ICJIA

ILLINOIS CRIMINAL JUSTICE INFORMATION AUTHORITY

120 S. Riverside Plaza, Suite 1016
Chicago, Illinois 60606

Tel: (312) 793-8550
Fax: (312) 793-8422
TDD: (312) 793-4170

www.icjia.state.il.us

Rod R. Blagojevich
Governor

Sheldon Sorosky
Chairman

Lori G. Levin
Executive Director

June 2004

"Privacy Schmrivacy?"

DRAFTING PRIVACY POLICY IN AN INTEGRATED JUSTICE ENVIRONMENT

(and why it's important)

“Privacy Schmrivacy?”
Drafting Privacy Policy in an Integrated Justice Environment (and why it’s important)

by Wil Nagel

Wil Nagel holds a Bachelor of Science in Criminal Justice from Loyola University Chicago and is a Juris Doctor Candidate at the John Marshall Law School. He is also an analyst with the Illinois Criminal Justice Information Authority working on the Illinois Integrated Justice Information System (IIJIS) initiative. His work on the IIJIS initiative centers on the development of a privacy policy intended to guide the sharing of information throughout Illinois’ justice system.

Robert Boehmer, General Counsel of the Authority, provided editorial assistance and guidance.

This project was supported by grants 99-DB-BX-0017 and 01-MX-CX-0031 awarded by the U.S. Department of Justice. Points of view or opinions contained in this document do not necessarily represent the official position or policies of the U.S. Department of Justice.

I.
INTRODUCTION

In response to public outrage spurred by the revelation that the FBI compiled files on Vietnam War protestors, civil rights activists, celebrities, and thousands of other citizens seemingly selected at random, Congress passed the Privacy Act of 1974.[1] The purpose of the Privacy Act was "to promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch…to observe certain constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals."[2] Specifically, the act was "designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens [by] over-zealous investigators and [curious] government administrators."[3]

To a limited extent the Privacy Act has worked. "While the law doesn't explicitly prohibit the government from compiling dossiers on presumably law-abiding private citizens, the FBI and other agencies in the past have generally interpreted it that way."[4] Additionally, several agencies, including the FBI and the Justice Department's computer crime unit, have promulgated internal guidelines that bar them from actively assembling such files themselves.[5]

September 11th, however, has changed these attitudes. Law enforcement and government demand for data has increased as programs that seek to prevent acts of terror proliferate.[6] But even before Sept. 11, 2001, 20,000 IRS agents had access from their desktop computers to outside data on taxpayers' assets, driving histories, phone numbers, and other personal statistics.[7] Likewise, the FBI and the U.S. Marshals Service had access, with just a few keystrokes, to motor vehicle, driver, and boat registrations, liens and deed transfers, phone listings, military personnel records, and even voter rolls.[8]

The call for increased information sharing has been sounded. From the federal government's Total Information Awareness proposal (renamed in the face of controversy to "Terrorist Information Awareness")[9] and the impending implementation of the Computer Assisted Passenger Prescreening System (CAPPS II), to local and statewide justice integration efforts across the nation, the utilization of technology to improve the collection, analysis, and sharing of data has become an answer to terrorism. And this sharing of data is not limited to the exchange of information among government agencies. The government is interested in the books people read, purchases made on the internet, how payments for services are made, living arrangements, travel reservations, and e-mails as well as telephone, medical, and bank records.[10] Federal and state governments pay about $50 million a year to comb through privately operated databases containing this information.[11]

With the advent of newly integrated, electronic information sharing, citizens face the threat of becoming a society under surveillance. As with any information system, that surveillance can be abused. In Los Angeles, a detective illegally ran a computer background check on a little league baseball coach he didn't like.[12] Another Los Angeles police officer used the police database

hundreds of times to access celebrities' law enforcement records in order to sell them to tabloid newspapers and magazines.[13] In response to concerns regarding private citizens' use of publicly available databases, the New Hampshire Supreme Court ruled that the family of a young woman killed by her obsessed stalker had grounds to sue the internet data broker he hired to locate his victim.[14] As information systems become more thoroughly integrated, the amount of information these abuses may reveal about someone increases greatly.

With these concerns in mind, Illinois Executive Order No. 16 (2003), creating the Illinois Integrated Justice Information System (IIJIS) Implementation Board, contains specific provisions intended to ensure that the privacy and civil liberties of all citizens are enhanced rather than diminished by implementation of the IIJIS.[15] Furthermore, the Illinois Integrated Justice Information System Strategic Plan also recognized the need to develop systems and policies that preserve the integrity and effectiveness of public safety efforts, protect individuals from inappropriate use or release of their information, and promote appropriate public access for oversight of the justice process.[16]

This paper proposes a process for drafting a privacy policy in an integrated justice effort. The recommendations included herein are intended to guide the activities of a privacy policy committee composed of representatives with diverse privacy interests. The paper sets forth several steps necessary for the efficient and informed direction of a committee whose function is to draft a comprehensive privacy policy intended to govern the operation of an integrated justice system. Throughout this paper, the term privacy policy is understood to mean the written procedures that control the collection, use, and dissemination of information including statutes and regulations, as well as other written documents that assist local agencies in implementing statewide policies.

Part II of this paper briefly discusses the need for any justice system integration effort to create or adopt a comprehensive privacy policy. It points out that the public is interested in these privacy issues and can be expected to support the development of new rules for societal uses of criminal history information in an age where technological advances may have made informal methods of protection both insufficient and ineffective. It also advocates the creation of a comprehensive policy to avoid the gaps and oversights involved with ad hoc lawmaking.

Part III argues that while many recognize the importance of privacy they are unable to explain precisely what privacy is. It explains that the way people understand privacy profoundly influences how they shape legal and policy solutions. This part provides a concise overview of privacy by addressing the value of privacy. It also combines many concepts of privacy into more manageable clusters in order to facilitate understanding.

Part IV introduces the National Criminal Justice Association's *Justice Information Privacy Guideline*, which discusses a variety of privacy issues intended to inform the decision-making practices of justice leaders when developing privacy policies.[17] Part IV contends, however, that the needs of a statewide integrated justice information system are somewhat different from the proposed guidelines. This part provides several recommendations for directing the discussions and activities of a privacy policy committee.

Much emphasis is placed on informed policymaking by outlining the research that should be conducted before a committee is convened. Part IV also introduces the decline of practical obscurity in our age of data aggregation as a significant issue facing the development of a privacy policy in an integrated justice environment. This part ends with a discussion of the committee's final report, specifically its recommended components and uses.

The paper concludes that the proposed process will assist a policy committee by aiding in its understanding of integration-specific privacy issues. This understanding, it is contended, will allow the privacy policy to more completely address the privacy issues created by an integrated justice system.

II.
THE NEED FOR AN INTEGRATED JUSTICE PRIVACY POLICY

In January 1999, the Chief Executive Officer of Sun Microsystems told a room full of reporters and analysts that consumer privacy issues are a red herring and that "you have zero privacy anyway—get over it."[18] Given this statement, it is no wonder that nearly 90 percent of adult Americans are concerned about the possible misuse of personal information.[19]

The percentage of Americans concerned about privacy threats has increased steadily since 1970.[20] Despite the decades since Watergate, social protest movements against the Vietnam War, racial justice, and gender discrimination, (events that caused a general fall of public confidence in government institutions) the percent of the public concerned about threats to their privacy has increased from 66 percent in 1978 to 94 percent in 1999.[21] While the impact of terrorism against the United States is a factor, the primary reason for current concern appears to relate directly to the changing nature and magnitude of threats to privacy due to technology.[22]

Changes in technology have usually provided the impetus for the evolution of the American concept of information privacy and privacy law.[23] Currently, technology has made it significantly easier to collect data regarding individuals and to collate that data into a dossier that may shape and define how an individual is perceived and treated with regard to government and the justice system.[24] It is uncertain whether the increased access to information and the ability to relate disparate pieces of a person's information result in a distorted and inaccurate picture of that person.[25]

Although the privacy implications of easy access to vast quantities of information and the analytical capabilities of today's technology are undetermined, governments and agencies in the U.S. (federal, state, and local) have already collected extensive data on American citizens and other persons of interest.[26] Some of the more prominent data collection entities that are bound by certain dissemination limitations include: (a) the U.S. Census Bureau; (b) the National Crime Information Center (NCIC), which collects and stores criminal records of every person arrested in the United States for a felony or serious misdemeanor and interfaces with over 64,000 state and local governments and some foreign nations; (c) the Internal Revenue Service (IRS) which collects substantial personal information; (d) the Social Security Administration; (e) the national Office of Personnel Management and their state equivalents; and (f) state motor vehicle administrations.[27]

However, TSA's new Computer Assisted Passenger Prescreening System (CAPPS II), the FBI's Carnivore system, now renamed to the more innocuous "DCS1000,"[28] and the partially defunded Terrorist Information Awareness System (TIA),[29] create instances where raw data is

or will be under the control of agencies with limited public accountability. In each of these systems, few regulations are in place controlling how long collected data will be maintained, who will have access to the data, or how the information will be shared with other agencies.[30] Furthermore, few, if any procedural recourses are available to persons who believe they are wrongfully affected by their inclusion in these systems.[31]

When fully implemented, CAPPS II will, based upon a rapid search of commercial and government databases, provide airline passengers with a red, yellow, or green risk code that will determine the level of security scrutiny a passenger will receive while at the airport.[32] Passengers posing an acceptable level of risk are coded green and will follow normal security screening; passengers posing a potential or unknown risk are coded yellow and subjected to heightened screening, such as a bag search and a search of their person; finally, passengers whose level of risk is unacceptable are coded red and will not be issued boarding passes until law enforcement officials determine whether the individual will be allowed to travel.[33] Carnivore monitors all internet traffic and e-mail traveling through an internet service provider[34] and before it was defunded, TIA was expected to provide persistent storage of everything from credit card, to employment, to medical, to internet service provider records.[35]

Congress was so worried about TIA's lack of public accountability that it prohibited the deployment, implementation, or transfer of any part of the TIA program until the Pentagon, the CIA, and the Justice Department reported on the project's privacy implications and detailed the scope of the system operations.[36] The Senate requested a similar report on behalf of the CAPPS II project.[37] These later developments clearly denote that public concern or a damaging privacy incident can bring a multimillion-dollar information system to a halt.[38]

While only 12 percent of adult Americans say that their privacy has been invaded or has been lessened as a result of a law enforcement agency (and only 10 percent by a government tax, social service, welfare, or license agency), 25 percent to 30 percent of the public say that they feel their privacy has been violated by business activities.[39] This disparity between the public's perceptions regarding violations of privacy by government and businesses may be misleading. In an earlier survey taken in the mid-1990s, the American public identified business and government as equal threats to privacy.[40] Furthermore, information distributed and used by businesses often times originates from a government agency. For example, agencies such as circuit court clerks' offices routinely sell, according to their own policies, bulk data—large amounts of personally and non-personally identifiable information disseminated at one time from an electronic information system—to commercial users who repackage and resell the information to secondary business users.[41] Freedom of information acts also contribute to these information disclosures.[42] Criminal charges and convictions are among the types of information made available by these means.

Because criminal charges and convictions are made so readily available, there is a high level of concern (69 percent) about the collection, maintenance, and distribution of criminal history records by private companies,[43] which purchase the information and compile it by name and date of birth. Without additional identifying characteristics, such as fingerprints, the risks of incorrectly portraying innocent people as criminals because they have the same or similar names to criminal defendants increases substantially. As such, 85 percent of adults feel that such commercial companies should follow the same fair information rules and procedures as would bind government criminal history agencies.[44] Furthermore, there is a general sense among the public that there are major changes in the uses of criminal history information in our society because of advanced information technology.[45] This sense may be driven by statutes that require the production of criminal history information for various non-criminal justice users,

such as those providing licensing standards for people who deal with senior citizens, children, and school systems.[46]

It is important to note here that infringements on privacy tend to be "creeping," that is, they often occur in small encroachments into our private lives. Privacy is often destroyed by an aggregation of these minor encroachments and not always by a large exercise of state power.[47] Despite the patchwork of state and federal statutes that have been passed in response to perceived privacy concerns,[48] many now view government policy makers as falling behind in the effort to protect citizens' privacy, thus leaving the law enforcement community and the marketing industry to determine how much privacy there will be in the future.[49] Continuing the process of ad hoc law making is not advisable; a more comprehensive privacy policy is clearly favored.[50]

The public is interested in these privacy issues and should support the development of new rules and policies for societal uses of criminal history information in an age where technological advances may have made informal methods of protection both insufficient and ineffective.[51] By addressing the public's privacy concerns in a clear and informed manner, a privacy policy has the potential to significantly increase the public's confidence in justice information practices and, by doing so, decrease the level of concern regarding the potential misuse of personal information contained in an integrated justice system.

III.
GOT PRIVACY?

The need for flexibility in conceptualizing privacy is epitomized in the Supreme Court's 1928 decision in *Olmstead v. United States*.[52] There, the Court held that the wiretapping of a person's home telephone (done outside a person's house) was not contrary to the Fourth Amendment because it did not involve a trespass inside a person's home.[53] The *Olmstead* Court had clung to the outmoded view that the privacy protected by the Fourth Amendment was merely freedom from physical incursions.[54] As a result, for almost 40 years the Fourth Amendment failed to apply to wiretapping—one of the most significant threats to privacy in the 20th century.[55]

Judicial opinions, statutes, and policies have largely failed to adapt to the information practices of today in much the same manner that the Supreme Court failed to adapt the Constitution to the new problems posed by wiretapping in *Olmstead*. This failure is often caused by the difficulty in articulating what privacy is and why it is important.[56] Indeed, the attempt to define privacy implicates the span of human history and virtually all academic disciplines that seek to better understand the essence of the human condition.[57] Nevertheless, an understanding of privacy is necessary in order to guide policymaking and subsequent legal interpretation.

But what is privacy? While we all have some intuitive sense that there are certain aspects of life that are private,[58] this intuitive sense does not clearly articulate what aspects of life are protected nor the nature and scope of that protection. Many recognize the importance of privacy for achieving important ends (i.e., freedom, democracy, social welfare, self-creation, independence, autonomy, creativity, and freedom of thought) and assert that privacy is worth

protecting at significant cost, often restraining other important interests such as efficient law enforcement and freedom of speech and press.[59] But why is privacy valuable enough to make substantial trade-offs to protect it?

A. THE VALUE OF PRIVACY

Understanding why individuals value privacy can illuminate what privacy is and enable us to begin resolving privacy issues. A popular method of evaluating the value of privacy involves categorizing the values as contextual or functional. Functional values include: avoiding embarrassment, constructing intimacy, and averting misuse. Along with identifying the functional value of privacy, privacy can also be valued contextually.

Privacy is valuable because it serves to prevent the simple pain of embarrassment. The exposure of certain behaviors, actions, or physical attributes to the public may cause embarrassment—especially when individuals keep those behaviors, actions, or physical attributes from the view of others based upon social practices.[60] As a society, we are upset about such disclosures, not because they reveal a secret; rather, we are upset because these aspects of human life have been socially relegated to the private sphere and as such are connected to human dignity.[61]

Privacy is also valuable in its ability to construct intimacy. The ability to selectively reveal personal information partly creates intimacy.[62] Intimacy must exist between two individuals in order for their relationship to evolve from the basic respect due to all human beings into a relationship of trust, friendship, or love. Privacy fosters the construction of deep social relationships by allowing individuals to display certain behaviors unseen in public areas such as playfulness, childlikeness, and certain types of physical touching.[63] Surveillance arguably could inhibit the free and spontaneous display of care and affection toward others.[64]

Another value of privacy is that it protects against improper uses of personal information. This is the value of privacy that integration affects the most. The misuse of personal information can occur in two ways. First, it can unduly influence an otherwise fair process that distributes benefits and burdens.[65] Employment opportunities, political offices, and respect—as well as animosity, disrespect, and imprisonment—are granted or denied us based upon information about ourselves. If society allocates these social benefits and burdens based upon inaccurate information, technically accurate but misleading (because it is incomplete or outdated) information, or inappropriately considered information, unfairness may result.

Second, the misuse of information can make us vulnerable to unlawful, disingenuous, and prejudicial acts. Not only can the knowledge of our home phone number and address expose us to harassers and stalkers, but accessible personal information can also make us vulnerable to identify theft. Vulnerability of individuals can result in significant social consequences. Such vulnerability can chill individuals from engaging in perfectly legal, but unpopular activities that can corrode private experimentation, deliberation, and reflection.[66] This self-repression can result in bland, unoriginal thinking and could undermine the self-critical capacities of a body politic.[67]

In addition to the functional value of privacy in achieving the ends of avoiding embarrassment, constructing intimacy, and securing personal information, privacy should also be valued

contextually. For example, when analyzing the value of the privacy of the home in order to make legal and policy decisions, one must look to the purposes of the privacy practices of the home.[68] One purpose of the home today is to serve as a place where one can retreat from the bustle of public life and enjoy tranquility and solitude necessary for individual self-development.[69] Oftentimes other values (such as the free speech rights of protestors to congregate outside a person's home) conflict with our desire to protect this purpose of the home.[70] Similarly, privacy issues confronting the integration of justice information systems should be analyzed in the context of the public safety concerns of the justice system. If privacy furthers a socially desirable practice, then privacy is recommended; if privacy negatively affects the protected interest, then less privacy may be desirable.

B. THE CLUSTERS OF PRIVACY

Understanding why privacy is important is only a beginning. We also need to understand what it *means* if we are going to draft a key policy designed to affect the information practices of today. Rather than cling to a single unified theory of privacy, a better policy can be drafted by examining the areas of our lives that are most affected by justice information sharing. By understanding the three privacy clusters of space, decision, and information, one can better explain the privacy issues that the policy should address. It is important to note that these clusters overlap and are not sharply separate from each other.[71]

The spatial cluster of privacy involves the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals.[72] This understanding has been defined as "the right to be let alone, to live one's life as one chooses, free from assault, intrusion or invasion except as can be justified by the clear needs of community living under government law."[73] It is this understanding of privacy that informs Fourth Amendment expectations of privacy.[74] This is also the sense of privacy invaded by a telemarketing call or Internet spam.

The second cluster of privacy is concerned with an individual's ability to make significant, self-defining decisions without interference (usually from the state). This decisional cluster of privacy is espoused in several of the Supreme Court's substantive due process decisions.[75] Generally, federal constitutional law recognizes decisional privacy rights in matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.[76]

The informational cluster of privacy concerns an individual's control over the acquisition, disclosure, and use of personal information. This understanding of privacy should not be confused with the public disclosure of previously concealed information.[77] Privacy in this informational sense is "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used."[78] This is also the cluster of privacy that an integrated justice system most threatens.

In order to understand the informational cluster of privacy, one must understand what is meant by "information identifiable to the individual." There are three ways that information can be identifiable to an individual. The information can bear (1) an authorship relation to the individual, (2) a descriptive relation to the individual, or (3) an instrumental mapping relation to the individual.

Information can be connected to an individual when that person purposefully creates or prepares the information in order to communicate it to another party.[79] This author-relationship may be broader than copyright law and explains why a telephone conversation, personal diary, love letter, or e-mail constitutes personal information.[80]

Information can describe an individual in many ways. The information could indicate some permanent biological status of the individual such as sex, height, weight, blood type, fingerprint, retina pattern, or DNA profile.[81] It could relate biographical facts including birth date, marital status, sexual orientation, immigration status, criminal history, or educational degrees.[82] Descriptive information can also include social connections, such as membership in religious and political organizations, as well as surveillance data.[83]

Information can further be identifiable to the individual if it is an instrument used to track the individual, secure access, or provide some service or good.[84] The best example is a social security number which is neither created nor authored by the individual nor does it describe the individual's state-of-being or actions.[85] Rather, the federal government attaches this number for record keeping purposes. This category of personal information includes network login passwords and automatic teller machine personal identification numbers.

Because the way people understand privacy profoundly influences how they shape legal solutions,[86] it is essential that the committee understand what privacy means if it is going to design a policy that will meaningfully influence the information practices of an integrated justice system. While several state and federal statutes have already defined and protected significant areas of personal information,[87] new privacy problems, such as the decline of practical obscurity and the development of digital dossiers, are emerging because of new information technologies. Furthermore, current solutions to old privacy problems may need revision. In order to construct the best solution to privacy problems, the committee must understand the nature of the problem, what is at stake, and what important values are in conflict. Understanding privacy itself is only part of this process.

IV.
A MODEST PROPOSAL

In September 2002, the National Criminal Justice Association published the JUSTICE INFORMATION PRIVACY GUIDELINE.[88] An impressive 121-page document, the GUIDELINE discusses a variety of subjects intended to inform the decision-making practices of justice leaders when developing privacy policies.[89] However, the GUIDELINE'S national perspective may not provide enough background for state-level justice integration leaders. Rather, state-level policy makers may require a more focused discussion on the issues that directly affect their privacy policy drafting needs.

This Part supplements the GUIDELINE by providing additional privacy foundation and setting forth several steps necessary for the efficient and informed direction of a committee whose function it is to draft a comprehensive privacy policy intended to govern the operation of an integrated justice system. It is envisioned that a policy will emerge from an assessment of the state's

current privacy environment and recommended amendments where integration technology unintentionally creates a gap in the privacy policies otherwise advanced by the legislature. Particular emphasis is placed on research and analysis intended to inform policy decisions and expound upon the purposeful nature of the committee's policy decisions. This part also includes a capsule summary of the diminishing availability of practical obscurity to protect individuals' privacy rights. The part concludes with some final remarks about the structure and use of the privacy committee's final report.

A. A WORD ABOUT THE PRIVACY COMMITTEE

By its very definition, an integrated justice system encompasses interagency, interdisciplinary, and intergovernmental information systems that access, collect, use, and disseminate critical information at key decision points throughout the justice process.[90] Because of the multiple agency nature of an integrated justice system initiative, the utilization of a committee to make policy recommendations concerning the sharing of justice information is imperative if those decisions are to bind all the participating agencies. Furthermore, the collaboration of participating justice practitioners on the development of the privacy policy will help ensure their agencies' "buy-in" of the completed product.

While essential to the development of the privacy policy, merely including participating agencies will not accomplish the committee's goals. Rather, by virtue of its subject matter and the governmental nature of integrated justice initiatives, the privacy committee will require representatives from academia, victims' rights groups, media and commercial sectors, as well as the public to be complete. These parties are necessary to ensure a sufficiently diverse committee able to identify relevant privacy issues and articulate potentially opposing perspectives.[91] If one of the goals of the privacy committee is to secure legislation enacting the final policy, then a representative from the state legislature may be appropriate. In addition to ensuring that the privacy committee includes representatives with diverse privacy interests, this broad range of viewpoints will also facilitate public buy-in of the integrated justice system's privacy policy.

It is important to acknowledge here that privacy principles and policies discussed in a committee of this make-up will not satisfy every criticism. As a result, committee decisions may not be resolved by a clear majority or even a consensus. It is at this point in committee deliberations that the quality of the background research can most influence policy decisions. Most often, background research would be prepared beforehand by privacy committee staff whose responsibility it will be to take the raw privacy material and synthesize it into useful documents for committee members. By providing the committee with clear, concise, and focused research, the committee can make informed policy decisions, more fully aware of those decisions' potential consequences and anticipated repercussions.

In some instances, however, it may be desirable for committee members to draft short position papers supporting or opposing a proposed section of the privacy policy based upon that section's anticipated effect upon their agency. This would allow the person or agency with the most detailed knowledge to educate the committee on the effects of the proposed section. Whenever possible, a supporting and an opposing paper should be provided to the committee. The next subpart focuses on the importance of this background research and provides

suggestions on topics that will require further analysis before the actual work of the committee should begin.

B. RESEARCH, RESEARCH, & MORE RESEARCH

One cannot overstate the importance of making informed policy decisions—especially in the area of privacy. Privacy is a complex and crucial area that is facing new challenges as integrated justice systems provide easier access to information on individuals and the analytical capability to combine that data into digital dossiers. Because the way we understand privacy profoundly influences how we shape policy solutions,[92] it is essential that a significant portion of the development of the privacy policy take place behind the scenes of the committee in the form of research.

The amount of information regarding privacy is vast. Sorting through the countless papers, scholarly journals, government pamphlets, law review articles, national association reports, and newspaper articles is a daunting task to say the least. By far the most difficult component to privacy research is defining its scope. This subpart will help the privacy committee staff by providing recommendations intended to narrow the scope of the research.

The first subsection discusses the fair information practices (FIPs), which have been universally recognized as a solid foundation on which to build privacy legislation and policies.[93] Because the FIPs were not originally developed to operate within the context of justice information sharing, they may require some modification to ensure that public safety information is available where and when it is needed. These areas are discussed below and the subsection concludes that if those modifications strip the FIPs of their protective power, a new model might be necessary.

The second subsection provides a brief discussion on the concept of practical obscurity. Practical obscurity is at the crux of privacy issues created by integrated justice systems. This subsection points out that there is a difference between public records obtained after a diligent search of courthouse files and a computerized summary located in a single clearing house of information.[94] Because the decline of practical obscurity is such a significant issue, only a brief discussion can be provided here and the reader is invited to conduct further research into this area.

Subsection three indicates several areas of federal and state laws whose operation in an integrated justice system will require further research and analysis. It identifies which federal information access, collection, and protection laws might affect the information sharing practices of an integrated justice system. Furthermore, using Illinois as an example, the subsection points out several state statutes and regulations that may affect the operation of an integrated justice system. This subsection serves to demonstrate the ad hoc, patchwork nature of state and federal regulation of information sharing as well as their complex interaction.

Finally, the fourth subsection provides a brief discussion of the major privacy issues that confront any integrated justice system. The topics introduced in this subsection represent the primary work of the committee. The preliminary research conducted on these issues should serve to inform the policy deliberations conducted by the committee.

§ 1. FAIR INFORMATION PRACTICES

In 1973, the Department of Health, Education, and Welfare published a groundbreaking report responding to concerns that harmful consequences may result from the storing of personal information in computer systems. That report, entitled "Records, Computers and the Rights of Citizens," articulated several principles the department deemed essential to the fair collection, use, storage, and dissemination of personal information by electronic information systems.[95] The five basic principles held that: (1) there must be no personal data record keeping systems whose very existence is secret; (2) there must be a way for an individual to find out what information about him is in a record and how it is used; (3) there must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent; (4) there must be a way for an individual to correct or amend a record of identifiable information about him; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[96]

The report even went so far as to recommend that these principles be enacted in a Federal Code of Fair Information Practices applicable to all information systems.[97] While the Federal Code of Fair Information Practices was never enacted, the report was one of the earliest acknowledgements by the federal government that the public's privacy needed to be protected against arbitrary and abusive record-keeping practices. The report also recognized the need to establish standards of record-keeping practices appropriate for the computer age.

The fair information practices that evolved from the 1973 report have largely remained unchanged despite several advances in technology. Furthermore, various aspects of fair information practices have been incorporated into numerous federal statutes, including the Federal Privacy Act of 1974,[98] the Family Educational Rights and Privacy Act of 1974,[99] the Video Protection Act of 1988,[100] and the Health Insurance Portability and Accountability Act of 1996,[101] as well as many other federal and state statutory privacy protection schemes. Even though fair information practices have been in existence for more than 30 years, they are still universally recognized as a solid foundation on which to build everything from privacy legislation and policies to self-regulated privacy standards for the private sector.[102]

While many state and federal privacy provisions exist to protect justice information, current statutes and policies may not be sufficient to encompass the collection, analysis, use, and dissemination of justice information within an integrated justice system.[103] Current privacy provisions may be insufficient for two main reasons.

First, the expanded information sharing capabilities of an integrated justice system are likely to blur the lines between traditional and non-traditional justice information. Non-traditional justice information may include sensitive social service, educational, and medical records that once in the possession of the justice enterprise may fall outside the protective scope of existing legal frameworks.[104]

Second, the expanded information sharing capabilities of an integrated justice system allow justice agencies to gather, analyze, and compile various types of information into a digital biography of an individual.[105] This digital biography could then be shared by components of the

justice system in order to make decisions affecting that individual. Where existing legal frameworks fail to address these issues, it is appropriate for the integrated justice system to address these issues in a manner consistent with the state's existing privacy protections.

To do this, the privacy committee needs to be familiar with relevant federal and state privacy policies as well as the theoretical bases for those policies. It is the FIPs, often in a modified form, that provide those theoretical bases. The Privacy Committee will need to review relevant statutes and regulations (as well as the eight primary FIPs incorporated therein) in order to determine whether those or similar protections should apply to currently unregulated justice information.

FIP Basics

The fair information practices provide rules governing the processing of data subjects' personal data. "Processing," "data subjects," and "personal data" are broadly defined terms.[106] Privacy protection in a justice information system extends to all data subjects regardless of their relationship with the justice system. As such, data subjects can include suspects, offenders, victims, witnesses, and jurors as well as arresting officers.

As previously discussed in Section III, "personal data" is any information relating to an identified or identifiable person.[107] Information can be identifiable to an individual in three ways: (1) the individual could author the information as in the case of an e-mail or telephone conversation; (2) the information can describe the individual either biologically (DNA profile, fingerprint), biographically (marital status, sexual orientation), or socially (religious or political affiliations); or (3) the information can be an instrument that is used to track the individual such as an identifying number.[108]

The fair information practices extend only to data processed electronically or manually.[109] "Processing," however, is conceived broadly to include data collection, recording, organization, analysis, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, erasure and destruction.[110] These broad definitions mean that the FIPs affect the daily activities of an integrated justice system.

Generally speaking, the function of the FIPs is to limit the collection, use, and disclosure of information. As alluded to earlier, the FIPs are clearly stated *guidelines*. As originally created in 1973, they do not contain words limiting their applicability to reasonable circumstances or to situations where they are not unduly burdensome. Where these absolute limitations come up against a compelling interest, however, the typical response has been to add a balancing element to the FIP. In the integrated justice context, applying that balancing element involves weighing the privacy rights of the individual (as expressed in the FIP) against the public safety interest of the justice system. This balancing element is itself a modification of the original FIP.

The FIPs represent a general policy of protecting individuals' privacy rights. Modifying the FIPs themselves, as opposed to creating discrete exceptions to their operation, risks stripping the FIPs of their status as guidelines. While creating discrete exceptions in order to fulfill the compelling interests involved with the justice enterprise may reduce the effectiveness of the FIPs, such exceptions do not dramatically alter the FIPs themselves.

However, the National Criminal Justice Association and the Global Justice Information Sharing Initiative (Global) Advisory Committee have indicated that the FIPs should be modified to

include the flexibility necessary to ensure the public safety by providing relevant information to justice decision makers. If the FIPs are to be modified so that they better apply in the integrated justice context, care must be given that they are not modified so much so that they lose their powers to protect the citizenry's rights to privacy. It is the challenge of the Privacy Committee to make certain that the FIPs are not made too flexible as to eliminate their value as the foundation of the privacy policy.

FIP1. Purpose specification

The Purpose Specification FIP restricts the uses of information to the reasons for which it was collected. According to this FIP, personal information should be collected for specified, explicit, and legitimate purposes and not processed for other purposes.[111] This requires an agency that collects personal information to clearly articulate the reason for information collection.

The Purpose Specification FIP, as it was originally intended to operate, poses considerable problems when applied to the justice enterprise. Too broadly or too narrowly drafting purpose statements dramatically reduces the efficacy of the Purpose Specification FIP. Broadly drafted purpose statements may provide flexibility that might be necessary for the justice system to fulfill its duties but will not result in any meaningful restriction on the justice system's ability to collect personal, and potentially irrelevant, information. Alternatively, too narrowly drafted purpose statements may result in the collection of insufficient information for the prosecution of crimes or the prevention of criminal acts.

As originally drafted, the Purpose Specification FIP did not contemplate the compelled disclosure of information under Freedom of Information Act (FOIA) statutes; however, because of their governmental nature, an integrated justice system and its component agencies will be subject to such public access requirements. While FOIAs attempt to protect personally identifiable information, the compelled disclosure of information may result in a subsequent disclosure and use of personal information in a manner potentially inconsistent with the purposes for its initial collection.

Furthermore, the scope of the Purpose Specification FIP seems limited to the collection and subsequent use of *existing* personal information by justice agencies. As a result, purpose specification does not seem to apply to the information *created* by the activities of the justice system. It is important to recognize that personal information is *generated* by the workings of the justice system as the offender moves through its various components.[112] For example, when an arrestee's fingerprints are taken, a biometrically supported identification number is issued. This identification number is created by the justice system, passed through it, and maintained as part of an official criminal history record. Thus, the principle does not limit how the generating agency may use the identification number.

If purpose specification can be modified to address these issues, an additional step must take place to apply the FIP in the integrated justice context. Before information can be seamlessly exchanged within an integrated justice system, participating agencies would need to harmonize their purpose statements. This is because subsequent use of the information must also comply with the stated purposes for collecting the information. [113]

FIP2. Collection limitation

The efficacy of the justice process depends upon the collection of personal information. Law enforcement, prosecutors, defense attorneys, and pretrial services officers all collect personal information about suspects and the people associated with them such as victims, witnesses, as well as friends and family members.[114] The Collection Limitation FIP calls on agencies to examine why they collect information in order to avoid collecting information unnecessarily.

The FIP limitations on the collection of personal information take two forms: means and relevance.[115] First, personal information for use in the justice system should only be acquired through lawful and fair means. It is expected that this prong of the Collection Limitation FIP will not pose significant difficulties because Fourth Amendment case law provides justice practitioners with a great deal of guidance on what constitutes fair and lawful means of collecting information.

The second prong for the Collection Limitation FIP poses a more complex challenge. According to the FIP as it was originally intended, agencies should avoid collecting personal information that is extraneous to the goals of the justice system. However, there are several difficulties involved with determining which pieces of information are extraneous and which are not *at the time of collection*. Oftentimes it is not until much later in the justice process that the relevancy of a certain piece of information is ascertainable.

This difficulty was cited by the Department of Justice in its proposal to exempt several of the FBI's information systems from the requirements of the Privacy Act. Specifically, the Department of Justice sought exemption "because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed…would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement."[116]

It may not be possible to mesh the collection limitation principle with the goals of the justice enterprise. If this is the case and an exception is made permitting the justice system to collect seemingly irrelevant information on the grounds that it may acquire relevance as an investigation evolves, an additional check and balance might be found in the Use Limitation FIP. Under that check and balance, while the justice system might be allowed to collect seemingly irrelevant information (an exception to the collection limitation principle), information that did not become relevant to that case may need to be purged from justice information record systems in accordance with the use limitation principle.

This interaction between the FIPs, where one FIP makes up for the lack of compliance in another, serves to demonstrate why exceptions may be preferable to modifications to the FIPs. Such interactions further the goals of the justice system and protect individuals from the disclosure of personal information that was not relevant to an offense. The Use Limitation FIP is discussed further below.

FIP3. Use limitation

Under the Use Limitation FIP, agencies are required to limit the use and disclosure of personal information to the purposes articulated in their purpose statements.[117] While the Use Limitation

FIP seems to function as a relatively strict control use of information, it is one instance where the FIP contains several discreet exceptions. Specifically, personal information can be used for any number of reasons not related to reasons the justice system collected it when (a) the subject of the data consents, (b) the agency has the legal authority to do so, (c) the safety of the community is at issue, or (d) a public access policy permits the disclosure.[118]

These four exceptions, however, are not as explicit as they first appear. For instance, the scope of the consent required under the first exception is unclear. Consent is often described as willingness or a grant of assent, but it is not known whether a data subject's consent is assumed or if he must take some affirmative action in order to consent to the disclosure of his information. Further, if the data subject must take affirmative steps to consent, the exception is not clear as to whether a global waiver of information is sufficient to fulfill the consent requirement or if a more precise and unambiguous agreement is necessary.[119]

The Privacy Committee will focus much of its research on the second and the fourth exceptions. As discussed later, the current ad hoc approach to privacy legislation has made it extremely difficult to determine if an agency has the legal authority to use information for reasons other than why it was collected or if a public access policy permits the disclosure.[120] One of the goals of the Privacy Committee is to compile all the various statutes governing the privacy of justice information and determine whether they provide an appropriate privacy framework or lead to inconsistent privacy protections.

The third exception to the Use Limitation FIP allows the use of justice information when the safety of the community is at issue. This exception, however, fails to articulate precisely what level of risk is required before the justice information can be disseminated in accordance with its terms. For example, while the police are almost expected to provide a sketch or photo of a suspected murderer at large in the community, or booking photographs of prison escapees, does this exception also allow a local police department to distribute a flyer entitled "Active Shoplifters" containing the arrest booking photos of shoplifting suspects who were arrested but not necessarily convicted?[121] If this exception is to function legitimately, what qualifies as a sufficient risk necessitating the dissemination of justice information must be better defined. The failure to do so may result in unequal privacy treatment among differing jurisdictions.

Even though the Use Limitation FIP doesn't touch upon the issue, it is important to note that valid uses of personal information also include its retention and destruction. In fact, the original fair information practices call for the destruction of personal information when it no longer serves the original processing purposes.[122] It is unlikely that justice system practitioner will accept this principle as criminal history record information repositories provide much of the information necessary for informed decision-making.

The Use Limitation FIP is of significant importance in the integrated justice context because such systems are *designed* to easily transfer information for reuse. If the use limitation principle is to effectively apply in the integrated justice context, participating agencies would need to harmonize their purpose statements so that the transmission of information within an integrated justice system is consistent with both the individual agency's and the integrated justice system's mandates.[123] As discussed earlier, the difficulty in drafting purpose statements may pose a considerable challenge to this end. Moreover, because the Use Limitation FIP takes on even greater significance when those outside the justice system disclose personal information, particular emphasis must be applied where justice information is disseminated to the public pursuant one of the four exceptions.

FIP4. Data quality

Under the Data Quality FIP, agencies must verify the accuracy, completeness, and currency of their information.[124] While concerns over data quality have existed for several decades and there are many efforts under way nationwide to improve the quality of justice data, the FIP imposes considerable constrains upon an integrated justice system. This is not to say that the justice system should not strive to collect and maintain complete and accurate data; rather, there must be some acknowledgement that, in instances where public safety is in jeopardy, the use of potentially inaccurate or incomplete information may be appropriate.

The criminal justice system poses two unique challenges to the collection and use of complete and timely information – the sealing and expunging of criminal history records and the use of intelligence and investigative data.

The first challenge unique to the justice system involves the modern trend of providing qualifying offenders an opportunity to clear their criminal history record of certain arrests and convictions through the operation of expungement and sealing statutes. Several difficulties exist in measuring the accuracy, completeness, and timeliness of the record expungement process because of the nature of these orders and the *prior* public nature of the information involved. Compliance isn't the only data quality issue involved with expungement and sealing statutes; expungement orders, in effect, are legislative and judicial pronouncements that otherwise accurate and complete information can no longer serve as the basis of any decision because it is essentially not quality data.

Investigative and intelligence data creates its own issues when the information must meet certain quality standards before the justice system can disseminate or use it. Raw investigative as well as intelligence data may be fraught with inaccuracies until verified or crosschecked with other data.[125] In light of the justice enterprise's paradigm shift from responding to criminal or terrorist activity to preventing such acts, it is anticipated that these types of information will require special consideration or even exemption from the requirements traditionally imposed by the Data Quality FIP.

A policy that addresses data quality issues in an integrated justice system should include provisions for data source identification (i.e., where the data came from and who has the ultimate responsibility for complying with the relevant privacy policies); data management; uses of the data including cross referencing, correction, and dissemination logs; record retention and destruction; as well as administrative standards for modifying incorrect records.[126] Because poor data quality is oftentimes the result of poor enforcement of policies rather than a failure of the policies themselves, the Accountability FIP will take on increased importance in this area.

FIP5. Openness of data management practices

Under the Openness FIP, agencies are required to provide notice about how they collect, maintain, and disseminate personal information.[127] This notice should include a statement:

(a) Indicating the main purposes for the data's use;[128]
(b) Identifying the person and office responsible for the data;
(c) Identifying those who may access or receive the data;
(d) Explaining whether the information is mandatory or voluntary and the consequences of failing to provide the information; and
(e) Informing the data subject that he has a right to access the data and rectify errors.[129]

Adherence to the Openness FIP also requires agencies to clearly communicate to affected individuals when third parties request, sell, or release individuals' justice records.[130]

The Openness FIP focuses on the management of the data instead of the actual data itself; it also imposes significant burdens upon agencies that collect personal information. However, the FIP is silent as to whether the failure to provide the required notice could potentially deny the collector of the information the right to use it.[131] Furthermore, it does not indicate what would amount to due diligence when the collector of the information was unable to readily locate the individual.

While the notice requirements of the FIP may be reasonably applied in the integrated justice context, requiring justice agencies to communicate to individuals that their records were requested, sold or released to third parties would most likely be considered unduly burdensome to the efficient administration of justice. Furthermore, during the course of an investigation or prosecution or a criminal offense, it may be a violation of policy, legal precedent, and evidentiary rules to notify the individual of such disseminations of justice information.[132]

FIP6. Individual participation

Originally stated, the Individual Participation FIP requires agencies to allow easy and convenient access by individuals to their personal information. Except where it would compromise an investigation, case, or court proceeding, individuals should have the right to:

(a) Obtain confirmation of whether or not the agency has data relating to him,
(b) Have the data communicated to him in a reasonable time and manner at reasonable cost,
(c) Challenge a denied request under (a) or (b), and
(d) Challenge incorrect data and if successful have the data erased, rectified, completed, or amended with notification to all parties who received the incorrect information.[133]

The Individual Participation FIP further requires an annotation to the data where an organization decides not to amend information as requested by the individual.[134]

While the Department of Justice requires criminal history repositories to provide individuals with the right to review and challenge their criminal history transcripts,[135] there are several types of justice information potentially part of the integrated system, that do not provide such a right. The committee will need to examine to what extent, if any, a right to review and challenge these types of information should exist. Currently, no standards or factors exist to help make this determination.

Where information not currently subject to access and review requirements is later subjected to such challenges, several administrative procedures must be developed. Standards should be developed for how quickly and how often the integrated justice system or the originating agency should provide the requested information to the data subject.[136] Furthermore, the form and manner in which the information is provided to the requestor should also be standardized. In addition, according to the Individual Participation FIP, the information reviewed by the data subject should include how the information is being used, whether it is being used, and to whom the information has been disclosed.[137] Finally, administrative standards for modifying an incorrect record must be developed and implemented for each additional type of information subject to the new access and review requirements.[138] The Privacy Committee will need to determine which types of justice information should appropriately be subject to review and challenge and with types should not.

FIP7. Security safeguards

The process of building an integrated justice information system increases interface points among justice agencies and with the public.[139] With the dramatic increase in electronic information exchanges and transactions inherent in an integrated justice system, valuable information resources will likely increase the system's exposure to privacy violations and security breaches.[140] As a result, the privacy policy should address the protection of personal data by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.[141]

Inherent in the justice system's authority to collect information of a highly sensitive nature is the responsibility to protect it – through both policy and technology. Security is an area that is constantly driven by technology. However, informed privacy policy decisions should drive the design and development of technology, rather than technological capability dictating the formation of privacy policy.[142] Furthermore, the Security Safeguard FIP is one form of implementation of the privacy policy through such technologies as encryption, public key infrastructure, digital signature, biometrics, firewalls, intrusion detection, and virtual private networks.[143] As such, the Security Safeguard FIP will most likely only be addressed in an introductory manner and will not be a focus of the privacy committee's deliberations.

FIP8. Accountability

The Accountability FIP requires agencies to have a means of ensuring that their policies are followed. Specifically, the Accountability FIP calls for the development and implementation of due process mechanisms, usually in the form of administrative procedures, through which an individual may challenge an agency's compliance with its privacy policy.[144] The FIP further insists upon a timely and fair response to the challenging party. Where an agency has failed to comply with its policies, the FIP mandates administrative penalties be imposed against the offending agency or its employee and also that affected individuals be informed of their available recourses.

It must first be noted that the Accountability FIP is concerned only with an agency's compliance with its privacy policy. This is fundamentally different than public accountability of the justice system concerning its efficacy. Accountability mechanisms in the context of justice information systems usually take two forms, administrative sanctions and judicial remedies. Administrative sanctions generally involve the loss of access to a justice information system for failing to comply with its policies. Judicial remedies can include both criminal and civil actions for the deliberate misuse of justice information.[145]

It is recommended that the Privacy Committee review existing accountability provisions and administrative sanctions for their design, implementation, and enforcement. Also, any existing judicial remedies for individuals aggrieved by a justice agency's misuse of justice information should also be identified and evaluated for their potential applicability to the integrated justice system. Finally, administrative procedures through which the integrated justice system's compliance with the privacy policy can be challenged will also need to be developed. As part of the accountability principle, the Privacy Committee may want to consider the feasibility of periodic audits to determine the integrated justice system's level of compliance with the privacy policy.

FIP Conclusion

As explained above, the FIPs are firmly stated principles designed to protect the individuals whose data is collected. While these principles have served as a *foundation* for privacy policies, they have traditionally been modified to the particular context in which they are to be applied. In order for the FIPs to effectively regulate information sharing within an integrated justice information system, it will be necessary to create exceptions to certain rules while modifying others altogether. Most often, modifications will involve adding a balancing element whereby individuals' privacy rights are weighed against the public's rights to safety.

Even when modified, however, the FIPs do not provide any additional factors to help inform that balancing. It is thus the responsibility of the Privacy Committee to develop relevant factors for use during the balancing tests; the development of such factors will be necessary in order to ensure uniform application of the test throughout the state. Even with such guidelines, however, there is the risk that the balancing element may not supply sufficient privacy protections where the government's compelling interest is the safety of its citizens. If these balancing mechanisms prove to be too vague to form the substance of the policy, or if the FIPs must *themselves* be modified to the extent that they provide insufficient protections of the citizenry's civil rights, a new model may be called for.

§ 2. PRACTICAL OBSCURITY FOR PRACTICAL PEOPLE

Perhaps the most significant of privacy issues created by an integrated justice system can be attributed to the decline of practical obscurity. Integrated justice systems are designed to enhance querying capabilities of regional, statewide, and national databases as well as aggregate and report critical information regarding the people or cases queried.[146] Or, stated another way, integration initiatives are efforts to improve the operation of the justice enterprise by eliminating barriers to accessing information.[147] Those barriers are the substance of practical obscurity.

"We know that our lives will remain private not in the sense that our personal information will be completely shielded from public access, but in the sense that for the most part, it will be lost in a sea of information about millions of people. Our personal information remains private because it is a needle in a haystack, and usually nobody will take the time to try to find it. This anonymity is rapidly disappearing as access to information increases [with the analytical ability to compile that information into digital biographies]."[148]

Until recently, public records were difficult to access and were only available locally.[149] Finding information about a person often involved a treasure hunt around the country to a series of local offices to dig up records.[150] While courthouse doors and files were open, there were far too many courthouses to visit in the hope of finding something of interest.[151] Furthermore, "because most people didn't bother to go down to the courthouse to rifle through the files to see what allegations might have been made against their neighbors, the result was only people with a true interest in the matter ever bothered to access the material. We had to wrestle with the loss of practical obscurity."[152]

"The notion that public records are limited by the built-in protection of practical obscurity was first advanced by the Supreme Court in [*U.S. Department of Justice v. Reporters Committee for Freedom of the Press*].[153] There, a press organization made a Freedom of Information Act

request for an individual's FBI rap sheet, which compiled arrests, prosecutions, convictions, and acquittals from several states into a computer-stored criminal history summary.[154] In discussing the individuals' privacy interests in his criminal history, the court noted that the issue was "whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by the disclosure of that information."[155] Although the individual records contained in the criminal history were public, the court ruled that they were in a sense protected by the barriers of time and inconvenience involved in collecting them.[156] Thus, the court ruled that there is a "vast difference between public records that might be found after a diligent search of courthouse files…and a computerized summary located in a single clearinghouse of information."[157]

The rubber hits the road where freedom of information acts provide for the release of vast quantities of information that were previously obscure and information technologies provide the capability to aggregate those records into personal dossiers. Freedom of information acts serve three purposes: "first and most important, ensure public access to the information necessary to evaluate the conduct of government officials; second, ensure pubic access to information concerning public policy; and third, protect against secret laws, rules and decision making."[158] Thus, freedom of information acts created a checks and balances system in which the public could monitor and regulate government agencies.[159] Statutes serving these purposes are often referred to as "open access," "right to know," or "sunshine" laws.[160]

Much of the information contained in public records, however, does not necessarily shed light on the way government carries out its functions.[161] Rather, this information reveals more about the people who are the subjects of the government's regulatory machinery.[162] As a result, the vast majority of FOIA requests are made by businesses for commercial purposes.[163] Freedom of information acts turn agencies into information brokers instead of providing a window for public oversight of governmental operations.[164] Add the technological capability to relate disparate pieces of a person's information to this state of affairs and the stage is set for the data aggregation problem.

Viewed in isolation, each piece of information created by one's day-to-day activities is not at all telling; however, viewed in combination, that information begins to paint a portrait of that individual's personality.[165] This is the aggregation problem. It arises from the fact that integrated systems enable information from disparate sources to be easily collected and analyzed.[166] In a system such as this, information breeds information: information such as social security number, while not in and of itself informative, provides access to a host of additional information such as financial, educational, and medical records.[167]

Ultimately, the privacy committee should review the jurisdiction's freedom of information acts and any public access policies that would potentially provide electronic access to the data contained in the integrated justice system. The committee should discuss precisely how much information contained in an integrated justice system could reveal about a person as well as the role of privately compiled "biographies" during investigations and prosecutions of criminal activity.

When drafting policy for the sharing of justice information, the privacy committee may want to start from the perspective that all information is potentially available electronically. Such a perspective should lessen the member's reliance on practical obscurity. In essence, it removes practical obscurity from consideration as a privacy mechanism and requires the committee to confront exactly what information is contained in the justice system as well as its potential impact upon the lives of citizens if improperly released.

§ 3. FEDERAL AND STATE STATUTES & REGULATIONS

Since the 1970s, Congress has grappled with the problems of database privacy, accuracy, and completeness, but has been slow to take action.[168] Congress has been so slow, in fact, that its approach has been characterized as "reactive rather than anticipatory, incremental rather than comprehensive, and fragmented rather than coherent."[169] Congress has passed a series of statutes narrowly tailored to specific privacy problems.[170] The resulting patchwork of regulation contains significant gaps and omissions resulting in many laws but little privacy protection.[171]

What protection federal and state laws do afford individuals must, however, be analyzed and presented to the privacy committee for its review and discussion. Research staff must sort through the eclectic array of federal and state laws that may influence how and to what extent information can be shared seamlessly within an integrated justice system. Additionally, laws that contain public access provisions should also be reviewed for their impact on the integration initiative.

One of the goals of the integrated justice privacy policy is that it acts as a comprehensive collection of privacy directives for the integrated justice system—including its component agencies. This goal was formed because of the realization that an ad hoc approach to privacy legislation makes it difficult to determine whether the various statutes are collectively greater than the sum of their parts or more accurately mirror Humpty-Dumpty after the great fall. To achieve this goal, each relevant statute and regulation should be identified and analyzed. Furthermore, any case law that helps interpret the statutes should also be obtained to facilitate the committee's understanding of the current legal privacy environment.

Research should start by identifying federal legislation that requires states to comply with federal privacy policies and regulations. This represents the federal policy choices. Next, areas of privacy policy left to the discretion of the states should be identified and should correlate to state statutes and regulations. This represents the state's policy choices. These state statutes and regulations are often implemented at the local level through the use of agency-specific written guidelines. If state laws and regulations left some policy decisions to the local agencies, local policy choices would be found within the agency-specific guidelines. It is these privacy choices—federal, state, and local—that the integrated justice privacy policy should endeavor to follow. Where existing statutes, regulations, and guidelines fail to address a specific privacy issue, the privacy committee will need to make recommendations that operate in accordance with existing privacy policy choices and/or the fair information practices. Furthermore, the committee may make recommendations where the sharing of justice information is contemplated by existing regulations but the advent of systems integration alters the bases of those previous policy decisions.

The following is a substantial, but nevertheless partial, listing of federal and Illinois statutes and regulations.

Federal statutes and regulations

Generally, there are no blanket prohibitions on federal government access to publicly available information.[172]

Justice information

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968[173]
- Criminal justice information systems regulations[174]
- Criminal intelligence systems operating policies[175]
- USA PATRIOT Act of 2001[176]
- Homeland Security Act of 2002[177]
- Foreign Intelligence Surveillance Act of 1978[178]
- Attorney General's guidelines on general crimes, racketeering enterprise and domestic security/terrorism investigations
- Identity Theft & Assumption Deterrence Act of 1998[179]

Information contained in government information systems

- Privacy Act of 1974[180]
- Freedom of Information Act of 1974[181]
- Electronic Freedom of Information Act of 1996[182]
- Paperwork Reduction Act[183]
- E-Government Act of 2002[184]
- Privacy Protection Act of 1980[185]
- Federal Records Act of 1950[186]

Financial information

- Fair Credit Reporting Act of 1970[187]
- Right to Financial Privacy Act of 1978[188]
- Gramm-Leach-Bliley Act of 1999[189]
- Financial Modernization Services Act[190]
- Electronic Fund Transfer Act of 1978 and Regulation E[191]
- Provisions of the Internal Revenue Code that mandate the privacy of taxpayer information

Motor vehicle information

- Driver's Privacy Protection Act of 1994[192]

Education information

- Family Educational Rights and Privacy Act of 1974[193]

Telecommunications information

- Cable Communications Policy Act of 1984[194]
- Video Privacy Protection Act of 1988[195]
- Telecommunications Act of 1996[196]
- Electronic Communications Privacy Act of 1986[197]
- Children's Online Privacy Protection Act of 1998[198]
- Child Online Protection Act of 1998[199]
- Computer Matching and Privacy Protection Act of 1988[200]
- Telephone Consumer Protection Act of 1991[201]
- Counterfeit Access Device and Computer Fraud and Abuse Act[202]

Health information

- Health Insurance Portability and Accountability Act of 1996[203]

Illinois statutes and regulations

Justice information

- Criminal Identification Act[204]
- Firearm Owners Identification Card Act[205]
- Illinois Uniform Conviction Information Act[206]
- Department of State Police Law[207]
- Probation And Probation Officers Act[208]
- Statewide Organized Crime Database Act[209]
- Unified Code Of Corrections[210]
- Sex Offender & Child Murderer Community Notification Law[211]
- Sex Offender Registration Act[212]
- Sexually Violent Persons Commitment Act[213]
- Statewide Senior Citizen Victimizer Database Act[214]

Information contained in government information systems

- Illinois State Auditing Act[215]
- Vital Records Act[216]
- Freedom of Information Act[217]

Health information

- AIDS Confidentiality Act[218]
- Alcoholism & Other Drug Abuse & Dependency Act[219]
- Illinois Health Statistics Act[220]
- Department of Public Health Powers And Duties Law[221]
- Medical Patient Rights Act[222]
- Mental Health & Developmental Disabilities Code[223]
- Mental Health & Developmental Disabilities Confidentiality Act[224]

Juvenile information

- Abused And Neglected Child Reporting Act[225]
- Department of Children and Family Services Powers Law[226]
- Intergovernmental Missing Child Recovery Act of 1984[227]

Compile justice agencies' current policies

Either during or after the research staff's investigation into relevant federal and state laws, committee members should be requested to provide their various agencies' official information use policies. These policies should be reviewed for the ways in which they implement the statutorily required privacy practices. Some of these policies may also provide reliable language that can be utilized in the integrated justice privacy policy.

§ 4. POLICY CREATION: PRIVACY ISSUES & DESIRED PRACTICES

It is expected that the majority of integrated justice privacy policies are already written in the form of the many statutes and regulations already being implemented nation- and statewide. The challenge lies in compiling these diverse statutes and regulations into a single comprehensive document that can be easily referenced by justice practitioners.

Issues may exist that are not addressed by current statutes and regulations by virtue of the novel nature of integrated justice initiatives. Other issues will be familiar but contain greater levels of complexity when discussed in the integrated justice context. A brief discussion of the issues we expect to encounter follows. This discussion is by no means exhaustive and research staff are encouraged to meet with each stakeholder group to discuss the privacy issues that confront their agencies or associations.

A series of objectively prepared research papers should be prepared on each privacy issue in order to inform policy decisions. These research documents should be made part of the committee's final report and placed near the relevant sections of the privacy policy to demonstrate that the committee made informed policy decisions and, furthermore, that those policy decisions were purposeful.

Information life cycle

Historically, justice agencies faced with physical storage limitations developed policies for maintaining quantities of paper files out of practical necessity. Additionally, the utility of old documents was marginal as stored documents were not easily retrievable, even with detailed indexing systems.[228] With practically unlimited storage capabilities and the enhanced access, retrieval, and analysis of stored documents available in an integrated justice system, the decision on whether to keep or destroy records becomes a part of a privacy policy rather than a practical necessity.[229]

Furthermore, the General Assembly routinely makes policy decisions concerning the expungement and sealing of criminal history records. These statutes need to be referenced and their impact upon an integrated justice system examined. For instance, it is very likely that current expungement statutes, when applied to an integrated justice information system, would not lead to the total expungement of a criminal history record where the various data sources and repositories contained within the integrated system are not specifically referenced by the statute.

Information life cycle issues to be addressed

- What impact does the sealing of records have on the availability of information in the integrated justice system?
- What impact does the expungement of records have on the availability of information in the integrated justice system?
- Can a record *truly* be expunged?
- Is the secondary dissemination of information contained in the integrated justice system adequately addressed?
- If once a record becomes public it is forever public, then why does it matter how long public records are retained?
- Is the information life cycle more applicable to non-public information retention?

Individual access to records contained in integrated justice information systems

As previously discussed, several statutes already provide an individual with access to records concerning him that are contained in a government information system. Criminal history repositories funded with federal funds are required to provide an individual with access to his criminal history information.[230] Law enforcement data systems, however, tend not to allow an individual to access the data contained therein.[231] The privacy committee will need to determine what information contained in the integrated justice system the individual it relates to can access. This determination will most likely be based upon current practices revealed through an analysis of current statutes and regulations and the underlying policies they further.

Individual access issues to be addressed

- How quickly and how often should the integrated justice system provide the requested information to the data subject?
- In what form and manner should the information be provided to the requestor?
- Should this form and manner be standardized?
- How much of the information contained in the integrated justice system is considered to concern the individual?
- Does this information include how the information is being used, whether it is being used, and to whom the information is disclosed?
- What should the administrative standards for modifying an incorrect record be?

Accountability of the integrated justice system

Determining the accountability of the integrated justice system to the public is of significant importance to the privacy policy. Because the public bears the ultimate risk that personal information contained in the integrated justice system may be accessed or released inappropriately, causing possible loss of employment, diminished social status, or other adverse consequences, the integrated justice system should be held responsible for complying with the privacy policy.

The accountability provisions contained in current statutes and regulations should be researched and their current applicability to the integrated justice information system evaluated. In the instances where there is no current accountability, the privacy committee should develop accountability provisions to ensure compliance with the privacy policy.

Accountability issues to be addressed

- How do freedom of information acts (FOIAs) impact the operation of the integrated justice system?
- How do the First Amendment and common law access to court records affect the integrated justice system?
- Is there a presumption of public access to records contained in the integrated justice system? If so, to what extent does that presumption influence the privacy policy?
- How often should compliance audits be performed and who should perform those audits?
- What administrative procedures should be created to challenge the integrated justice system's compliance with the privacy policy? Would the individual need to suffer injury before he can challenge?
- What other recourses will an affected party have to affect redress of a violation of the privacy policy that harms him?

- Will the privacy policy or state law provide a civil cause of action for aggrieved individuals?
- Will the individual have to exhaust any administrative remedies first? What will those administrative remedies be?
- Will the state law make willful non-compliance with the privacy policy a crime?

Availability of statistical information made easily available by integrated justice information systems

Theoretically, an integrated justice information system can easily run reports of the transactional information generated by the criminal justice system. Statistical information such as the number of arrests, the number of times charges are brought or dropped, the number of convictions, guilty pleas, and acquittals, sentencing statistics (perhaps even indexed by judge), the number of prisoners released, and even recidivism rates could potentially be generated by the integrated justice information system. These pieces of statistical information may be very useful in the oversight of the justice system—oversight by justice policy makers and the general public.

First, it must be determined whether the integrated justice information system has these capabilities and, if not, whether it should have them. Second, provided the integrated justice system can generate these types of statistical reports, it must be determined whether those reports are of such a nature that they should or shouldn't be released. The Privacy Committee should examine current freedom of information acts for guidance and may also want to address the issue of whether the system should be made to generate specific reports upon a public request.

Accessibility of victim and witness information

In many cases, a crime victim's most fundamental need is for physical safety. To achieve physical safety, victims of crime need a broad range of relief—from privacy regarding the violence that occurred to confidential addresses and counseling. Victims of crime may forego legal protections if they are achieved at the expense of privacy. Fear about who might have access to police reports, pre-sentence investigations, victim compensation files, or victim impact statements may prevent victims from notifying authorities or participating in a criminal prosecution.

Victim and witness information issues to be addressed

- What is the purpose for collecting specific information from crime victims?
- What harm could come to the crime victim and her family if this information was disclosed to the offender or the public?
- In light of any identified risk, should this information be recorded at all?
- If the information is necessary to the function of the particular justice agency, what should that record contain and how should it be shared in an integrated justice system?

Accessibility of offender and victim health information

Health information collected by the justice system includes otherwise confidential medical and mental heath records. These records can include information ranging from a victim's HIV status to an offender's previous hospitalization in a mental institution. The privacy policy should address how these records concerning victims and offenders are collected and shared by the integrated justice system in order to ensure their appropriate use.

Collection, use, and dissemination of social security numbers

Information breeds information; although one's social security number does not in and of itself reveal much about an individual, it provides access to one's financial information, educational records, medical records, and a host of other information.[232] Social Security numbers are the currency of identity theft—one of the most rapidly escalating forms of crime. [233] The privacy policy should address where in the justice process Social security numbers are collected and disseminated by the integrated justice system to ensure their appropriate use.

C. THE FINAL REPORT

Briefly stated, the Privacy Committee will create a final report consisting of four components. First, the report should convey a strong understanding of the current status of federal and state privacy law. This understanding will include the identification of all relevant statutes and regulations, as well as an analysis of their accompanying case law.

Second, the report should include a summary of the research performed by committee staff as well as any policy research conducted by member agencies. Third, any significant policy deliberations transcribed during the course of the committee's meetings should also be included. Optimally, these discussions would be strategically positioned near the relevant portions of the privacy policy in order to provide context for the implementation of the privacy policy provisions.

Fourth, where appropriate, the final report should also include recommendations for amendments to current privacy statutes and regulations where the integrated justice information system operates outside the scope of their provisions but plainly should not.

The privacy policy will be integrated into the final report so that the supplementary supporting documentation can provide direction on how local agencies should implement the policy in practice. This also allows the final report to more fully explain the policy decisions contained therein. Explaining the rationale for a particular policy decision is important because it can aid in the resolution of future privacy issues that may not have been foreseen during the privacy policy's development. An un-annotated version of the privacy policy would also be provided in an appendix to the final report.

V.
CONCLUSION

"The greatest dangers to liberty lurk in the insidious encroachment by men of zeal, well-meaning but without understanding."[234] Justice Brandeis said this when he felt the court was looking only to the letter of the law and not its underlying policies. This paper has placed great emphasis on researching and analyzing the privacy policy choices already made in the area of justice information sharing. It is hoped that through this understanding, a committee charged with the overwhelming task of compiling a comprehensive privacy policy for an integrated justice system can address new privacy challenges in a manner consistent with existing policies.

[1]Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001, at A1. The Privacy Act of 1974 can be found at 5 U.S.C. § 552a. *See also* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1441 (2001) (stating that the Privacy Act of 1974 was a good beginning but criticizing its applicability only to federal agencies).

[2] S. REP. NO. 93-1183 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916.

[3] *Id*. To view an interesting, partial list of famous persons investigated by the FBI, including links to the documents contained in their FBI files, see http://foia.fbi.gov/famous.htm (last visited Jul. 6, 2004).

[4] Simpson, *supra* note 1.

[5] *Id*.

[6] Jim Krane, *Tracking U.S. Fugitives with Commercial Data*, CHICAGO DAILY LAW BULLETIN, Apr. 14, 2003, at 2.

[7] Simpson, *supra* note 1.

[8] *Id*.

[9] Ariana Eunjung Cha, *Pentagon Details New Surveillance System*, WASHINGTON POST, May 21, 2003, at A06. *See also* Steven M. Cherry, *TIA is Dead – Long Live TIA*, IEEE SPECTRUM ONLINE, Nov. 13, 2003, *at* http://www.spectrum.ieee.org/WEBONLY/resource/nov03/1103ntia.html (explaining that, while a joint House-Senate appropriations committee voted on September 24, 2003 to defund TIA through 2004, the committee allowed at least eight programs to continue under different agencies making some TIA projects even less visible and accountable than before).

[10] Jim McKay, *Big Brother: Is He Watching You?*, GOVERNMENT TECHNOLOGY, Apr. 2003, *available at* http://www.govtech.net/magazine/story.phtml?id=45918.

[11] Krane, *supra* note 6.

[12] *Report: LAPD let internal cases slide*, CNN.COM, May 19, 2003, *at* http://www.cnn.com/2003/US/West/05/19/police.corruption.ap/.

[13] *Police officer accused of selling celebrity date to tabloids*, USA TODAY, Apr. 9, 2003, *at* http://www.usatoday.com/tech/news/2003-04-09-policy-celebrity_x.htm.

[14] Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003). *See also* Peter Page, *Internet Data Seller Can Be Sued in Stalking-Murder Case*, LAW.COM, Mar. 10, 2003, *at* http://www.law.com/jsp/article.jsp?id=1046833530025.

[15] ILL. EXEC. ORDER NO. 16 (2003), *available at* http://www.illinois.gov/Gov/pdfdocs/execorder2003-16.pdf.

[16] ILLINOIS CRIMINAL JUSTICE INFORMATION AUTHORITY, IIJIS STRATEGIC PLAN 2003-2004 24-26 (2002), *available at* http://www.icjia.state.il.us/iijis/public/pdf/strategicplan_final.pdf (last visited Jul. 7, 2004).

[17] NATIONAL CRIMINAL JUSTICE ASSOCIATION, JUSTICE INFORMATION PRIVACY GUIDELINE 9 (2002), *available at* http://www.ncja.org/pdf/privacyguideline.pdf [hereinafter GUIDELINE].

[18] Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED NEWS, Jan. 26, 1999, *at* http://www.wired.com/news/politics/0,1283,17538,00.html.

[19] U.S. DEP'T OF JUSTICE, PUBLIC ATTITUDES TOWARD USES OF CRIMINAL HISTORY INFORMATION 4 (2001), *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/pauchi.pdf.

[20] *Id*. at 7.

[21] *Id*.

[22] Rob Reilly, *Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward*, 6 RICH. J.L. & TECH. 6, 7 (1999).

[23] Paul F. Kendall et al., *Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: The Need for Principles of Responsible Use*, 21st Annual International Conference on Data Protection and Information Privacy, Hong Kong 7-8 (Sept. 1999), *available at* http://www.pco.org.hk/english/infocentre/files/kendall(formatted).doc (last visited May 20, 2003).

[24] Eugene J. Yannon, *Privacy Law*, 34 MD. B.J. 24, 26 (2001).

[25] Kendall, *supra* note 23, at 1.

[26] Yannon, *supra* note 24.

[27] *Id.*

[28] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1098 (2002).

[29] Cherry, *supra* note 9.

[30] *See* Roy Mark, *Senate Wants Oversight of CAPPS II Program*, INTERNETNEWS.COM, Mar. 17, 2003, (visited June 5, 2003) http://www.internetnews.com/bus-news/article.php/2110391. On August 1, 2003, the Transportation Security Administration (TSA) announced the latest framework for the CAPPS II program, *see* 68 Fed. Reg. 45266 (Aug. 1, 2003). *But see* Jill D. Rhodes, *CAPPS II: Red Light, Green Light, or 'Mother, May I?'*, JOURNAL OF HOMELAND SECURITY (March 2004), *available at* http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=107 (stating that the announcement, even combined with the earlier CAPPS II announcement in 68 Fed. Reg. 2102 (Jan. 15, 2003), does not provide a clear understanding of the system and has led to more confusion than clarification about the workings of the CAPPS II program) (last visited Jul. 7, 2004).

[31] *See* Dave Lindorff, *Grounded*, SALON.COM, Nov. 15, 2002, *available at* http://www.salon.com/news/feature/2002/11/15/no_fly/print.html. *See also* U.S. GEN. ACCT. OFF., REPORT TO CONGRESSIONAL COMMITTEES ON AVIATION SECURITY: COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES, GAO-04-385, at 4, 20, 24-26, 41-44 (February 2004) [hereinafter GAO REPORT] (explaining that the Department of Homeland Security (DHS) and the TSA have not yet identified and addressed all privacy concerns nor have they developed and documented a process under which passengers impacted by CAPPS II can appeal decisions and correct erroneous information).

[32] Rhodes, *supra* note 30 (stating that CAPPS II is scheduled to be activated in August or September 2004, *but see* GAO REPORT *supra* note 31, at 9-13, which concludes that CAPPS II is behind schedule and that its new completion date is unknown).

[33] GAO REPORT, *supra* note 31, at 7; Rhodes, *supra* note 30.

[34] *See* Farad Manjoo, *FBI Analysis: We Don't Compute*, WIRED NEWS, May 30, 2002, *available at* http://www.wired.com/news/politics/0,1283,52853,00.html.

[35] Elliot Borin, *Feds Open 'Total' Tech Spy System*, WIRED NEWS, Aug. 7, 2002, *available at* http://www.wired.com/news/conflict/0,2100,54342,00.html.

[36] Ryan Singel, *Spy Plan Faces Critical Deadline*, WIRED NEWS, May 19, 2003, *available at* http://www.wired.com/news/politics/0,1283,58871,00.html. However, see Cherry, *supra* note 9 (explaining that eight TIA programs are funded and related research will be carried out by the National Foreign Intelligence Program (NFIP) whose budget is classified, as is the full definition of the work it is now authorized to develop).

[37] Mark, *supra* note 30. That report was completed in February 2004, *see GAO REPORT supra* note 31.

[38] *See* GUIDELINE, *supra* note 17, at 14. The Multistate Anti-Terrorism Information Exchange (MATRIX) is just one recent example of a justice information system that is losing support because of its failure to adequately address privacy concerns. *See* John Schwartz, *Privacy Fears Erode Support for a Network to Fight Crime*, N.Y. TIMES, Mar. 15, 2004 (stating that, while at its peak 16 states were members of the MATRIX program, all but 5 have withdrawn largely due to security and privacy concerns).

[39] U.S. DEP'T OF JUSTICE, *supra* note 19, at 4, 10.

[40] *Id.* at 7.

[41] GUIDELINE, *supra* note 17, at 52.

[42] *See infra* Part IV, B §3.

[43] U.S. DEP'T OF JUSTICE, *supra* note 19, at 38.

[44] *Id*. at 39.

[45] *Id*. at 8. *See* U.S. DEP'T OF JUSTICE, REPORT OF THE NATIONAL TASK FORCE ON PRIVACY, TECHNOLOGY, AND CRIMINAL JUSTICE INFORMATION 2001, *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/rntfptcj.pdf (last visited Jul. 7, 2004).

[46] U.S. DEP'T OF JUSTICE, *supra* note 19, at 8.

[47] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1120 (2002).

[48] *See infra* Part IV §B(2).

[49] Reilly, *supra* note 22, at 15.

[50] Yannon, *supra* note 24, at 29.

[51] Such as practical obscurity discussed *infra* Part IV §B(3).

[52] *Olmstead*, 277 U.S. 438 (1928).

[53] *Id*. at 465.

[54] Solove, *Conceptualizing Privacy*, *supra* note 47, at 1146.

[55] *Id*. S*ee also* Katz v. United States, 389 U.S. 347 (1967) (holding, finally, that the Fourth Amendment did apply to wiretapping).

[56] Solove, *Conceptualizing Privacy*, *supra* note 47, at 1090.

[57] Yannon, *supra* note 24, at 24.

[58] Solove, *Conceptualizing Privacy*, *supra* note 47, at 1093.

[59] *Id*. at 1093-1094, 1145-1146.

[60] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1212 (1998); *and* Solove, *Conceptualizing Privacy*, *supra* note 47, at 1148. *See also,* Benitez v. KFC National Management Co., 714 N.E.2d 1002 (Ill. App. 2d Dist. 1999). This case demonstrates the dangers of not understanding this value of privacy. In *Benitez*, the court held that allegations that the defendants took pictures of the plaintiffs in the restroom and described the plaintiffs' body parts to others were *not* the focus of the plaintiffs' invasion of privacy claim and had it not been for *additional* allegations of voyeurism, the court "would be reluctant to classify [the defendants'] conduct as invasion of privacy at all." *Id*. at 1006.

[61] Solove, *Conceptualizing Privacy*, *supra* note 47, at 1148.

[62] Kang, *supra* note 60, at 1213 (*citing* Charles Fried, *Privacy*, 77 YALE L.J. 475, 484-485 (1968)).

[63] *Id*. at 1213.

[64] *Id*. (*noting* Richard A. Wasserstrom, *Privacy: Some Arguments and Assumptions*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 317, 324 (Ferdinand David Schoeman ed., 1984)).

[65] *Id*. at 1214.

[66] *Id*. at 1216.

[67] *Id*. at 1216-1217.

[68] Solove, *Conceptualizing Privacy*, *supra* note 47, at 1143-1144.

[69] *Id*. at 1138.

[70] *Id*. at 1144; *see* Frisby v. Schultz, 487 U.S. 474 (1988) (finding constitutional an ordinance prohibiting picketing on public streets in front of a specific residence because privacy interests are of the highest order and people are captive audiences in their homes).

[71] Kang, *supra* note 60, at 1203-1204. These clusters are interconnected and often simultaneously implicated by the same event or practice. *See* Kendall, *supra* note 23, at 2 n3 (stating that an argument can be made that where a state violates an individual's privacy by disclosing personal information about that individual to the public, the state has deprived the individual of the opportunity to define him or herself; this example implicates both decisional and information clusters simultaneously).

[72] Kang, *supra* note 60, at 1202.

[73] Solove, *Conceptualizing Privacy*, *supra* note 47, at 1101 (*quoting* Time Inc. v. Hill, 385 U.S. 374, 413 (1967) (Fortas, J., dissenting) Justice Fortas was expanding on the famous definition of privacy as "the right to be let alone" (formulated in Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890))).

[74] Kang, *supra* note 60, at 1202; *see* California v. Ciraolo, 476 U.S. 207, 212-213 (1986) (stating that "the protection afforded to curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened").

[75] *See* Griswold v. Connecticut, 381 U.S. 479, 485-486 (1965) (holding that a law criminalizing the use of contraceptives by married couples intruded on the right of marital privacy protected by the Constitution); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (extending *Griswold* to the use of contraceptives by non-married individuals and holding that the right to privacy includes the right to decide whether or not to bear or beget a child); and Roe v. Wade, 410 U.S. 113 (1973) (finding that the constitutional right to privacy encompasses the decision to procure an abortion).

[76] Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 838 (1992) (stating, more eloquently: "These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State." *Id*. at 859).

[77] Under this view, privacy is violated by the public disclosure of previously concealed information. However, this view of privacy often leads to the conclusion that once a fact is divulged to the public, no matter how limited or narrow the disclosure, it can no longer remain private. Meaningful discussion of privacy requires the recognition that ordinarily we are interested in selective disclosure, not total secrecy. Solove, *Conceptualizing Privacy*, *supra* note 47, at 1107-8.

[78] Kang, *supra* note 60, at 1205 (*quoting* President Clinton's INFORMATION INFRASTRUCTURE TASK FORCE (IITF), PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION 5 (1995)).

[79] *Id*. at 1206.

[80] *Id*.

[81] *Id*.

[82] *Id*.

[83] *Id*.

[84] *Id.* at 1208.

[85] *Id*.

[86] Solove, *Conceptualizing Privacy*, *supra* note 47, at 1154.

[87] *See infra* Part IV §B(2).

[88] GUIDELINE, *supra* note 17.

[89] *Id*. at 9.

[90] *Id*. at 16.

[91] *Id*. at 36.

[92] Solove, *Conceptualizing* Privacy, *supra* note 47, at 1154; *see also infra* Part III.

[93] GUIDELINE, *supra* note 17 at 22.

[94] *See* U.S. Dep't of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 764 (1989) [hereinafter "Reporters Committee"].

[95] U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973) xx-xxi, *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm (last visited Jan. 27, 2003).

[96] *Id*.

[97] *Id*.

[98] 5 U.S.C. § 552a.

[99] 20 U.S.C. § 1232g; *see* Solove, *Privacy and Power*, *supra* note 1 (pointing out the narrow scope of the statute and the exclusions for records maintained by school law enforcement officials and health and psychological records).

[100] 18 U.S.C. § 2710; *see* Solove, *Privacy and Power*, *supra* note 1, at 1442 (criticizing the fact that the restrictions are not extended to bookstores, record stores, or any other type of retailer, magazine producer, or catalog company).

[101] 42 U.S.C. § 1320d to 1320d-8 (2002); *see generally* Peter A. Winn, *Confidentiality in Cyberspace: the HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617 (2002).

[102] GUIDELINE, *supra* note 17, at 22.

[103] Kendall, *supra* note 23, at 16.

[104] GUIDELINE, *supra* note 17, at 19.

[105] Kendall, *supra* note 23, at 2 (using "virtual picture" nomenclature in place of Professor Solove's "digital biography"); *see generally* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002).

[106] Barbara Crutchfield George, et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 752 (2001).

[107] *Id*.

[108] Kang, *supra* note 60, at 1206-1208; *see infra* Part III §B.

[109] George, *supra* note 106, at 753.

[110] *Id*. at 752-753.

[111] *Id*. at 754.

[112] GUIDELINE, *supra* note 17, at 27.

[113] *Id*. at 25-26.

[114] *Id*. at 27.

[115] *Id*.

[116] *See* 68 Fed. Reg. 4974, (Jan 31, 2003) (to be codified at 28 C.F.R. pt 16).

[117] GUIDELINE, *supra* note 17, at 29.

[118] *Id*.

[119] George, *supra* note 106, at 759; *see also* Solove, *Privacy and Power*, *supra* note 1, at 1426-1427 (noting that "The choices given to people over their information are hardly choices at all. People must relinquish personal data to gain employment, procure insurance, obtain a credit card, or otherwise participate like a normal citizen in today's economy. Consent is virtually meaningless in many contexts.")

[120] *See infra* Part IV B §3.

[121] While not addressing this precise question, Paul v. Davis, 424 U.S. 693 (1976) contains a factually similar situation.

[122] George, *supra* note 106, at 754.

[123] *See* GUIDELINE, *supra* note 17, at 26.

[124] *Id*. at 28.

[125] *Id*. at 28 n29.

[126] *Id*. at 28.

[127] *Id*. at 31.

[128] *See infra* Part IV, B §1 (FIP1.)

[129] *See* George, *supra* note 106, at 756.

[130] GUIDELINE, *supra* note 17, at 32.

[131] George, *supra* note 106, at 756

[132] GUIDELINE, *supra* note 17 at 32.

[133] *Id*. at 33.

[134] *Id*.

[135] 28 C.F.R. § 20.21(g).

[136] George, *supra* note 106, at 757.

[137] *Id*.

[138] *See infra* Part IV B §1(FIP4).

[139] ALAN HARBITTER & JEFF LANGFORD, IJIS INDUSTRY WORKING GROUP, INFORMATION SECURITY IN INTEGRATED JUSTICE APPLICATIONS, 1 (2002), *available at* http://it.ojp.gov/global/security/infosec4ijis3-19-02.pdf (last visited May 29, 2003)

[140] *Id*.

[141] GUIDELINE, *supra* note 17, at 30.

[142] *Id*.

[143] HARBITTER, *supra* note 139, at 3-15.

[144] GUIDELINE, *supra* note 17, at 34.

[145] *See* Ramos v. City of Peru, 775 N.E.2d 184, 187-188 (Ill. App. 3d Dist. 2002) (holding that the Illinois Uniform Conviction Information Act clearly contemplates that aggrieved individuals may pursue judicial remedies against state agencies and units of local governments for negligent dissemination of inaccurate or incomplete conviction information).

[146] GUIDELINE, *supra* note 17, at 16.

[147] *Id*.

[148] Solove, Access and Aggregation, *supra* note 105, at 1178; *see also* Jonathan Franzen, *Imperial Bedroom*, *in* HOW TO BE ALONE: ESSAYS 39-54 (2002).

[149] Solove, *Access and* Aggregation, *supra* note 105, at 1139.

[150] *Id*.

[151] Lewis A. Kaplan, *Litigation, Privacy and the Electronic Age*, 4 YALE SYMP. ON L. & TECH. 1 (2001).

[152] Amy Harmon, *As Public Records Go Online, Some Say They're Too Public*, N.Y. TIMES, Aug. 24, 2001, Late Edition- Final § A at 1, (*quoting* the Honorable John W. Lungstrum, chief judge of the Federal District Court in Kansas).

[153] *Id*.; Reporters Committee, 489 U.S. 749 (1989).

[154] 489 U.S. 749.

[155] *Id*. at 764.

[156] Harmon, *supra* note 152.

[157] Reporters Committee, 489 U.S. at 764.

[158] Solove, *Access and Aggregation*, *supra* note 105, at 1161 (*citing* Fred H. Cate et al., *The Right to Privacy and the Public's Right to Know: The "Central Purpose" of the Freedom of Information Act*, 46 ADMIN. L. REV. 41, 65 (1994)).

[159] Victoria S. Salzmann, *Are Public Records Really Public?: The Collision Between the Right to Privacy and the Release of Public Court Records Over the Internet*, 52 BAYLOR L. REV. 355, 357 (2000).

[160] Solove, *Access and Aggregation*, *supra* note 105, at 1160.

[161] *Id*. at 1195-1196.

[162] *Id*. at 1196.

[163] *Id*.

[164] Salzmann, *supra* note, 159 at 358; *see also* Solove, *Access and Aggregation*, *supra* note 105, at 1196.

[165] Solove, *Access and Aggregation*, *supra* note 105, at 1185.

[166] *Id*.

[167] *Id*.

[168] Solove, *Privacy and Power*, *supra* note 1, at 1440.

[169] *Id*. at 1444 (*citing* Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 99, 113 (Philip E. Agre & Marc Rotenberg eds., 1997)).

[170] *Id*. at 1440.

[171] *Id*. at 1444.

[172] GINA MARIE STEVENS, CONGRESSIONAL RESEARCH SERVICE, PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS 4 (2003).

[173] 42 U.S.C. 3711, *et seq*., as amended by the Crime Control Act of 1973, 28 U.S.C. 534, Pub. L. 90–351, Pub. L. 91–644, Pub. L. 92–544, Pub. L. 93–83, Pub. L. 93–415, Pub. L. 94–430, Pub. L. 94–503, Pub. L. 95–115, Pub. L. 96–157, Pub. L. 98–473, Pub. L. 99–570, Pub. L. 100–690, and Pub. L. 101–647. The federal wiretapping and electronic eavesdropping statute permits federal and state law enforcement officers to use wiretapping and electronic eavesdropping under strict limitations. 18 U.S.C. 2510, *et seq*. Criminal, civil, and administrative sanctions are available for illegal interception, and evidence secured through an unlawful interception may be declared inadmissible in subsequent judicial or administrative proceedings. STEVENS, *supra* note 172, at 12.

[174] 28 C.F.R. pt. 20. Criminal justice information systems regulations are promulgated to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.

[175] 28 C.F.R. pt. 23. Recognizing that certain criminal activities involve some degree of regular coordination and permanent organization involving participants over broad geographical areas, justice agencies often collect and exchange intelligence data necessary to expose such criminal networks. The Criminal Intelligence Systems Operating Policies have been promulgated to assure that systems containing criminal intelligence data are utilized in conformance with the privacy and constitutional rights of individuals.

[176] Pub. L. No. 107-56, § 202 (Oct. 26, 2001). The USA PATRIOT Act substantively amended Title III of the Omnibus Crime Control and Safe Streets Act, the Electronic Communications Privacy Act, and the Foreign Intelligence Surveillance Act of 1978 and authorized the disclosure of wiretap and grand jury information to "any federal, law enforcement, intelligence, protective, immigration, national defense, or national security official" for the performance of his duties.

[177] Pub. L. No. 107-296 (Nov. 25, 2002). The Homeland Security Act also amended Title III of the Omnibus Crime Control and Safe Streets Act, the Electronic Communications Privacy Act, and the Foreign Intelligence Surveillance Act of 1978, this time to authorize sharing the results of the federal government's information gathering efforts under those statutes with relevant foreign, state and local officials.

[178] 50 U.S.C. §§ 1861-1863. The Foreign Intelligence Surveillance Act governs the use of wiretapping to collect "foreign intelligence" which is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." Unlawful surveillance is subject to criminal, civil, and administrative sanctions, and evidence illegally secured may be suppressed. STEVENS, *supra* note 172, at 12.

[179] Pub. L. No. 105-318 (Oct. 30, 1998).

[180] 5 U.S.C. § 552a. Congress' most significant piece of privacy legislation of the 1970s, the Privacy Act of 1974, was implemented to protect the privacy of individuals identified in information systems maintained by federal executive branch agencies by controlling the collection, use, and sharing of that information. The act restricts disclosure of personally identifiable records maintained by agencies; grants individuals increased rights of access to agency records maintained on themselves; grants individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete; and establishes a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records. STEVENS, *supra* note 172 at 6.

[181] 5 U.S.C. § 552.

[182] Pub. L. No. 104-231 (Oct. 2, 1996). *See generally,* Salzmann, *supra* note 159, at 358-359.

[183] 44 U.S.C. §§ 3501-3521.

[184] Pub. L. No. 107-347 (Dec. 7, 2002), 116 Stat. 2899.

[185] Pub. L. No. 96-440 (Oct. 13, 1980) (codified at 42 U.S.C. § 2000aa (1981)).

[186] 64 Stat. 583.

[187] 15 U.S.C. § 1681. Inspired by allegations of abuse and lack of responsiveness of credit agencies, the Fair Credit Reporting Act sets forth rights for individuals and responsibilities for consumer "credit reporting agencies" in connection with the preparation and dissemination of personal information in a consumer report. The act, however, permits credit reporting agencies to sell the "credit header" portion of credit histories that contain names, addresses, former addresses, telephone number, Social Security number, employment information, and date of birth. Solove, *Privacy and Power*, *supra* note 1, at 1440-1441.

[188] 12 U.S.C. §§ 3414-3422. In response to the 1976 decision of the Supreme Court in United States v. Miller, 425 U.S. 435 (1976) (holding that individuals have no Fourth Amendment "expectation of privacy" in records maintained by their banks), Congress enacted the Right to Financial Privacy Act which sets forth procedures for the federal government's access to financial institution customer records. RFPA covers the records of individuals who are customers of banks, thrifts, credit unions, credit card issuers, and consumer finance companies and requires the government to obtain valid subpoenas, summons, or warrants before the information can be released. STEVENS, *supra* note 172, at 15.

[189] Pub. L. No. 106-202 (May 18, 2000), 113 Stat. 1338, (codified at 15 U.S.C. §§ 6801-6809 (2001)). The Gramm-Leach-Bliley Act permits banks, insurers, and investment companies that are affiliated to share the "nonpublic personal information" that each affiliate possesses. Affiliates must inform customers that they are sharing this information but there is no way for individuals to block this sharing of information. Solove, *Privacy and Power*, *supra* note 1, at 1443-1444. Exceptions permit sharing of such information in

response to judicial process; as permitted or required under other provisions of law, and in accordance with the Right to Financial Privacy Act; and to provide information to law enforcement agencies, or for an investigation on a matter of public safety. STEVENS, *supra* note 172, at 15.

[190] Pub. L. No. 106-102 (Nov. 12, 1999).

[191] 12 C.F.R. § 205.11 (1996).

[192] 18 U.S.C. § 2721. The Driver's Privacy Protection Act of 1994 finally addressed the longstanding practice of many states of selling personal information in their motor vehicle records to marketers forcing states to acquire a driver's consent before making such a disclosure. The personal information regulated by the act includes an individual's photograph, Social Security number, driver identification number, name, address, telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status. STEVENS, *supra* note 172, at 11.

[193] 20 U.S.C. § 1232g. The Family Educational Rights and Privacy Act of 1974, also known as the "Buckley Amendment," governs the accessibility and disclosure of personally identifiable information in educational records held by federally funded educational institutions and agencies. STEVENS, *supra* note 172, at 8; Solove, *Privacy and Power*, *supra* note 1, at 1441. Excluded from the act are records maintained by school law enforcement officials as well as health and psychological records. *Id*.

[194] 47 U.S.C. § 551. The Cable Communications Policy Act of 1984 limits the disclosure of cable television subscriber names, addresses, and viewing habits and is enforced with a private cause of action.

[195] 18 U.S.C. § 2710. After reporters obtained Supreme Court Justice nominee Robert Bork's videocassette rental data, Congress passed the Video Privacy Protection Act of 1988, which has also become known as the "Bork Bill." The act prohibits videotape service providers from knowingly disclosing their customers' names, addresses, and specific videotapes rented or purchased without consent and provides a private cause of action for disclosures in violation of its terms. Solove, *Privacy and Power*, *supra* note 1, at 1442 (criticizing the fact that the restrictions are not extended to bookstores, record stores, or any other type of retailer, magazine producer, or catalog company).

[196] 47 U.S.C. § 222. The Telecommunications Act of 1996 limits the use and disclosure of customer proprietary network information (CPNI) by telecommunications service providers. CPNI is information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, and includes information contained in the bills pertaining to telephone exchange service or telephone toll service, but does not include subscriber list information. STEVENS, *supra* note 172, at 9.

[197] 18 U.S.C. §§ 2510-2522. The focus of the Electronic Communications Privacy Act is on eavesdropping and monitoring of communications. The act extends the protections of the Federal Wiretap Act of 1968 to new forms of voice, data, and video communications, including cellular phones, and e-mail or other computer transmissions. Solove, *Privacy and Power*, *supra* note 1, at 1441.

[198] 15 U.S.C. §§ 6501-6506. The first federal law directly addressing privacy in cyberspace, the Children's Online Privacy Protection Act, regulates the collection of children's personal information on the Internet. Websites targeted at children must post privacy policies and must obtain parental consent for the collection, use or disclosure of personal information from children. Solove, *Privacy and Power*, *supra* note 1, at 1443. Parental consent is not required for the operator of such a website or online service to collect, use, or disclose such information to respond to judicial process; or to provide information, to the extent permitted under other laws, to law enforcement agencies or for an investigation on a matter related to public safety. STEVENS, *supra* note 172, at 15-16.

[199] Pub. L. No. 105-277, Div. C, Title XIV, § 1401, (Oct. 21, 1998), 112 Stat. 2681-736.

[200] Pub. L. No. 100-503 (Oct. 18, 1988).

[201] Pub. L. No. 102-243 (Dec. 20, 1991), 105 Stat. 2394 (codified at 47 U.S.C. 227 et seq.).

[202] 18 U.S.C. § 1030.

[203] Pub. L. No. 104-191 § 264 (Aug. 21, 1996) (codified at 42 U.S.C. § 1320d). The Health Insurance Portability and Accountability Act ("HIPAA") of 1996 required the Department of Health and Human Services to promulgate regulations to govern the privacy of medical records. The regulations were issued and require authorization for all uses and disclosures of medical records beyond those for treatment, payment, or healthcare operation. Solove, *Privacy and Power*, *supra* note 1, at 1443.

[204] 20 ILL. COMP. STAT. 2630/1-2630/13 (*implemented by* ILL. ADMIN. CODE tit. 20 §§ 1210, 1240, 1265).

[205] 430 ILL. COMP. STAT. 65/1-65/13-3.

[206] 20 ILL. COMP. STAT. 2635/1-2635/34, (*implemented by* ILL. ADMIN. CODE tit. 20 § 1215).

[207] 20 ILL. COMP. STAT. 2605/2605-1-2605/2605-555.

[208] 730 ILL. COMP. STAT. 110/9-110/17.

[209] 20 ILL. COMP. STAT. 2640/1-2640/20.

[210] 730 ILL. COMP. STAT. 5/1-1-1 – 5/1-1-2, (*implemented by* ILL. ADMIN. CODE tit. 20 §§ 107, 701, 720, 1285).

[211] 730 ILL. COMP. STAT. 152/101-152/199, (*implemented by* ILL. ADMIN. CODE tit. 20 § 1282).

[212] 730 ILL. COMP. STAT. 150/1-150/12, (*implemented by* ILL. ADMIN. CODE tit. 20 § 1280).

[213] 725 ILL. COMP. STAT. 207/1-207/99.

[214] 20 ILL. COMP. STAT. 2645/1-2645/15.

[215] 30 ILL. COMP. STAT. 5/1-1 – 5/1-20.

[216] 410 ILL. COMP. STAT. 535/1-535/49, (*implemented by* ILL. ADMIN. CODE tit. 77 § 500).

[217] 5 ILL. COMP. STAT. 140/1-140/11.

[218] 410 ILL. COMP. STAT. 305/1-305/16.

[219] 20 ILL. COMP. STAT. 301/1-1-301/1-10, (*implemented by* ILL. ADMIN. CODE tit. 77 § 2030).

[220] 410 ILL. COMP. STAT. 520/1-520/11, (*implemented by* ILL. ADMIN. CODE tit. 77 § 1005).

[221] 20 ILL. COMP. STAT. 2310/2310-1 – 2310/2310-605.

[222] 410 ILL. COMP. STAT. 50/1-50/99.

[223] 405 ILL. COMP. STAT. 5/1-100 - 5/1-129.

[224] 740 ILL. COMP. STAT. 110/1-110/17.

[225] 325 ILL. COMP. STAT. 5/1-5/11.7.

[226] 20 ILL. COMP. STAT. 510/510-1 – 510/510-200.

[227] 325 ILL. COMP. STAT. 40/1-40/8, (*implemented by* ILL. ADMIN. CODE tit. 20 § 1260).

[228] GUIDELINE, *supra* note 17, at 42.

[229] *Id*.

[230] *See* Criminal Justice Information Systems Regulations, 28 C.F.R. part 20.34.

[231] *See* Law Enforcement Agencies Data System (LEADS) Regulations, ILL. ADMIN. CODE tit. 20 § 1240.30.

[232] Solove, *Access and* Aggregation, *supra* note 105, at 1185.

[233] *Id*. at 1191.

[234] Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).