advent of justice information sharing, however, is testing the adequacy of these privacy policies. While many of these issues are not new, what are new are the large-scale implications; never before has so much justice information been immediately available at the touch of a button.

By taking a leadership role on this emerging issue, governors can continue to realize the public safety gains of improved justice information sharing while protecting the privacy and safety of individuals and avoiding costly lawsuits. States such as Illinois, Minnesota, and Wisconsin, as well as several national initiatives, have begun systematically to look for ways to protect the privacy of sensitive and personal information. These initiatives provide valuable lessons for other states looking to improve the privacy practices of their justice information sharing initiatives. Based on these lessons, recommendations for improving privacy protections include:

- Establishing a collaborative process to develop privacy policies for justice information sharing initiatives;
- Identifying areas where justice information sharing initiatives put individuals' privacy protections at risk;
- Conducting legal analyses of privacy laws and regulations that impact justice information sharing systems;
- Defining statewide privacy principles to govern the operation of justice information sharing initiatives;

- Developing privacy policies that protect information in different contextual settings; and
- Enforcing accountability and setting minimum security statewide standards for justice information sharing initiatives.

This *Issue Brief*, made possible through a grant from the U.S. Department of Justice Office of Justice Programs (OJP) Bureau of Justice Assistance (BJA), explores these issues and recommends strategies that governors and other state policymakers can employ to improve privacy protections within state justice information sharing initiatives. It also includes a number of resources to which states can turn for more in-depth information.

How Justice Information Sharing Has Changed the Privacy Landscape

Technological advances and policy innovations are allowing states to aggregate civil and justice information nearly seamlessly. Because of these improvements, new policy issues have begun to emerge that are distinct from more traditional privacy policies. Specifically, how do states develop privacy protections for information that when viewed in isolation is not personally identifiable but when integrated and shared across systems, as is done through states' justice information sharing initiatives, becomes personally identifiable?

Improving how justice information is shared has been a priority for states over much of the last decade, even more so since 9/11. As a result, states have dramatically improved the accessibility of justice information by law enforcement personnel, prosecutors, corrections officials, and courts. But as states have made these improvements, concerns about individual rights to privacy have begun to emerge. At the heart of these concerns is the question of whether the information now assembled through integrated justice information systems is fundamentally different than its formerly disparate parts. As noted in the Supreme Court decision *U.S. Department of Justice v. Reporters Committee*: "The issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interests implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[1]

Justice records have always been, at some stage in the process, public information, but an individual or business seeking to obtain a complete account of an incident from arrest to adjudication to corrections would need to physically go to a courthouse, police station, or public records repository. Now, individuals, private businesses, and other organizations can electronically access that same information instantly and remotely either directly from a state portal or through a private data firm. In fact, these types of exchanges are becoming major revenue streams for states. For example, last year the sale of a particular state's driver's license records brought in between $30 to $40 million. Considering that there are approximately 227 million registered drivers in the United States and states sell these records anywhere from 50¢ to $6 each, the revenue benefits are significant. When factoring in the sale of other records, such as, criminal history records and tax records, the revenue implications become even greater.

Privacy Protections in Integrated Justice Systems

The protections being discussed in this brief relate to privacy in the context of justice information sharing. The distinction being made here is that, as noted above in *Reporters*, the integrated information that results from state justice information sharing initiatives is different than its component parts and requires enhanced privacy protections. For the purposes of this brief, privacy refers to information that should otherwise not be released and has the potential for causing harm to an individual.

Privacy policies are expressions of public values and typically are built upon a foundation of guiding principles. One of the more widely recognized sets of such principles is the Fair Information Practices (FIPs). Although originally from European policies related to the commercial and transborder exchange of information, the FIPs "provide a straightforward description of the underlying principles and a simple framework for the legal analysis that needs to be done with regard to privacy in integrated systems."[2] The FIPs articulate standards related to the collection and exchange of personal information that policymakers can use to assess and benchmark the development of privacy policies for integrated justice initiatives.

While the Fair Information Practices are not privacy policies per se, they articulate the values that undergird many current privacy policies. The FIPs incorporate the following eight principles:

1. ***Purpose Specification Principle.*** Identify the purposes for which all personal information is collected and keep subsequent use of the information in conformance with such purposes.
2. ***Collection Limitation Principle.*** Review how personal information is collected to ensure it is collected lawfully and with appropriate authority; guard against the unnecessary, illegal, or unauthorized compilation of personal information.
3. ***Data Quality Principle.*** Implement safeguards to ensure information is accurate, complete, and current, and provide methods to correct information discovered to be deficient or erroneous.
4. **U*se Limitation Principle.*** Limit use and disclosure of information to the purposes stated in the purpose specification and implement realistic and workable information retention obligations.
5. ***Security Safeguards Principle.*** Assess the risk of loss or unauthorized access to information systems and ensure ongoing use conforms to use limitations.
6. ***Openness Principle.*** Provide reasonable notice about how information is collected, maintained, and disseminated and describe how the public can access information as allowed by law or policy.
7. ***Individual Participation Principle.*** Allow affected individuals access to information related to them in a manner consistent with the agency mission and when such access would otherwise not compromise an investigation, case, court proceeding, or agency purpose and mission.
8. ***Accountability Principle.*** Have a formal means of oversight to ensure the privacy and information quality policies and the design principles contained therein are being honored by agency personnel.

States face new privacy concerns in other areas that are expanding the role of information technology, such as the sharing of health information and education records. While these areas are governed by various controlling pieces of federal legislation, in particular the Health Insurance Portability and Accountability Act (HIPAA) and The Family Educational Rights and Privacy Act (FERPA), similar protections for justice information do not exist yet. This gap presents both a challenge and an opportunity for policymakers.

Who and What is At Risk?

The risks to individuals' privacy and safety begin when personal information of any kind is entered into justice information systems. In general, the privacy risks associated with justice information sharing can be broken down into the following categories:

- Risks to innocent individuals in contact with the justice system;
- Risks to individuals because of wrong or incomplete information;
- Risks to individuals because of illicit insider use of information;
- Risks to individuals because of identity theft;
- Risks to individuals because of access to juvenile records; and
- Risks to individuals regarding sealed or expunged records.

Risks to innocent individuals in contact with the justice system. Information about victims, witnesses, children, informants, jurors, and court and law enforcement personnel is now available as never before, potentially exposing them to harm. For example, given advanced data aggregation and search capabilities, it is now possible for an individual with criminal intent to search court and law enforcement records and identify an unnamed victim or witness in a case. While the court record may not explicitly provide personally identifiable information, that same record may provide adequate information that, in conjunction with additional data sources, would make it possible to identify a victim or witness.

"Personally identifiable information is one or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is sufficient to specify a unique individual."[3] It is important to emphasize that these separate data elements may be widely distributed across components of states' justice information systems. In isolation, they may not be meaningful. However, the recent improvements in justice information sharing now allow this information to be combined across multiple criminal and non-criminal justice information systems. For example, a court record may only contain name and age, but a corresponding police record may also include a driver's license number and ethnicity. By integrating these random pieces of information it would be possible for a criminal to track down and intimidate a witness or victim.

Risks to individuals because of wrong or incomplete information. Another risk is that information in a court or police record may be inaccurate, incomplete, or erroneously merged with that of another individual. For example, if police arrest a John *H.* Doe for a sex offense but incorrectly enter the information as John *N.* Doe, it is possible that an innocent John N. Doe could lose his job or suffer other harms as a result of this wrong information. This is similar to what happened in 2005 when a Florida couple feared for their safety after their address was wrongly featured "hundreds of times" on a government television station as a sex offender's home.[4]

Another more tragic example occurred in "Texas where four men severely beat a 27-year-old mentally retarded man whose address, a group home for the disabled, was mistakenly listed on Texas's Internet registry as the residence of a child molester."[5]

Incidents such as these, as well as those related to incomplete information, raise significant questions of liability. These concerns are made even greater with the advent of high-profile commercial and government programs that link information from states' sex offender registries into a single portal. Compounding these challenges are the varying state statutes that set the parameters for inclusion in registries. While these programs serve as a central access point for state registries, states set the thresholds for including certain categories of crime. Some of these sites advise visitors that publicly-accessible Internet sites established by different states may "not be comparable with respect to the comprehensiveness of offender-related information that is made available for public disclosure. For example, a given state may limit public disclosure over its Web site of information concerning offenders who have been determined to be high-risk, while another state may provide for wider disclosure of offender information but make no representation as to risk level of specific offenders."[6] In other words, the public has no way of knowing whether individuals included in state registries are at a very low or very high risk of reoffending.

The issue of wrong or incomplete information also raises questions related to the sale of justice information. For example, if a state sells inaccurate or incomplete justice information about an individual to a data mining or data aggregation company, how is that information corrected, especially since it is now outside the direct control of a state? Who is liable if an individual is hurt because of wrong or incomplete information shared though a state justice information system? According to the U.S. Department of Justice, this is what happened in the case of an Ohio man whose social security number was mistakenly associated with a criminal. By the time the error was corrected within law enforcement information systems, the data already had been sold to private data companies and distributed nationally. Because it was impossible to correct the information in these private databases in a timely fashion, this individual lost his job and home.[7]

Risks to individuals because of illicit insider use of information. Another risk is associated with those in the justice enterprise who have access to public and non-public records. For example, what safeguards are in place to keep a police officer or a court clerk who may be involved in a domestic violence dispute from illegally accessing information regarding the whereabouts of his or her victim? This is what happened in December 2002 "when former U.S. Drug Enforcement Administration agent Emilio Calatayud was sentenced to prison and fined on charges related to his use of protected law enforcement computer systems and databases. He obtained information from these protected systems, which he then provided to a Los Angeles private investigation firm in return for at least $22,500 in secret payments."[8]

The U.S. Secret Service recognizes many of these same concerns in their *Insider Threat Study.* They write, "The nation's dependence on interconnected networks and communications systems significantly increases the risk of harm that could result from the activities of insiders. In addition, the actions of a single insider can cause extensive financial damage or irreparable damage to an organization's data, systems, business operations, or reputation."[9]

Risks to individuals because of identity theft. Another growing threat facing states is the issue of identity theft. Court and police records often contain vast amounts of information criminals could troll through to perpetrate identity theft. For example, a public court record for a divorce

proceeding may contain information such as addresses, dates of birth, credit information, social security numbers, and spouses and children's information. Criminals could gain access to this information through legitimate channels by purchasing it in bulk or accessing it via the Internet. They could then use this information to apply illegally for credit cards or loans. This could all be performed outside the United States, for example, by the Russian mafia that has become particularly active in recent years in identity theft.

Given how widely accessible justice information has become in recent years, states need to consider how they protect personal information—including individual elements of information—if they are to protect individuals from identity theft.

Risks to individuals because of access to juvenile records. In the past, states have taken great measures to protect information related to juveniles and minors in the justice system. However, improvements in information sharing are quickly eroding these protections. For example, in Iowa, court records, regardless of final disposition (i.e., guilty or not guilty verdicts), are available for free and for purchase on the Internet for all cases involving individuals 10 years or older. In other words, the records of a 14-year-old child who was charged but not convicted of stealing a car are still available to a potential employer who may, based on the charge alone and not the disposition, opt not to hire that individual later in life. While such information may have always been available to potential employers, the advances in information sharing now make searching and accessing this information nearly effortless. In fact, for many businesses, extensive background checks are now considered normal business practices even for entry-level jobs.

It should be noted here some states have in place protections against the use of court and arrest information that did not result in convictions when making employment decisions. However, given the wide availability of information, enforcing these statutes and proving discrimination can be difficult.

Risks to individuals regarding sealed or expunged records. If an individual is charged with a crime he or she did not commit and is found not guilty, he or she may request the criminal record be expunged so they will not suffer adverse consequences, such as loss of social status, loss of employment, or denial of a loan. However, given how information is shared across agencies, sold to data aggregators, or placed on the Internet, expunging criminal records may no longer be feasible. In the past, expunging records involved the physical destruction of files and notes. Now that these same records are electronic and move across the world at the speed of light, how can states protect innocent individuals? In fact, what does it now mean to "expunge" a record?

Similarly, individuals who were rightfully convicted of a crime and may have served their time and have gone years without being charged or convicted of subsequent crimes may seek to have a record sealed. For example, an individual convicted in their late teens for a simple drug possession charge may, at age 30, wish to seal that record to improve their job prospects. The question now becomes, how do states seal records, especially since information may be in various public and private repositories? If a criminal record can be used—rightly or wrongly—to discriminate against an individual applying for a job, housing, or other services, it raises some fundamental questions related to the nation's justice system. For example, did policymakers intend for former offenders to be exposed to such potentially damaging collateral consequences years after they served their time or made retribution?

Challenges to Protecting Privacy in Integrated Systems

There is little debate that improved justice information sharing has resulted in significant improvements in public safety. As these improvements have occurred, there also has been a corresponding growth in expectations and demand for public services such as instant comprehensive up-to-the-minute background checks. This is sometimes referred to as the "CSI effect."[10] This growth in expectations and demand presents a challenge for policymakers looking to improve privacy safeguards. Nowhere else is that challenge more evident than in homeland security where policymakers are struggling to balance the often competing interests of personal privacy and national security.

In addition to balancing privacy and public safety, other challenges make developing effective privacy policies for state justice information sharing initiatives difficult. These include the following:

- ***Protecting access to data.*** States need to be concerned with the security of their information systems, especially as access to one node on a state information network, for example in a rural sheriff's office, potentially provides access to all the information contained within a state's justice information system. There are two primary concerns related to security that states need to consider, including access and technical safety (e.g., firewalls and other security measures). For example, states need to be concerned with how information is stored and who is accessing information and for what purpose. If a state's aim is to protect privacy, they need to ensure appropriate safeguards, in terms of access and storage of information, are in place and enforced statewide. Without effective security, privacy protections are difficult, if not impossible, to enforce.
- ***Implementing and monitoring privacy policies in distributed systems.*** Another challenge is the distributed nature of justice information systems and the multiple privacy policies in place in different agencies. This becomes even more difficult when justice information is shared across states and with the federal government. Most state justice information sharing systems are not repositories in the traditional sense. Rather, these systems are designed to reach out and access information from multiple sources. Each participating agency or entity sets the standards and guidelines for the type of information it is willing to release. However, various state agencies and the federal government sometimes are willing to share information that one of their counterparts is not willing to share. For example, as was noted in a recent forum hosted by NGA, federal law enforcement will share background information a particular state is prohibited by law from sharing. As a result, a requesting business, agency, or individual may be told by a state an individual has no criminal record while information received on the same individual from a federal law enforcement agency may show otherwise. The irony here is most information contained within federal systems is provided by states. In other words, while a state may be prohibited from sharing certain information with the public, the same information can be accessed publicly through a federal system.
- ***Ensuring privacy protections in different and changing contextual settings.*** In addition to the difficulties raised by the distributed nature of justice information systems, the privacy sensitivity of information often depends on the context and

timing of that information. Some information may be private in one context and at a particular point in time, but not private in another context and at another time. For example, a court record may be open until a defendant is found not guilty and the records ordered expunged. Privacy policies will need to take into account this changing context of information.

- ***Protecting the privacy of information that has moved beyond the direct control of a state.*** A final challenge is the question of how states can protect the privacy of information that has moved beyond their control, especially given the growth in sale and exchange of information. For example, how do states protect information from being used beyond its original purpose? How do states correct inaccurate information given how freely that information now moves across public and private systems? Can states compel private data aggregation firms to correct erroneous information or remove sealed or expunged records? How do states control information that has moved outside the borders of the United States?

Recommendations to Improve Privacy in Integrated Justice Systems

States are just beginning to address the privacy concerns created by the recent improvements in justice information sharing. Governors' leadership in raising the visibility of these issues is essential. According to the BJA's *Privavcy and Information Quality Policy Development for the Justice Decision Maker*, "failure to develop, implement, and maintain dynamic privacy and information quality policies can result in harm to individuals, public criticism, lawsuits and liability, inconsistent actions within agencies, (and) proliferation of agency databases with inaccurate data."[11]

Three states in particular—Illinois, Minnesota, and Wisconsin—have taken steps toward developing more effective and comprehensive privacy policies that address some of the privacy risks and challenges associated with justice information sharing. In addition, BJA's Global Privacy and Information Quality Workgroup (GPIQW) and the National Criminal Justice Association (NCJA) have produced guides and other publications designed to assist policymakers in these areas. (More information on these are available in the *Resources* section of this brief.) While early in their efforts, several lessons and strategies have emerged that provide actions governors can take. These include the following recommendations.

Establish a collaborative process to develop privacy policies for justice information sharing initiatives. Given the distributed nature of justice information sharing, states such as Illinois and Wisconsin have tasked particular groups with the primary responsibility for leading the work on privacy. Wisconsin formed a privacy workgroup that led an 18-month study and presented its initial findings in January 2005 to the state's justice information sharing governance body.

In Illinois, this responsibility is housed in the Illinois Criminal Justice Information Authority (ICJIA). In 2003, Illinois Governor Rod Blagojevich signed an Executive Order creating the Integrated Justice Information System (IIJIS) Implementation Board within the ICJIA. The executive order recognized that "in light of the need to share critical subject information for protecting citizens from a terrorist attack and ensuring public safety, Illinois government officials must safeguard individual privacy interests and prevent unauthorized disclosures of information." The executive order creates a 23-member board comprised of individuals from across the state's

justice system (e.g., attorney general, corrections, courts, law enforcement, etc.). It is the responsibility of the IIJIS Implementation Board to "promulgate policies that protect individuals' privacy rights related to the sharing of justice information."[12]

Using the executive order as a springboard, the IIJIS has launched one of the first and most comprehensive efforts in the country to address the privacy concerns related to integrated justice information. Even though the work of the IIJIS is not complete, many of the processes described here and elsewhere build on that work.

Identify areas where a state's justice information sharing initiative potentially puts individuals at risk. Essential to improving privacy protections is identifying the areas where a state's justice information sharing initiative places individuals at risk. Similarly, states need to identify the areas where they might be liable for damages as a result of how justice information is shared. For example, do open records make it more likely that a domestic violence victim will be revictimized by an abuser? Or that a witness will be intimidated? What happens when wrong or poor quality information is shared and an individual (or address) is wrongfully included on a list of sex offenders?

One way states can prospectively identify risk is to compel agencies that collect and exchange information to conduct privacy impact assessments (PIAs). "The privacy impact assessment is a process used to evaluate privacy in information systems. The process is designed to guide system owners and developers in assessing privacy through the early stages of development. The process consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by the Privacy Advocate."[13]

The PIA process is utilized in a number other areas and could be useful to states in assessing their justice information sharing initiatives.

Conduct legal analyses of current laws and regulations. States already have in place a variety of privacy policies embedded in law, practice, and rules and regulation. The challenge is in parsing out and understanding how these specific privacy polices affect the sharing of justice information. Initially, the goal of the Illinois IIJIS Implementation Board was to develop a comprehensive privacy policy to govern all aspects related to justice information sharing. What became clear to them, immediately, however, was the number of requirements to which they were already subject.

In response, Illinois embarked on an effort to develop an understanding of their current privacy practices. To do this, the IIJIS Implementation Board constructed a matrix that included all the state, local, and federal privacy policies to which they were subject given their justice information sharing schema. This matrix sets forth all the state and federal policy choices surrounding the collection, use, and sharing of criminal history record information. It was created to help understand not only what current privacy decisions have already been made, but also why and where those decisions were made. This was done because understanding the rationale for a privacy policy helps agencies implement it and also can provide guidance to policymakers as to whether the decision should be applied in other contexts. Additionally, knowing where a decision was made can influence the amount of deference granted to it and identify where proposals to change those decisions should be directed.

While the information contained within the matrix was specific to Illinois, other states have the opportunity to take and build on this framework in assessing their own extant legal requirements. (More information on the ICJIA is included in the *Resources* section of this brief.).

Define statewide privacy principles to govern the operation of justice information sharing initiatives. Establishing a core set of privacy principles will be useful in assessing and advancing a comprehensive unified approach as states develop privacy policies to govern their justice information sharing initiatives. For example, guiding the work of the Illinois Integrated Justice Information Systems Implementation Board has been the Fair Information Practices (FIPs). Using the FIPs as a benchmark, Illinois is assessing the privacy protections of their justice information sharing initiative against the eight FIP principles. The resulting information has helped to guide their privacy policy development process.

The Privacy Policy Development Guide, produced by the U.S. Department of Justice Global Justice information sharing Initiative, builds upon the work of the ICJIA and structures a process by which states can use the FIPs to assess their privacy protections. For example, on the issue of limitations of information use, the guide states: "One of the main purposes of gathering information is to share it with others in the justice system so that the system better accomplishes its mission. However, there must be limits on the sharing of information, both as to with whom and under what circumstances it may be shared. The FIPs Use Limitation Principle asserts that the information gathered should be shared or used only for the purpose for which it was gathered. This is the key to protecting individual privacy."

The Privacy Policy Development Guide provides questions based on each of the FIP principles states can use to direct the development of a privacy policy. For example, Figure 1 presents a series of questions that correspond to the Use Limitation Principle. State policymakers can use questions such as these to frame their approach to privacy policy development. The *Guide* includes similar sets of questions across each of the FIPs state policymakers can use to assess the privacy protections of their justice information sharing initiatives.

Figure 1: Questions related to the Fair Information Practices Use Limitation Principle.

- Are there legal provisions regarding sharing of information? With whom can information be shared or not shared?
- What do the state constitution, statutes, and case law, interpreting the provisions, say about openness of agency records and the extent of public access to the information?
- Is there a law enforcement exception to this public access? If so, how broad is it? To what classes of information does the exception apply?
- What exceptions exist for specific types of information (for example, arrests or convictions)?
- What legal exceptions are there regarding specific uses of information? Are there legal provisions with regard to providing information for background checks, preemployment checks, or other noncriminal justice uses? Has certain information been received that is subject to restrictions concerning further dissemination?
- Are the public access rules for court records more open than for other agencies? When do these rules begin to apply? When is information from other justice system entities introduced into the court record in a case?
- Are there provisions allowing selling of information to information brokers or third parties? Are there specific categories or types of information for which such bulk transfer of information is permitted or prohibited? Can downstream or third-party use of the information given to information brokers be controlled?
- What are the requirements for uniquely identifying an individual who seeks access to the information maintained by the agency, that is, what are the means of authenticating users? What are the means of keeping an historical record of the persons or entities with whom information has been shared?"[1]

Source: U.S. Department of Justice, Bureau of Justice Assistance, *Privacy Policy Development Guide*, (Washington, DC: 2006) 7.2.4.1.3.

Develop privacy policies that protect information in different contextual settings. The privacy sensitivity of information often varies greatly depending on the context of that information. Information may be protected in one setting or context and be free to be shared without restriction in another. As states develop privacy policies to support justice information sharing initiatives, they need to include provisions that account for these changing sensitivities. For these policies to be effective, they may need to be attached to and follow specific data elements across state and federal systems, as well as to information purchasers.

If information from an agency with very restrictive privacy polices is shared with another agency with less restrictive privacy policies, the privacy policies of the agency sharing information need to remain in control of that information. For example, if a law enforcement agency shares sensitive and confidential information about a victim or witness with a court, a state's privacy policy should take into account these restrictions and ensure the privacy protections remain intact even as information moves beyond the boundaries of that agency.

Currently, however, these types of protections are not a generally accepted practice. But with such privacy protections in place, an individual, private business, or agency would not be able to access information from a secondary source that they could not otherwise receive directly from an agency collecting or producing that information. Similarly, if a state sells information to a private data firm, for example a court or criminal record, and that information is later ordered sealed or expunged, state privacy policies need to extend to that information even though it is now beyond the court's direct control.

Enforce accountability and set minimum security standards. States need to develop and enforce sanctions for violations of privacy and security policies about collection, use, and dissemination of information about individuals. At a minimum, states need to compel participating agencies to maintain and regularly monitor audit trails of who is accessing information and for what purpose.

Similarly, states need to promulgate minimum security practices for all consumers of and contributors to justice information sharing initiatives. According to Office of Justice Program's Global Security Working Group (GSWG), "security of the entire information exchange enterprise is only as strong as the weakest link…Of particular importance is determining effective security standards for legacy networks/systems, as well as the new and enhanced networks and systems to which they are joined."[14]

The GSWG's mission is "to enable the trusted sharing of justice information by recommending best practices for security guidelines, technologies, and procedures." The GSWG has developed a potentially useful resource, *Applying Security Practices to Justice Information Sharing*, for educating justice executives and managers on basic security practices. It includes background information, overviews of best practices, guidelines for secure information sharing, and 15 identified security disciplines.[15]

By promoting security and access standards, such as audit trails, changing passwords regularly, limiting access to sensitive information to authorized individuals, and requiring up-to-date firewalls, states can help to ensure private information is less likely to be stolen, accessed inappropriately, or shared inadvertently.

Conclusion

The advent of justice information sharing, wide access to the Internet, the growth in professional data miners and aggregators, and sophisticated searchable technologies are testing the limits of states' privacy policies as information is being used in ways previously not envisioned. It is a case of technology being farther ahead than policy.

By raising the prominence of these issues and posing difficult questions to their justice executives, governors can help to ensure the public safety gains made through justice information sharing continue. It is and will continue to be a delicate balance between public safety and personal privacy However, there is general agreement in the field that concerns about privacy protections within justice information sharing initiatives are going to continue to proliferate. If not at the forefront of these efforts, states run the risk of having to react to challenges as opposed to leading change and promoting improvements.

Resources

Highlighted below are resources that governors and other policymakers can turn to for additional information and assistance in addressing the privacy issues associated with justice information sharing initiatives.

Compendium of State Privacy, and Security Legislation: 2002 Overview. This compendium compiled for the Bureau of Justice Statistics by SEARCH, the National Consortium for Justice Information and Statistics Bureau of Justice Statistics is the twelfth in a series of reports referencing and analyzing state laws, administrative regulations and attorneys general's opinions relating to the security, confidentiality, accuracy, and completeness of criminal history records.

Global Privacy and Information Quality Working Group (GPIQWG). The work of the GPIQWG is designed "to assist government agencies, institutions, and other justice entities in ensuring that personal information is appropriately collected, used, and disseminated within integrated justice information systems." Of particular interest are two resources developed by the working group:

- ***Privacy and Information Quality Policy Development for the Justice Decision Maker*** is a high-level publication aimed at justice executives and other policymakers. It identifies the issues and challenges the policymakers needs to address. To access this publication go to: https://it.ojp.gov/documents/200411_global_privacy_document.pdf.
- ***Privacy Policy Development Guide*** is geared toward the justice practitioner charged with developing or revising an agency's privacy policy and is a practical, hands-on resource that provides guidance on the process for developing a privacy policy. To access this publication go to: https://it.ojp.gov/documents/Privacy_Guide_Final.pdf.

Global Security Working Group (GSWG). "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 methodology will be to provide a security architecture and framework that meets the requirements of the justice community for trusted information sharing." A product of the GSWG is ***Applying Security Practices to Justice information sharing*** **CD, Version 2.0**, which was developed to educate justice executives and managers on good, basic, foundational security practices. It includes background information, overviews of best practices, guidelines for secure information sharing, and fifteen identified security disciplines.

The GPIQWG and the GSWG are standing committees 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 initiatives. Global was created to support the broad scale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment."[16] For more information on Global and to access these guides, go to: http://it.ojp.gov/topic.jsp?topic_id=8.

For more information on federal justice information technology projects visit: http://it.ojp.gov/index.jsp.

Illinois Criminal Justice Information Authority. Information on the Illinois Criminal Justice Information Authority (ICJIA) can be found at: http://www.icjia.org/public/index.cfm. In

addition, a case study of Illinois' efforts to develop a privacy policy can be found in Appendix B of the GPIQWG's ***Privacy Policy Development Guide.***

A useful document that highlights the work of the ICJIA is ***Privacy Schmrivacy? Drafting Privacy Policy in an Integrated Justice Environment (and why it's important).*** This guide helps to establish the case for drafting privacy guideline and proposes some suggested steps states can adopt. This report was produced by ICJIA and is available at: www.icjia.state.il.us/iijis/public/pdf/PRV/PrivacySchmrivacy_FINAL.pdf.

For more information on the ICJIA's matrix visit:
http://www.icjia.state.il.us/iijis/public/index.cfm?metasection=tools&metapage=privacyFront
http://www.icjia.state.il.us/iijis/public/excel/CHRI_policies6th.xls

Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems. The Guideline was produced by the National Criminal Justice Association (NCJA) through a national and international collaboration of nearly 100 state, local and tribal justice leaders, as well as academia, elected officials, the media and the commercial sector. This publication is designed to provide assistance to policymakers and practitioners who "seek to balance public safety, public access, and privacy when developing privacy policies for their agencies' systems, whether already operating or being planned and whether independent of or integrated with those of other agencies." The Guideline provides specific direction on how to employ collection and use practices and discusses a number of other privacy issues, including determining the sensitivity or public accessibility of certain data. The report is available at: http://www.ncja.org/pdf/privacyguideline.pdf.

For more information on the NGA Center for Best Practices work on justice information sharing initiatives visit: www.nga.org/cener/jit.

End Notes

[1] U.S. Supreme Court, *United States Department of Justice et al. V. Reporter Committee for Freedom of the Press et al.* (1989), 489 U.S. 749, No. 87-1379.

[2] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Privacy Policy Development Guide*, (Washington, DC: 2005) p. 7-11.

[3] Ibid C-9.

[4] "Couple's Address Wrongly Broadcast as Sex Offender's Home." *WFTV.com* [online] <http://www.wftv.com> [cited June 6, 2005].

[5] Alan Gustafson, "Neighbors, Part 3: Residents resort to violence," *Statesman Journal* [online] <http://news.statesmanjournal.com/article.cfm?i=19416> [cited February 5, 2001].

[6] U.S. Department of Justice, *National Sex Offender Public Registry* [online] Washington, DC: U.S. Department of Justice. Available at: <http://www.nsopr.gov/>.

[7] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Privacy and Information Quality Policy Development for the Justice Decision Maker*, (Washington, DC: 2005) p. 4.

[8] Ibid p. 4.

[9] United States Secret Service, "Executive Summary," *Insider Threat Study* [online] Washington, DC: U.S. Secret Service. Available at: <http://www.treas.gov/usss/ntac_its.shtml> p. 1.

[10] The "CSI effect" refers to a popular television show that fictionally portrays investigatory technologies. One result of such dramatizations is a public expectation that law enforcement forensics are more advanced than they are.

[11] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Privacy and Information Quality Policy Development for the Justice Decision Maker*, (Washington, DC: 2005) p. 1.

[12] 2003-16 Executive Order Creating the Illinois Integrated Justice Information System Implement Board <http://www.illinois.gov/Gov/pdfdocs/execorder2003-16.pdf.>

[13] Internal Revenue Service *Privacy Impact Assessment: Version 1.3* (Washington, DC: December 17, 1996) <http://www.cio.gov/spci/spci/docs/IRS.pdf#search='privacy%20impact%20assessment'>.

[14] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, "Global Security Working Group," *Informational Technology Initiatives*. [online] Available at: <http://it.ojp.gov/topic.jsp?topic_id=58>.

[15] Ibid.

[16] US Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, [online] Washington, DC, January 2006. Available at: <http://it.ojp.gov/topic.jsp?topic_id=8>.