U.S. Department of Justice
Office of Justice Programs

Bureau of Justice Statistics

Report of the National Task Force on Privacy, Technology, and Criminal Justice Information

Law and policy
Change drivers
Recommendations

Privacy, Technology, and Criminal Justice Information

U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Statistics

Report of the National Task Force on Privacy, Technology, and Criminal Justice Information

August 2001, NCJ 187669

Report of the work prepared under Cooperative Agreement number 96-BJ-CX-K010, awarded to SEARCH Group, Incorporated, 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831. Contents of this document do not necessarily represent the views or policies of the Bureau of Justice Statistics or the U.S. Department of Justice.

U.S. Department of Justice
Bureau of Justice Statistics

Lawrence A. Greenfeld
Acting Director

Acknowledgments. This report was prepared by SEARCH, The National Consortium for Justice Information and Statistics, Kenneth E. Bischoff, Chair, and Gary R. Cooper, Executive Director. The project director was Sheila J. Barton, Deputy Executive Director. Robert R. Belair, SEARCH General Counsel, wrote this report. Kevin L. Coy, Associate, Mullenholz, Brimsek & Belair, assisted in its preparation. Twyla R. Cunningham, Manager, Corporate Communications, and Linda B. Townsdin, Writer/Editor, edited this report, and Jane L. Bassett, Publishing Specialist, provided layout and design assistance. The Federal project monitor was Carol G. Kaplan, Chief, Criminal History Improvement Programs, Bureau of Justice Statistics.

Report of work prepared under Cooperative Agreement number 96-BJ-CX-K010, awarded to SEARCH Group, Incorporated, 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831. Contents of this document do not necessarily represent the views or policies of the Bureau of Justice Statistics or the U.S. Department of Justice.

Contents

I. Introduction and executive summary

Rationale for Bureau of Justice Statistics and SEARCH project

In 1998, the Bureau of Justice Statistics (BJS) in the Office of Justice Programs (OJP), U.S. Department of Justice, and SEARCH, The National Consortium for Justice Information and Statistics,[1] determined that the time was appropriate to conduct a comprehensive project[2] to review the law and policy addressing the collection, use, and dissemination of criminal justice record information and, particularly, criminal history record information (CHRI).[3]

In the mid-1970s and again in the mid-1980s, BJS and its predecessor organizations, along with SEARCH, had looked closely and comprehensively at this very issue. Those reviews:

- Concluded that CHRI should not be made available to the general public.
- Recognized that there are some legitimate, noncriminal justice uses of CHRI (for example, for background checks for positions of trust).
- Recognized a sharp distinction between arrest-only and conviction information, and recommended more relaxed rules for the dissemination of conviction information.
- Strongly endorsed the view that CHRI should be made available for various noncriminal justice purposes only after a search conducted on the basis of fingerprints.
- Recommended that various privacy and fair information practice protections should attach to the handling of CHRI, including a right on the part of the record subject to see and correct the record.

Those efforts and recommendations by BJS and SEARCH made a direct contribution to the development of law and policy for the handling of CHRI in all 50 States.

By the late 1990s, however, it had become apparent that changes in technology, as well as in the public's attitude about access to information and privacy, made it appropriate and important to take a new look at CHRI law and policy. In particular, the existing CHRI law takes a "smokestack" approach: one body of law for the comprehensive CHRI maintained by law enforcement at a central State repository (sometimes referred to as a "rap sheet"); an entirely separate body of law regulating the dissemination and use of the very same records (albeit, not as comprehensive or complete) maintained in the courts; another separate body of law and policy for the collection, use, and dissemination of this information by various commercial compilers; and a different set of laws for the media's handling of this information. This smokestack approach, combined with an eruption of public concern about privacy, and further combined with a necessary and constructive effort sweeping the Nation to integrate criminal justice and other governmental information systems, set the scene for an in-depth review of CHRI law and policy.

---

[1]Hereafter, SEARCH.

[2]The project was funded by and operated under the auspices of the Bureau of Justice Statistics (BJS). Since its inception, BJS has taken a leadership role in the improvement of criminal history record information and the development of appropriate policies for handling this information. SEARCH is a State criminal justice support organization comprised of one governor's appointee from each State, the District of Columbia, and the territories of Puerto Rico and the U.S. Virgin Islands, as well eight at-large Members selected by the SEARCH Chair. For over 3 decades, SEARCH has promoted the effective and appropriate use of information, identification, and communications technology for State and local criminal justice agencies. For the same period of time, SEARCH has been vitally concerned with the privacy and public access implications of the automation and use of personally identifiable criminal justice record information.

[3]CHRI consists of arrest and conviction information, as well as other types of disposition information.

Goals and deliverables

The goal of BJS and SEARCH was to craft a road map for the development of a new generation of CHRI law and policy. Specifically, the BJS/SEARCH effort consists of four deliverables:

1. This report**,** which analyzes existing law and policy for handling CHRI; identifies the technological and societal developments that may be changing the criminal justice privacy environment; and makes initial recommendations to address the next generation of criminal justice information law and policy.
2. A first-ever, public opinion survey about public access to CHRI undertaken by the Opinion Research Corporation and Dr. Alan F. Westin.[4]
3. A national conference — the proceedings of which will be published separately — to address and highlight emerging criminal justice information privacy issues, which was held in Washington, D.C., on May 31 and June 1, 2000.
4. Targeted standards applying the recommendations of the National Task Force on Privacy, Technology and Criminal Justice Information,[5] as set forth in this report, to specific types of criminal justice record information and integrated systems. Work in this area began with the development of design principles for safeguarding the privacy of personal information in integrated criminal justice systems (to be published separately). Additional projects to promote the next generation of criminal justice information privacy law and policy recommended in this report are under development.

To assist in conducting the project, BJS and SEARCH convened a Task Force of preeminent academics, criminal justice officials (including representatives from law enforcement, the courts, corrections, and prosecution), private-sector compilers and resellers of criminal justice record information, the media, and the criminal justice record user community.[6] The Task Force held three, multiple-day meetings: Asilomar in Pacific Grove, California, on January 13-14, 1999; Boston, Massachusetts, on May 11-12, 1999; and Victoria, British Columbia, Canada, on October 18-19, 1999. The observations and recommendations in the report reflect the Task Force's consensus views, but do not necessarily reflect the views of any particular member of the Task Force or of his or her institutional affiliations.

Key factors changing the criminal history record information environment

The Task Force identified the following technological, cultural, economic, and other "change drivers" that are moving the Nation toward a new information environment and impelling the consideration of new criminal justice record information privacy policies.

- **Public concern about privacy**. In the late 1990s, the American public registered the strongest concerns ever recorded about threats to their personal privacy from both government and business. In a 1999 study conducted by Dr. Alan F. Westin, 94 percent of respondents said they are concerned about the possible misuse of their personal information. Of the concerned, 77 percent said they were "very concerned."
- **The "Information Culture."** A new and emerging culture of information access and use facilitated by personal computers, browsers, search engines, online databases, and the Internet, has helped to create a demand for, and a market in, information, including criminal justice information,

[4]The summary results of this survey, along with interpretive commentary, is being published separately by BJS in a forthcoming companion report titled "Privacy, Technology and Criminal Justice Information: Public Attitudes Toward Uses of Criminal History Information, Summary of Survey Findings," (NCJ 187633). Hereafter, Privacy Survey Report.

[5]Hereafter, Privacy Task Force or Task Force.

[6]Biographies of Task Force participants are included as Appendix 1.

while, at the same time, fostering in many a sense of lack of control over one's personal information and a loss of privacy.

- **Technological change**. Revolutionary improvements in information, identification, and communications technologies (including increasingly advanced software applications and Internet-based technologies), and the increased affordability of these technologies fuels the appetite for information and creates new players in the criminal justice information arena.
- **System integration**. Initiatives to integrate criminal justice information systems operated by law enforcement, courts, prosecution, and corrections, as well as initiatives to integrate these systems with information systems maintaining other types of personal information, create powerful new information resources. At the same time, these integration initiatives may create uncertainty about the types of privacy laws and policies that apply to these new systems and which dilute existing policies designed to keep information separate.
- **New approach that closely resembles a "Business Model" for the criminal justice system**. Two fundamental changes in the way the criminal justice system operates have had a profound impact upon the approach that criminal justice agencies take toward obtaining and using information — a "data-driven, problem-solving approach." These changes are: a new, more cooperative, community-based relationship between criminal justice agencies and citizens; and added criminal justice agency responsibilities to provide information to surrounding communities, Federal, State, and local agencies, other police departments, and other organizations. This new approach also creates privacy risks through a wider circulation of criminal justice information.
- **Noncriminal justice demand**. A persistent and ever-increasing demand by noncriminal justice users to obtain CHRI has had a pervasive and important impact on the availability of information.
- **Commercial compilation and sale**. Changes in the information marketplace — which feature the private sector's acquisition, compilation, and sale of criminal justice information obtained from police and, more particularly, court-based open record systems — are making information similar to that found in criminal history records more widely available to those outside the criminal justice system.
- **Government statutes and initiatives**. A host of new government initiatives and laws, aimed at providing criminal justice information to broader audiences, on a more cost-effective and timely basis, has also fueled the availability of criminal justice information.
- **Juvenile justice reform**. Demands for juvenile justice records, particularly those involving violent offenses that result in treating juvenile information in a way which very much resembles the handling of adult records, is also putting pressure on traditional information and privacy policies.
- **Intelligence systems**. Criminal justice intelligence systems are being automated, regionalized, and armed with CHRI and other personal information to create detailed personal profiles for law enforcement use.

Content of project report

This project report begins with a review of information privacy law and policy. The report identifies five interests critical to a democracy and that are served by information privacy: (1) due process and fairness, (2) individual dignity, (3) individual autonomy, (4) oversight and trust in governmental institutions, and (5) the promotion of privacy-dependent relationships.

In reviewing the history of information privacy, the report describes the development of the code of fair information practices in the early 1970s, a code that continues to shape both U.S. and worldwide privacy policy to this day.

The report provides further background information with an overview of the criminal justice information system structure. The report describes the Nation's system for the interstate exchange of CHRI, including the role of the Federal Bureau of Investigation (FBI), the central State repositories of CHRI, the Interstate Identification Index (III), the National Crime Prevention and Privacy Compact (which establishes formal procedures and governance structures for noncriminal justice use of the III), and the Compact Council. The report also enumerates the types of personally identifiable information that are encompassed within the term "criminal justice record information," including juvenile justice information, investigative and intelligence information, various kinds of original records of entry, and, of course, the criminal history record.

The report also sets forth the constitutional and common law standards that apply to CHRI. The report emphasizes that the courts recognize individuals have a privacy interest in CHRI which pertains to them, but that this interest has seldom been relied upon by the courts to strike down or limit statutory and regulatory standards for the collection, use, and dissemination of CHRI.

The report provides further background by tracing the development of Federal and State criminal history record legislation and regulation. In the period since 1967, the Congress, the Justice Department, State legislatures, and regulatory bodies have devoted considerable attention to standards for collecting, maintaining, using, and disseminating CHRI. Both BJS and SEARCH have been active participants in the development of these standards. The report notes that today, these standards provide for the following: subject access and correction rights; restrictions on the amalgamation of criminal history information with other types of personal information; various kinds of standards to ensure the accuracy, completeness, and timeliness of CHRI; fingerprint support of information entered into law enforcement criminal history systems and obtained from those systems; various kinds of disposition reporting requirements; sealing and purging standards in the case of old information or arrest information without a disposition; security standards; standards for criminal history use or dissemination; widespread criminal justice access to CHRI; limited noncriminal justice access to CHRI; and very limited public access to CHRI.

The report also includes brief case studies of three States that have taken very different approaches to public access to law enforcement CHRI: Florida, which takes an "open record" approach; Washington, which takes an "intermediate" approach (providing significant access to conviction information but very limited access to nonconviction information); and Massachusetts, a largely "closed-record" State that permits access only to criminal justice entities.

The bulk of the report focuses on the "change drivers" described above. In particular, the report gives attention to the public's concern about privacy and the technological changes that make previously inaccessible court records widely available.

Task Force recommendations

Finally, the report presents the 14 recommendations adopted by the National Task Force on Privacy, Technology and Criminal Justice Information.

Several points should be emphasized about these recommendations:

- First, the purpose of these recommendations is not to prescribe the specifics of a new generation of law and policy for criminal justice record information. Rather,

the purpose of the recommendations is to address the conceptual and structural outline of a new generation of law and policy. Accordingly, the Task Force recommends that further work on these specifics be undertaken by a statutorily chartered study organization with a 3-year sunset.

- Second, in looking at the approach to CHRI, the Task Force recommends a global policy to address criminal history and juvenile justice record information largely without regard to whether this information is held by law enforcement agencies (that is, the central State repositories), the courts, or commercial compilers and aggregators. The Task Force's rationale for this approach is that the privacy and information implications are largely unaffected by whether the information is sourced to courts, law enforcement, or commercial compilers.
- Third, the Task Force reaffirms the importance of using fingerprints to the extent that technology, cost, and availability make fingerprints available to law enforcement, the courts, and the commercial sector. Only with the use of fingerprints can a reliable determination be made that a criminal history record pertains to the person who is the subject of the search.
- Fourth, the Task Force view is that the creation of comprehensive profiles about individuals is a threat to privacy and, importantly, is perceived by the public as a threat to privacy. Accordingly, the Task Force recommends that criminal justice record information not be amalgamated with other types of personal information (such as financial or medical information) in databases of criminal history and criminal justice records.
- Fifth, the Task Force view is that the national initiative to integrate various criminal justice record information systems, in order to improve the utility, effectiveness, and cost efficiency of these systems, is a positive development and should be encouraged. The Task Force recognizes, however, that the establishment of these kinds of systems raises privacy and profiling issues and, therefore, the structure and content of integrated information systems should be shaped to minimize these threats.

Specifically, the Task Force adopted the following recommendations, which were subsequently endorsed in January 2000 by SEARCH's Membership Group (governors' appointees):

I. The Task Force recommends that a body be statutorily created to consider and make policy recommendations to the Federal and State legislative, executive, and judicial branches of government as they work to balance the increasing demand for all forms of criminal justice information and the privacy risks associated with the collection and use of such information. The Task Force recommends that the body look at information and privacy issues arising from all types of criminal justice information, including criminal history record information, intelligence and investigative information, victim and witness information, indexes and flagging systems, wanted person information, and civil restraining orders. The Task Force further recommends that such a body be comprised of public and private stakeholders; that the body be limited to an advisory role; and that it have neither rulemaking nor adjudicatory authority. Finally, the Task Force recommends that the body sunset after not more than 3 years, unless statutorily reauthorized.

II. The Task Force recommends the development of a new generation of criminal justice information and privacy law and policy, taking into account public safety, privacy, and government

oversight interests. This law and policy should be broad in scope, so as to address the collection, maintenance, use, and dissemination of criminal justice record information by law enforcement agencies, including State central repositories and the FBI, the courts, and commercial compilers and resellers of criminal justice record information.

III. The Task Force recommends that the adequacy of existing legal remedies for invasions of privacy arising from the use of criminal history record information should be reexamined by legal scholars, State legislatures, Congress, State and Federal agencies, and the courts.

IV. The Task Force recommends the development of a new generation of confidentiality and disclosure law and policy for criminal history record information, taking into account the type of criminal history record information; the extent to which the database contains other types of criminal justice information (victim and witness information, or intelligence or investigative information) and sensitive personal information (medical or financial information, and so on); the purpose for the intended use of the information; and the onward transfer of the information (the redissemination of the criminal history information by downstream users).

V. The Task Force recommends that intelligence and investigative information also be addressed by new privacy law and policy, but that this process should begin with the establishment of a Task Force dedicated exclusively to a review of intelligence and investigative systems, and the law and privacy issues related to those systems.

VI. The Task Force recommends that legislators and criminal history record information system managers develop, implement, and use the best available technologies to promote data quality and data security.

VII. The Task Force recommends that criminal history record information, whether held by the courts, by law enforcement, or by commercial compilers and resellers, should, subject to appropriate safeguards, be supported by and accessible by fingerprints to the extent legally permissible and to the extent that technology, cost, and the availability of fingerprints to both database managers and users make this practicable.

VIII. The Task Force recommends that criminal history record information should be sealed or expunged (purged) when the record no longer serves an important public safety or other public policy interest. A sealed record should be unsealed and available for criminal justice and/or public use only when the record subject has engaged in a subsequent offense or when other compelling public policy considerations substantially outweigh the record subject's privacy interests. During the period that a criminal history record is sealed, use and disclosure should be prohibited.

IX. The Task Force recommends that individuals who are the subject of criminal history record information be told about the practices, procedures, and policies for the collection, maintenance, use, and disclosure of criminal history information about them; be given a right of access to and correction of this information, including a right to see a record of the disclosure of the information in most circumstances; and enjoy effective remedies for a violation of any applicable privacy and information standards. In

addition, the Task Force recommends that States establish meaningful oversight mechanisms to ensure that these privacy protections are properly implemented and enforced.

X. The Task Force recommends that where public safety considerations so require, the record of a juvenile offender who commits an offense which, if committed by an adult, would be a felony or a violent misdemeanor, be treated in the same manner that similar adult records are treated. Even if a State opts to retain stronger privacy and confidentiality rules for these types of juvenile records, these records should be fingerprint-supported and should be capable of being captured in an automated, national system.

XI. The Task Force recommends that criminal justice record information law and policy should restrict the combining of different types of criminal justice record information into databases accessible to noncriminal justice users and should restrict the amalgamation of criminal justice record information in databases with other types of personal information, except where necessary to satisfy public policy objectives.

XII. The Task Force recommends that where public policy considerations require amalgamation of information, systems be designed to recognize and administer differing standards (including dissemination policies and standards) based upon differing levels of data sensitivity, and allow the flexibility necessary to revise those standards to reflect future changes in public policy.

XIII. The Task Force recommends that the integration of criminal justice information systems should be encouraged in recognition of the value of integrated systems in improving the utility, effectiveness, and cost efficiency of information systems. Prior to establishing integrated systems, however, privacy implications should be examined, and legal and policy protections in place, to ensure that future public- and private-sector uses of these information systems remain consistent with the purposes for which they were originally created. In addition, once an integrated system is created, any future uses or expansions of that system should be evaluated to assess the privacy implications.

XIV. The Task Force recommends that new criminal justice privacy law and policy should continue to give weight to the distinction between conviction information and nonconviction information. The Task Force recognizes, however, that there are certain instances in which disclosure of nonconviction information may be appropriate.

II. Report purpose and scope

It hardly comes as a surprise that Federal agencies collect vast amounts of personal information, including information collected through the criminal justice system. It is also no surprise that this information collection activity serves critical public safety and other public values. Moreover, access to public record information, including criminal justice information, promotes interests critical to a democratic society, including:

- **Promoting government accountability**. Access to public records helps the public monitor government activities, thereby assisting the public to hold elected officials and nonelected civil servants accountable and protecting against secret government activities.
- **Promoting first amendment rights**. Access to public record information helps to create the informed citizenry necessary for the robust, wide-open public debates that play an important structural role in securing and fostering free speech and republican self-government.
- **Promoting confidence in the judicial and political systems**. Access to public record information bolsters public knowledge about, and helps instill confidence in, the operation of the political system as well as the judicial system.
- **Promoting private-sector accountability**. The use of background checks that rely on public record information allows the verification of assertions made by individuals (or facts omitted by individuals), thereby permitting prospective employers and business partners to protect themselves and vulnerable populations which may be in their care, including children, the disabled, and the elderly.
- **Promoting meritocracy**. In a mobile society where merit (often initially represented by credentials) is often used rather than family connections and lineage for purposes such as employment, access to public records provides an important means of verifying an individual's credentials, including whether the individual has a criminal record.

Because this information is collected and used for the good of society, why isn't that the end of the debate? Why not make all information, including personal information collected by Federal agencies, publicly available? The answer, of course, is that there are powerful competing values, interests, and concerns. One such interest is privacy. Privacy encompasses not only secrecy but also fair information practices regarding the use, access, accuracy, right to challenge inaccurate information, and knowledge that record systems even exist.[7] These information privacy interests were given voice in the 1970s, at a time when centralized and automated record systems were chiefly associated with governmental activities. During the 1970s, a set of broad fair information practice policies emerged, with specific applications for criminal justice information. Since the 1970s, there have been many changes, including technological, political, and marketplace changes, that have changed the information environment.

This report identifies developments that may be outpacing established privacy and fair information practices protections for criminal justice information, and which may necessitate a new look at appropriate law and policy for managing this information. The report is intended to serve as a resource for State and Federal policymakers, the

[7]Other values and interests include national security interests, secrecy requirements necessary to facilitate ongoing law enforcement investigations, the protection of trade secrets, and so on.

courts, criminal justice agencies, private-sector, self-regulatory organizations, privacy advocates, and individuals interested in privacy and criminal justice issues.

For purposes of this report, "criminal justice information" is defined broadly to include all information obtained, maintained, or generated about an individual by the courts or a criminal justice agency as a result of suspicion that the individual may be engaging in criminal activity or in relation to his or her arrest and the subsequent disposition of this arrest. "Criminal justice information" includes: criminal history record information (CHRI); criminal intelligence information; criminal investigative information; disposition information; identification record information; nonconviction information; and wanted person information.[8]

Criminal intelligence and criminal investigative information are within the definition of criminal justice information as it is addressed in this report. The Task Force concluded after considerable deliberation, however, that changes in criminal intelligence and investigative information systems raise complex and discrete privacy issues. Those issues merit examination by a separate Task Force or other group devoted solely to that issue, particularly a group with more representation from the investigative and intelligence communities than is reflected in the membership of the Task Force on Privacy, Technology and Criminal Justice Information.

[8] *Technical Report No. 13: Standards for the Security and Privacy of Criminal History Record Information,* 3rd ed. (Sacramento: SEARCH Group, Inc., 1988) pp. 8-9. Hereafter, Technical Report No. 13, 3rd ed. A glossary of justice information terms is included as Appendix 2.

III. Information privacy standards: Background

Customarily, the term "information privacy" is used to refer to standards for the collection, maintenance, use, and disclosure of personally identifiable information. A central component of "information privacy" is the ability of an individual to control the use of information about him or herself.[9]

Information privacy is frequently distinguished from other clusters of personal interests that are nourished by the privacy doctrine, including *surveillance privacy* — the interest in being free from governmental and other organized surveillance of individual activities under circumstances where the individual has a reasonable expectation of privacy; and *behavioral privacy* — the right to engage in certain intimate and sensitive behaviors (such as behaviors relating to reproductive rights) free from governmental or other control.[10]

Protection of information privacy is widely seen as serving at least five interests that are critical to a democracy:

1. An interest in ensuring society (both public and private sectors) makes decisions about individuals in a way that comports with notions of due process and fairness. Accuracy of CHRI and use of that information which includes providing notice to the individual and giving the individual an opportunity to respond, is consistent with notions about fairness. The absence of these protections may produce erroneous or unjustified decisions about employment, credit, health care, housing, or other valued benefits or statuses.
2. An interest in protecting individual dignity. When individuals endure stigma, embarrassment, and humiliation arising from the uncontrolled use and disclosure of information about them, they lose the sense of dignity and integrity essential for effective participation in a free and democratic society.
3. An interest in protecting individual autonomy. When individuals lack control over personal information about themselves, they lose a sense of control over their lives. The ability of individuals to control personal information about themselves promotes personal autonomy and liberty.
4. An interest in promoting a sense of trust in, and a check upon the behavior of, institutions. When individuals lose the ability to selectively disclose their sensitive personal information, they lose trust in the public and private institutions that collect, hold, use, and disclose this personal information. (Public opinion surveys indicate that the public's "distrust index" (the extent to which the public distrusts the government) is at all-time high levels of approximately 80 percent.)[11]
5. An interest in promoting the viability of relationships critical to the effective functioning of a democratic society. Numerous relationships, such as the doctor-patient relationship, the lawyer-client relationship, or even the news media and confidential source relationship, depend upon promises of confidentiality in order to promote the candid sharing of personal information and trust within the relationship.

The concept of information privacy as a distinct branch of privacy is relatively new. The concept found full voice in the late 1960s, amid rising concerns about computers and growing disenchantment with government, and articulated in writings

[9]See, for example, Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) p. 7. Hereafter, Privacy and Freedom.

[10]In *Whalen* v. *Roe*, 429 U.S. 589, 599, 600 (1977), the Supreme Court discussed the various clusters of interests protected by the broad term "privacy."

[11]See note 75 *infra*.

such as Alan Westin's book, *Privacy and Freedom*,[12] with later iterations in the 1972 National Academy of Science's report, *Databanks in a Free Society*,[13] and the 1973 Report of the Secretary of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems (HEW Report).[14]

These seminal works recognized the importance of information privacy and the need to balance privacy with other competing interests, such as public safety. As part of this dialogue, the HEW Report's "Code of Fair Information Practices" set forth five basic procedural principles for fair information practices:

1. There must be no personal-data recordkeeping 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 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.
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 reasonable precautions to prevent misuse of the data.[15]

The HEW Code of Fair Information Practices was widely influential when it was released, and served as a basis for the *Federal Privacy Act of 1974*. The HEW Code of Fair Information Practices was further examined and applied to specific recordkeeping relationships in the 1977 Report of the Privacy Protection Study Commission.[16] Balancing privacy with competing interests has also been widely accepted as a means of accounting for privacy concerns.[17] Although some have questioned whether the Code of Fair Information Practices remains a viable approach,[18] the Code and balancing privacy with competing interests continues to provide a framework for fair information practices in the United States.[19]

[12]Privacy and Freedom, *supra* note 9.

[13]Alan F. Westin and Michael A. Baker, *Databanks in a Free Society: Computers, Record-Keeping and Privacy* (New York: Quadrangle Books, 1972). See also, Robert R. Belair, "Information Privacy: A Legal and Policy Analysis," in *Science, Technology and Uses of Information* (Washington, D.C.: National Science Foundation, 1986).

[14]*Records, Computers and the Rights of Citizens*, DHEW Publication No. (OS) 73-97 (Washington, D.C.: Department of Health, Education and Welfare, 1973), available at **http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm**.

[15]Ibid., p. 41.

[16]U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington, D.C.: U.S. Government Printing Office, July 1977).

[17]Charles D. Raab, "From Balancing to Steering: New Directions for Data Protection," in *Visions of Privacy: Policy Choices for the Digital Age*, Colin J. Bennett and Rebecca Grant, eds. (Toronto: University of Toronto Press, 1999) pp. 68-93.

[18]Ibid. Other privacy experts continue to believe that Fair Information Practices and the "balancing of interests" approach can continue to serve as the basis for privacy law and policy, either as currently constituted or with modifications. See, for example, David H. Flaherty, "Visions of Privacy: Past, Present and Future," in ibid., pp. 19-38.

[19]See, for example, Testimony of Donna E. Shalala, Secretary, U.S. Department of Health and Human Services, before the Senate Committee on Labor and Human Resources, September 11, 1997 (recommending that the Congress pass health information privacy legislation based upon the 1973 Code of Fair Information Practices). Not surprisingly, however, the Fair Information Practices outlined in the HEW Report have been expanded upon in the nearly 30 years since they were first promulgated. Today, influenced in part by developments in Europe, discussion of fair information practices also frequently focus, for example, on procedural and substantive safeguards surrounding the collection of information to ensure that information is used only for purposes consistent with those for which the information is collected, and that the information collected is relevant to the purpose for which it is being collected.

IV. Privacy protections for criminal justice information

A brief overview of the structure of the criminal justice information system

Before examining the legal and policy regime surrounding criminal justice information, this section briefly reviews the structure of the criminal justice information system as it relates to CHRI (at both the Federal and State levels), juvenile justice information, intelligence and investigative information, and original records of entry.

- **Criminal history record information: Federal role**. At the Federal level, the FBI functions as a criminal history record repository, holding both Federal offender information and records of arrest and dispositions under State law.
  - — *Interstate Identification Index (III).* During the last 30 years, the FBI, working with the State criminal justice information community, developed the III. The III consists of an FBI-maintained index of all individuals with State or Federal criminal history records, supported by a National Fingerprint File. Authorized requestors access the III to determine whether any State (or the FBI for Federal offenses) maintains a criminal history record about a particular individual.
  - — *III Compact.* In October 1998, the Congress enacted the *Crime Identification Technology Act* (CITA),[20] which includes as Title II, the *National Crime Prevention and Privacy Compact Act* (III Compact). Once ratified by the States, the III Compact will permit the III to be used by authorized, noncriminal justice requestors.[21]
- **Criminal history record information: central State repositories**. Every State has established a "central State repository" of criminal history information and fingerprints, operated by a State law enforcement agency. Central State repositories maintain a fingerprint record of every individual arrested in the State for a serious/reportable offense (standards vary among the States, but, customarily, reportable offenses are misdemeanors punishable by a year or more in prison, plus felonies). The repository also maintains an automated record of those individuals' arrests, along with all available dispositions. This record is referred to as a criminal history record or "rap sheet."
  - — *Repository mission*. The central State repository's principal mission is to provide CHRI to State and local law enforcement agencies. The repositories also provide CHRI to the other components of the criminal justice system — courts, prosecutors, and corrections — as well as certain noncriminal justice users.[22]
  - — *Information maintained by repositories*. Traditionally, central State repositories maintain subject identification information (fingerprint

[20] 42 U.S.C. § 14601.

[21] As of June 2001, 12 States (Montana, Georgia, Nevada, Florida, Colorado, Iowa, Connecticut, South Carolina, Arkansas, Alaska, Oklahoma, and Maine) had ratified the III Compact, which became effective on April 28, 1999, following the ratification of the Compact by the first two States. The Compact now applies between the States that have ratified it and the Federal government. See, "Crime Prevention and Privacy Compact," available at **http://www.search.org/policy/compact/privacy.asp**.

[22] Robert R. Belair and Paul L. Woodard, *Use and Management of Criminal History Record Information: A Comprehensive Report*, Criminal Justice Information Policy series, NCJ 143501 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, November 1993) pp. 14-17. Hereafter, Use and Management of CHRI.

records), criminal history information (which historically and traditionally consists of identifying information, arrests, and available dispositions, but little or no information about third parties such as witnesses, victims, or family members),[23] and certain other information (such as pretrial release information and felony conviction flags). Repositories virtually never maintain other types of personal information (employment history, medical history, military, or citizenship status, and so on).[24]

— *Liaison with FBI*. Repositories serve as a contact point and liaison with the FBI: sending fingerprints and arrest and disposition information to the FBI; responding to search inquiries from the FBI; and initiating search inquiries to the FBI on behalf of authorized, in-State requestors.

— *Information maintained by local agencies*. Over the past 30 years, local agencies, with rare exception for the very largest local agencies, have withdrawn from the business of maintaining formal and comprehensive criminal history records (other than booking information and other original records of entry). Instead, local agencies rely on the State repository and, through the State repository, the FBI to provide complete and comprehensive criminal history records.

· **Juvenile justice information**. Juvenile justice information is, broadly speaking, information on juveniles, which, but for the age of the juvenile, would be considered criminal justice information.[25] Traditionally, the repositories do not maintain juvenile justice information; for the few repositories that do, it is frequently not integrated with adult records of that individual. (As a practical matter, juvenile justice information, until very recently, was not available on any kind of reliable or organized basis. Rather, each separate juvenile or family court and each separate law enforcement agency would maintain juvenile records. These records frequently were not automated or fingerprint-supported. Moreover, traditionally, some of these records were not available by law (based on sealing requirements), even to criminal justice agencies.)

· **Investigative and intelligence information**. Customarily, investigative and intelligence information has rarely been maintained at a central State repository; when maintained, it has not been integrated with CHRI. Historically, investigative and intelligence information was maintained only at the local police agency or law enforcement agency level; it was not automated or fingerprint-supported; and it was shared on a closely held, need-to-know basis within the law enforcement community.[26]

· **Original records of entry**. Pieces of an individual's criminal history record, but only infrequently an individual's entire criminal history record, are held in "open record" files maintained by police agencies and courts. These original records of entry describe formal detentions and arrests and include incident reports, arrest reports, case reports, and other information that documents that an individual has been detained, taken into custody, or otherwise formally charged. In addition, records of court proceedings

[23]See, SEARCH Group, Inc., *Increasing the Utility of the Criminal History Record: Report of the National Task Force*, Criminal Justice Information Policy series, NCJ 156922 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, December 1995) pp. 23-27.

[24]Ibid., pp. 22-23.

[25]This age varies by State.

[26]See, Robert R. Belair, *Intelligence and Investigative Records*, Criminal Justice Information Policy series, NCJ 95787 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, February 1985) pp. 43-49.

maintained by the courts include indictments, arraignments, preliminary hearings, pretrial release hearings, and other court events that, by law and tradition, are open to public inspection. Until very recently, both types of open record systems were manual or, at best, only partially automated; they were not comprehensive or reliable, and related only to events occurring at the particular law enforcement agency or court. As a consequence, these systems were difficult and expensive to use and largely unsuitable for the compilation of a reliable or comprehensive criminal history record file. Compilation of these records into a criminal history file on an individual was also difficult because these record systems were incident-focused, rather than individual-focused, and were not comprehensive, cumulative, or otherwise linked on the basis of the individuals involved in each incident.

By the 1990s, these relatively traditional elements of the criminal justice information environment were changing. Criminal justice information, particularly including court-based CHRI, was largely automated and was becoming more publicly available. The role of the central repositories as the gatekeeper for CHRI was being challenged not only by the courts, but also by automated, for-profit information brokers and suppliers and by local criminal justice agencies. Fundamental changes in expectations about the availability and utility of criminal justice information fueled accelerating pressures for more and easier access to criminal justice information.

Constitutional and common law standards with respect to the privacy of criminal history record information

— Constitutional standards

The Constitution remains largely neutral with respect to the privacy of CHRI. In particular, the Supreme Court has held that the Constitution does not recognize a privacy interest in the dissemination by criminal justice agencies of information about official acts, such as arrests.[27] In 1989, in *Department of Justice* v. *Reporters Committee for Freedom of the Press*,[28] the Supreme Court did recognize, however, that there is a statutory privacy interest, under the Federal *Freedom of Information Act* (FOIA), in automated, comprehensive criminal history records.[29] The Court held "as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no 'official information' about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is 'unwarranted'" and therefore exempt from disclosure under FOIA's privacy provision.[30]

In 1995, the Court again addressed the privacy risk posed by computerized criminal history information. In *Arizona* v. *Evans*,[31] the Court found that the "exclusionary rule" does not require suppression of evidence seized incident to an arrest resulting from an inaccurate computer record when the error was caused by court, rather than police, personnel. In a concurring opinion, Justice O'Connor noted that "the advent of powerful, computer-based recordkeeping systems … facilitate[s] arrests in ways that have never before been possible. The police … are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities."[32]

---

[27] *Paul* v. *Davis*, 424 U.S. 693, 713 (1976).

[28] 489 U.S. 749 (1989).

[29] The Court has used statutory law, rather than constitutional law, to protect privacy in other contexts as well. In *Jaffee* v. *Redmond*, 518 U.S. 1 (1996), for example, the Court, recognizing the sensitivity of mental health information, held that Rule 501 of the Federal Rules of Evidence recognizes a psychotherapist-patient privilege, which extends to confidential communications between a licensed social worker and a patient in the course of psychotherapy.

[30] 489 U.S. 749, 780 (1989).

[31] 514 U.S. 1 (1995).

[32] Ibid., at 17-18 (O'Connor, J., concurring).

Justice Ginsburg, in dissent, also expressed concern over the impact of modern technology on privacy: "Widespread reliance on computers to store and convey information generates, along with manifold benefits, new possibilities of error, due to both computer malfunctions and operator mistakes … . [C]omputerization greatly amplifies an error's effect, and correspondingly intensifies the need for prompt correction; for inaccurate data can infect not only one agency, but the many agencies that share access to the database."[33]

During the 1999-2000 term, the Supreme Court handed down two decisions regarding statutory controls on access to public record information, which, while not decided on privacy grounds, are likely to encourage stronger privacy initiatives.

The first opinion, *Los Angeles Police Department* v. *United Reporting Publishing Corp.*,[34] arose from a 1996 change in California law governing the release of arrest information.[35] The change limited the release of arrestee and victim address information to those who certify that the request is made for scholarly, journalistic, political, or governmental purposes, or for investigative purposes by a licensed private investigator. The law specifically prohibits the use of such information "directly or indirectly to sell a product or service to any individual or group of individuals."

United Reporting Publishing Corp., a private publishing service that had been providing arrestee address information to clients under the old statute, filed suit, alleging that the statute was an unconstitutional violation of its first amendment commercial speech rights. The Ninth Circuit, while finding that arrestees have a substantial privacy interest in the information at issue, nevertheless concluded (as did the district court) the California law was an unconstitutional infringement on United Reporting's first amendment commercial speech rights because the "myriad of exceptions … precludes the statute from directly and materially advancing the government's purported privacy interest."[36]

On December 7, 1999, the Supreme Court voted 7 to 2 to reverse, reinstating the California statute. In its opinion, the majority characterized *United Reporting* as a case dealing with access to government records rather than restrictions on free speech.[37] The Supreme Court also characterized the case as a challenge to the "facial validity" of the California statute and not a challenge based upon the implementation or actual experience with the statute.[38] For these reasons the Court opined that California could distinguish among users and uses in crafting rules for access to State-held records. The Court left open the possibility, however, that the statute, as applied, might impinge on United Reporting's commercial speech rights.

---

[33]Ibid., at 26 (Ginsburg, J. dissenting).

[34]528 U.S. 32 (1999).

[35]CAL. GOV. CODE § 6254(f).

[36]*United Reporting Publishing Corp.* v. *Los Angeles Police Department*, 146 F.3d 1133, 1140 (9th Cir. 1998).

[37]The Court's decision did not address the commercial speech interests at issue in the regulation of the use of personal information in private records, an issue that has also drawn the attention of the appellate courts. The Tenth Circuit Court of Appeals, for example, acted on first amendment commercial speech grounds, to vacate a rule issued by the Federal Communications Commission that required consumers to opt-in to most disclosures of their consumer proprietary network information (CPNI). *U.S. West, Inc.* v. *Federal Communications Commission*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000). 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 that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, including most information contained in telephone bills. See, 47 U.S.C. § 222(f)(1)(A)-(B).

[38]In a related development, on December 13, 1999, the Supreme Court issued an order in *McClure* v. *Amelkin*, 528 U.S. 1059 (1999), setting aside a decision by the Sixth Circuit Court of Appeals that struck down a Kentucky law limiting access to motor vehicle accident reports. The Sixth Circuit struck down the law — which allows access to accident victims, victims' lawyers, victims' insurers, and the news media (but not for commercial purposes) — after finding that the law violates commercial free speech rights. The Supreme Court sent the case back to the Sixth Circuit and ordered the lower court to restudy the case, taking into consideration the Supreme Court's decision in *United Reporting*.

In the second opinion, *Reno* v. *Condon*,[39] the Supreme Court unanimously reversed the Fourth Circuit Court of Appeals, rejecting a tenth amendment[40] challenge by the State of South Carolina to the constitutionality of the *Driver's Privacy Protection Act of 1994* (DPPA).[41] The DPPA provides that State departments of motor vehicles (DMVs) "shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record."[42] The DPPA does contain 14 exceptions pursuant to which States may elect to disclose DMV records in certain instances.[43] Violation of the DPPA may result in criminal fines and a civil cause of action against a person who knowingly violates the statute.[44] Although the Court's brief opinion was based on tenth amendment rather than privacy grounds, the decision potentially opens the door for further Federal regulation of access to State records on privacy grounds.[45]

— Common law standards

Common law privacy doctrines, such as the widely recognized privacy tort of public disclosure of private facts, have proven largely ineffectual when applied to CHRI. Sovereign immunity, civil and official immunity, and the need to show tangible harm arising from the alleged disclosure or misuse of criminal history records have proven to be virtually insurmountable obstacles to common law privacy actions.[46] The limited nature of common law and constitutional privacy protections has meant that safeguarding information privacy interests has been left largely to the legislative arena.

Federal criminal history record legislation and regulations

Beginning in the late 1960s and extending throughout the 1970s, information privacy standards for criminal justice information and, in particular, criminal history records, received considerable attention in statutory provisions and U.S. Department of Justice (DOJ) regulations. Although the privacy protections that emerged from that debate were not driven by constitutional requirements, constitutional values — such as the presumption that an individual is innocent until proven guilty — have played a role in the development of the law and regulations governing the management of CHRI.[47]

---

[39]528 U.S. 32, 120 S.Ct. 483 (2000). The Fourth Circuit case was the first of four decisions issued by the Courts of Appeals on the constitutionality of the DPPA; two decisions upheld the constitutionality of the DPPA, two held it to be unconstitutional. See, *Condon* v. *Reno*, 155 F.3d 453 (4th Cir. 1998) (holding DPPA is unconstitutional); *Pryor* v. *Reno*, 171 F.3d 1281 (11th Cir. 1999) (holding DPPA is unconstitutional); *Travis* v. *Reno*, 160 F.3d. 1000 (7th Cir. 1998) (upholding DPPA); *Oklahoma* v. *United States*, 161 F.3d 1266 (10th Cir. 1998) (upholding DPPA). The DPPA has also been challenged on first amendment grounds; however, discussions of first amendment challenges are omitted here. See, for example, *Travis* v. *Reno* and *Oklahoma* v. *United States*

[40]"The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." U.S. Const., Amend. X.

[41]18 U.S.C. § 2721 *et seq*.

[42]18 U.S.C. § 2721(a).

[43]18 U.S.C. § 2721(b).

[44]18 U.S.C. §§ 2723(a), 2724(a).

[45]The Court concluded that "the DPPA does not require States in their sovereign capacity to regulate their own citizens. The DPPA regulates the States as the owners of databases. It does not require the South Carolina Legislature to enact any laws or regulations, and it does not require State officials to assist in the enforcement of Federal statutes regulating private individuals. We accordingly conclude that the DPPA is consistent with the constitutional principles enunciated in [*New York* v. *United States*, 505 U.S. 144 (1992); and *Printz* v. *United States*, 521 U.S. 898 (1997)]." *Reno* v. *Condon*, 528 U.S. 32, 120 S.Ct. 666, 672 (2000). In addition, the Court disagreed with the Fourth Circuit's holding that the DPPA exclusively regulated the States, finding instead that the "DPPA regulates the universe of entities that participate as suppliers to the market for motor vehicle information — the States as initial suppliers of the information in interstate commerce and private resellers or redisclosers of that information in commerce." Ibid. As a result, the Court did not address the "question whether general applicability is a constitutional requirement for federal regulation of the States."

[46]See, *Technical Memorandum No. 12: Criminal Justice Information, Perspective on Liabilities* (Sacramento: SEARCH Group, Inc., August 1977) (and as updated in 1981) pp. 5-20.

[47]As the Privacy Protection Study Commission noted in its 1977 report: "Constitutional standards specify that convictions, not arrests establish guilt. Thus denial of employment [for example] because of an unproved charge, a charge that has been dismissed, or one

In 1967, the Report of the President's Commission on Law Enforcement and the Administration of Justice spoke of the need for an "integrated national information system" and recommended that there be established a "national law enforcement directory that records an individual's arrests for serious crimes, the disposition of each case and all subsequent formal contacts with criminal justice agencies related to those arrests." The report also emphasized that it is "essential" to identify and protect security and privacy rights to ensure a fair, credible, and politically acceptable national criminal justice information system.[48]

For most of the last 30 years, the U.S. DOJ, working through the FBI, the Law Enforcement Assistance Administration (LEAA) and its successor agencies, including, in particular, OJP, BJS, and the Bureau of Justice Assistance (BJA), and the State and local criminal justice information community, including SEARCH and the FBI Criminal Justice Information Services Division's Advisory Policy Board (CJIS APB), have worked toward the implementation of an automated national system for the exchange of criminal history records, along with a set of comprehensive privacy standards. Several prominent features dominated that environment.

Privacy standards for CHRI have been left largely to statutory and regulatory initiative. During the 1970s, when public concern about privacy, automation, and governmental and private information systems was running high, the Congress considered several legislative proposals that would have imposed uniform, national information and privacy standards for CHRI. All of those proposals failed.[49]

While the comprehensive proposals for uniform, nationwide standards failed, Congress was not idle. In 1972, for example, Congress authorized the FBI to "exchange identification records" with State and local officials for "purposes of employment and licensing," provided that the exchange of information is authorized by State statute and approved by the Attorney General, and provided that the exchange of information is made only for official use and is subject to the same restrictions with respect to dissemination as would apply to the FBI.[50]

In 1973, Congress enacted the so-called "Kennedy Amendment" to the *Omnibus Crime Control and Safe Streets Act of 1968*, which provides that all CHRI collected, maintained, or disseminated by State and local criminal justice agencies with financial support under the *Omnibus Crime Control and Safe Streets Act* must be made available for review and challenge by record subjects and must be used only for law enforcement and other lawful purposes.[51] LEAA implemented the Kennedy Amendment by adopting

for which there has been an adjudication of innocence, is fundamentally unfair." *Supra* note 16, Appendix 3, Employment Records, p. 50. The value of arrest records as a decisionmaking tool, particularly in the employment context, has also been challenged on the grounds that racial minorities are arrested in disproportionately high numbers. As a result, the Equal Employment Opportunity Commission and several courts have found that inquiries about arrest records can be a violation of Title VII of the *Civil Rights Act of 1964*. See, for example, 29 C.F.R. § 1607.4(c)(1); and *Gregory* v. *Litton Sys.*, 316 F. Supp. 401 (C.D. Cal. 1970), *aff'd as modified*, 472 F.2d. 631 (9th Cir. 1972) (fact that an individual suffered a number of arrests without any convictions was not conclusive as to wrongdoing and was irrelevant to work qualifications and, because the mere inquiry into arrest records tends to have a chilling effect on minority job applicants, inquiries about arrests may violate Title VII). The U.S. DOJ requires that federally funded criminal justice information systems distinguish between nonconviction information (including certain arrest information) and conviction information. 20 C.F.R. § 20.21(b).

[48]Project SEARCH, *Technical Report No. 2: Security and Privacy Considerations in Criminal History Information Systems* (Sacramento: California Crime Technological Research Foundation, 1970) pp. 3-5 (quoting from the President's Commission Report).

[49]See, Use and Management of CHRI**,** *supra* note 22, p. 36. The FBI's basic statutory authority to maintain and disseminate criminal history records is at 28 U.S.C. § 534. This provision authorizes the Attorney General to "acquire, collect, classify and preserve criminal identification, crime and other records" and to "exchange such records and information with and for the official use of, authorized officials of the federal government, the States, cities and penal and other institutions."

[50]Pub. L. No. 92-544, Title II, § 201, 86 Stat. 1115.

[51]42 U.S.C. § 3789G(b), as amended by § 524(b) of the *Crime Control Act of 1973*, Pub. L. No. 93-83 (1973).

comprehensive regulations — known as the "DOJ regulations" — intended to "assure that CHRI wherever it appears is collected, stored, and disseminated in a manner to insure the completeness, integrity, accuracy and security of such information and to protect individual privacy."[52] The regulations set relatively detailed and ambitious standards for data quality, while giving States discretion to set their own standards for dissemination, recognizing that incomplete or inaccurate criminal history data, particularly arrest information without disposition information, could have negative implications for the record subject and his or her participation in society.

In addition to regulation of the handling of criminal history information by criminal justice agencies, Federal law also regulates private-sector uses of criminal history information in certain circumstances. The *Fair Credit Reporting Act* (FCRA), for example, regulates the compilation, disclosure, and use of consumer reports, which may include criminal history information.[53]

SEARCH *Technical Report No. 13*

SEARCH has also been active in the formulation of standards for the security and privacy of CHRI. Beginning in 1970, the year after SEARCH was established, SEARCH published a series of reports addressing privacy and security in computerized criminal history files, and providing guidance for legislative and regulatory protections for CHRI.[54]

In 1975, SEARCH published the widely influential *Technical Report No. 13*, SEARCH's first comprehensive statement of 25 recommendations for safeguarding the security and privacy of criminal justice information.[55] These recommendations influenced LEAA's development of the DOJ regulations discussed above, and the Appendix to the DOJ regulations refers States to *Technical Report No. 13* for guidance in formulating their State plans.[56] *Technical Report No. 13* has been revised twice since 1975 — most recently in 1988 — to reflect technological and societal changes that have had an impact on criminal justice information management and privacy.[57]

State legislation

The bulk of the criminal justice information maintained in the United States is maintained at the State level; therefore, most of the legislation on governing this information is found at the State level (with certain important exceptions, such as the DOJ regulations discussed above). Throughout the 1970s and into the 1980s, States adopted statutes based in large measure on the DOJ regulations and the SEARCH recommendations. By the early 1990s, approximately one-half of the States had enacted comprehensive criminal history record legislation, and every State had enacted statutes that address at least some aspects of criminal history records. The majority of State laws followed the scheme in the DOJ regulations that distinguishes between information referring to convictions and current arrests (arrests that are no older than 1 year and that do not yet have the disposition) and "nonconviction data," which includes arrests more than 1 year old without a disposition or arrests with dispositions favorable to the accused.

[52]28 C.F.R § 20.01.

[53]The *Fair Credit Reporting Act* is discussed in greater detail in *infra*, chapter V, p. 58.

[54]See, *Technical Report No. 2: Security and Privacy Considerations in Criminal History Information Systems*, *supra* note 48; Project SEARCH, *Technical Memorandum No. 3: A Model State Act for Criminal Offender Record Information* (Sacramento: California Crime Technological Research Foundation, May 1971); and Project SEARCH, *Technical Memorandum No. 4: Model Administrative Regulations for Criminal Offender Record Information* (Sacramento: California Crime Technological Research Foundation, 1972).

[55]See, *Technical Report No. 13: Standards for the Security and Privacy of Criminal Justice Information* (Sacramento: SEARCH Group, Inc., 1975).

[56]See, 28 C.F.R. Part 20, Appendix § 20.22(a).

[57]Technical Report No. 13, 3rd ed., *supra* note 8. The second revision occurred in 1977, at which time the commentary to the 1975 report was expanded, but the original recommendations were unchanged. Ibid., p. 1.

Under the DOJ regulations and many State laws, conviction information can be made available largely without restriction. Nonconviction data, on the other hand, can not be made available under the DOJ regulations unless authorized by a State statute, ordinance, executive order, or court rule.[58] Furthermore, the DOJ regulations provide that when CHRI is disseminated to noncriminal justice agencies, its use "shall be limited to the purpose for which it was given."[59]

Today, a relatively stable and uniform approach to protect the privacy of CHRI is in place throughout the United States.[60] Five fundamental principles, in many ways reflective of the HEW Code of Fair Information Practices, characterize the U.S. approach to protecting the privacy of CHRI:

1. **Subject access and correction**. As of 1999, 51 of the 53 jurisdictions surveyed (the 50 States plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands) give record subjects a right to inspect their criminal history records, and 44 jurisdictions permit record subjects to challenge and/or offer corrections for information in their criminal history records.[61]

1. **Restrictions on the collection and/or integration of criminal history information**. Most States have adopted formal or informal restrictions that segregate CHRI from other types of personal information. Thus, CHRI seldom includes juvenile justice information; customarily never includes investigative or intelligence information; and customarily never includes medical information, employment information, financial information, military or citizenship status information, or other types of personal information. Although repositories continue to segregate CHRI in this manner, end-users of information increasingly are able to combine CHRI obtained from the State repositories with noncriminal history record information obtained from commercial information vendors and other sources in order to create a more detailed picture of the individual.

1. **Data quality and data maintenance safeguards**. As of 1999, 52 of 53 jurisdictions have adopted standards for ensuring the accuracy and completeness of CHRI.[62]

   · *Fingerprint versus "name-only" access*. In virtually every State, all criminal histories maintained by a central State repository must be supported by a fingerprint record and, with certain exceptions, requests must be accompanied by a fingerprint. Fingerprint support ensures that the record maintained at the repository relates to the correct person, and that the repository's response similarly relates to the correct person. The principal exception for law enforcement requests occurs in instances where the law enforcement agency does not have the individual in custody and, therefore, cannot provide a fingerprint, or in situations requiring a quick turnaround. In those instances, a "name-only" check (customarily, not just a name but also other demographic information, such as gender, date of birth, race, and other physical indicators) is permitted.

   · *Disposition reporting*. Repositories attempt to obtain disposition information from the courts. In recent years, the percentage of arrests maintained at the repositories that include available dispositions has increased substantially; however, incom-

[58] 28 C.F.R. § 20.21(b).

[59] 28 C.F.R. § 20.21(c)(1).

[60] BJS supports a biennial survey, conducted by SEARCH, to assess State privacy practices. See, Paul L. Woodard and Eric C. Johnson, *Compendium of State Privacy and Security Legislation: 1999 Overview*, NCJ 182294 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, July 2000). Hereafter, Compendium.

[61] Ibid., p. 16.

[62] Ibid.

plete records remain a problem.[63]

- *Sealing and purging*. As of 1999, 42 States have adopted laws that permit the purging (destruction) of nonconviction information and 27 jurisdictions have adopted standards for the purging of conviction information if certain conditions are met. In addition, 33 States have adopted laws and regulations to permit the sealing of nonconviction information and 30 States have adopted laws and standards to permit the sealing of conviction information.[64]

2. **Security**. As of 1999, 42 jurisdictions have adopted formal standards for technical, administrative, physical, and/or personnel security.[65] As a practical matter, however, security standards are in place for all 52 jurisdictions that have established central State repositories. The extent and nature of those standards, however, vary substantially.

3. **Use and disclosure**. As of 1999, all 53 jurisdictions have adopted laws or regulations setting standards for the use and/or dissemination of CHRI.[66] As a practical matter, every State makes all CHRI available for criminal justice purposes. Outside of the criminal justice system, however, conviction information is widely available but nonconviction information remains largely unavailable or available only to certain types of users (licensing boards and certain kinds of employers who employ individuals in highly sensitive positions, such as school bus drivers or child care workers).[67] (Of course, sealing and purging provisions also work effectively to provide dissemination and confidentiality safeguards.)

- *Criminal justice access*. Law and policy in every State provides that criminal justice requestors can obtain all information in the criminal history record unless the information has been sealed by statute or court order. Most States, however, have some process for sealing or purging CHRI when it is no longer considered relevant.

- *Noncriminal justice access*. The repositories provide CHRI to noncriminal justice requestors authorized by State law, such as licensing boards and certain types of employers. In most States, authorized noncriminal justice requestors receive less than the full record — most often limited to conviction-only information.

- *Public access*. Except in a few "open record" States, such as Florida and Wisconsin, the general public is restricted in its ability to obtain CHRI from the central State repository, with the exception of certain classes of information, such as sex offender registry information.

[63]As of 1999, the most recent year for which figures are available, 18 States and the District of Columbia report that 80% or more of arrests within the past 5 years in the criminal history database had final dispositions recorded, while 32 States and the District of Columbia report that 60% or more of the arrests in the past 5 years have final dispositions attached. Overall, the figures are lower when arrests older than 5 years are factored in. When arrests greater than 5 years old are included, only 15 States report that 80% or more arrests in their entire criminal history database have final dispositions attached, while 32 States report that 60% or more arrests have dispositions attached. Sheila J. Barton, *Survey of State Criminal History Information Systems, 1999*, Criminal Justice Information Policy series, NCJ 184793 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, October 2000) p. 2.

[64]Compendium, *supra* note 60, p. 16.

[65]Ibid.

[66]Ibid.

[67]Traditionally, law and policy has distinguished sharply between conviction and nonconviction information. In many jurisdictions, conviction information is available to broad segments of noncriminal justice employers and other authorized users, if not the general public, through central repositories. By contrast, nonconviction information, even in 1999, is almost never publicly available from central repositories, with rare exceptions in some States for special categories of offenses, such as sex offenses.

Access to criminal history record information in "open," "intermediate," and "closed" record States: Three case studies

Florida: An "open records" State

In 1977, the Florida Department of Law Enforcement (FDLE) adopted a policy of making all State-generated criminal history records available upon request by any member of the public for any purpose, upon payment of the applicable fees, which are designed to offset the costs of public record access requests.

The policy, which is designed to implement the State's public record law, is interpreted in conjunction with Chapter 943 of the Florida Statutes, which regulates the collection, maintenance, and dissemination of criminal justice information. Section 943.053(2) effectively restricts the applicability of the State public records law to Florida-generated records by providing that criminal justice information obtained from the Federal government and other States shall only be disseminated in accordance with Federal law and policy, and the law and policy of the originating States. Similarly, section 943.054(1) restricts the ability of FDLE to make available any information derived from a system of the U.S. DOJ to only those noncriminal justice purposes approved by the Attorney General or the Attorney General's designee.

During fiscal year 1998-1999, FDLE responded to 1,484,273 requests for criminal history record checks. Criminal history checks for sensitive employment, licensing, and firearms purchases identified 264,148 individuals with criminal histories. Noncriminal justice recipients of criminal history records fall into two broad categories. The first category is comprised of agencies and organizations with approved statutory authorizations to receive information from the FBI as well as FDLE. As of September 30, 1999, this category included 221 agencies with FBI-assigned originating agency identifiers (ORIs) signifying approval of their access authority by the U.S. Attorney General. This category is comprised primarily of State departments and agencies authorized to access information for employment background checks, but the list also includes licensing bureaus, universities, State commissions, and the agency responsible for running the State lottery. For the fiscal year ending June 30, 1999, these agencies filed 271,230 records requests for approved licensing and employment purposes.

The second category is comprised of agencies and organizations without statutory authorization that are eligible to receive information only from FDLE files pursuant to the public records law. There is a $15 fee for processing requests made either by letter or electronic submission. Requestors in this second category can request a search of Florida-generated criminal records for any purpose, by paying the appropriate fee. These inquiries are typically "name only," although fingerprints will be compared if supplied by the requestor. Responses to these requests include all unsealed, Florida-generated criminal history records in the FDLE computerized files. As of September 30, 1999, this category includes approximately 15,913 agencies and organizations that filed 1,001,307 criminal record access checks under the public records law during fiscal year 1998-1999. These requests were filed by all levels and types of agencies for a wide variety of purposes, although FDLE officials report the most common reason was employment screening. Most of these agencies are regular users that have been assigned account numbers to facilitate billing and processing. Other requests are received on a one-time-only or irregular basis from agencies or individuals for undetermined purposes.

In addition to requests for an individual's entire criminal history record, FDLE administers databases of sexual offenders and sexual predators (as defined under Florida law) that the public can search over the Internet.

Searches can be conducted on-line, instantly, on the basis of county, city, ZIP code, and/or pattern for last name. FDLE estimates that these databases, which contain records on approximately 15,650 offenders, received 347,245 hits during fiscal year 1998-1999.

Sources:

- Florida Department of Law Enforcement.
- Florida Department of Law Enforcement, *Annual Performance Report, Fiscal Year 1998-1999.*
- Florida Department of Law Enforcement Internet site: **http://www.fdle.state.fl.us**
- Paul L. Woodard, *A Florida Case Study: Availability of Criminal History Records, The Effect of an Open Records Policy* (Sacramento: SEARCH Group, Inc., 1990).

Washington: An "intermediate records" State

The Washington State Patrol (WSP) is responsible for the maintenance of the Washington repository of CHRI.

Certified criminal justice agencies may request and receive CHRI without restriction for criminal justice purposes.

Noncriminal justice entities and individuals may receive access to only conviction information. Depending upon the purpose of the request, WSP may respond under two different statutes, the *Criminal Records Privacy Act* (Chapter 10.97 Revised Code of Washington (RCW)) or the *Child and Adult Abuse Information Act* (RCW §§ 43.43.830-.845). Responses to information requests made using Washington Access to Criminal History (WATCH), an online system, are immediate. Paper requests take 3-10 weeks for processing. Fees, which are waived for nonprofit organizations in certain circumstances, range from $10 for a "name-only" search to $25 for a fingerprint-supported search. WSP estimates that, from 1996 through 1999, it has responded to 1,128,392 noncriminal justice requests for CHRI.

Requests made pursuant to the *Criminal Records Privacy Act*, which provide the requestor with conviction information, can be made by anyone for any purpose, without the consent of the record subject. If there is a record, the requestor will receive a report detailing all State of Washington convictions and pending arrests under 1 year old without disposition. The record will also reflect whether the individual is a registered sex offender or kidnapper. Secondary disclosure of CHRI obtained pursuant to the statute, however, is restricted. WSP estimates that, from 1996 through 1999, it has responded to 392,218 requests for CHRI by noncriminal justice agencies under this Act.

Eligibility for access to CHRI under the *Child and Adult Abuse Information Act* is "limited to businesses or organizations licensed in the State of Washington; any agency of the State; or other governmental entities that educate, train, treat, supervise, house, or provide recreation to developmentally disabled persons, vulnerable adults, or children under 16 years of age." If a record exists, it will include "State of Washington convictions and pending arrest offenses under one year old of crimes against children or other persons, crimes of financial exploitation, civil adjudications, and sex offender and kidnapper registration information." The State requires that the requestor provide a copy of the report to the record subject. Use of records obtained by employers pursuant to this Act is limited by RCW 43.43.835(5) to "making the initial employment or engagement decision." Further dissemination or use of the record is prohibited. Violators are subject to civil damages. WSP estimates that, from 1996 through 1999, it responded to 692,734 requests from businesses/organizations/employers. This includes volunteer and employee record checks. WSP does not maintain statistics specifically regarding the number of employers who requested information.

WSP does not make sex offender information publicly available over the Internet, although some local departments do so. WSP does make some sex offender information available for certain employment background checks. WSP disseminates limited information on sex offenders to the general public in response to written requests. Based upon the risk level of the offender, local law enforcement may notify neighbors and community members or, in the case of high-risk offenders, issue press releases. WSP estimates that it responded to 36 written requests for information on specific sex offenders during 1999. These were specific requests for a list of sex/kidnapping offenders through the WSP Public Disclosure Office. Information provided includes name, date of birth, registering agency, and the date of registration.

Sources:

- Washington State Patrol.
- Washington State Patrol Internet site: **http:// www.wa.gov/wsp/crime /crimhist.htm**
- Devron B. Adams, *Update 1999: Summary of State Sex Offender Registry Dissemination Procedures,* Fact Sheet series, NCJ 177620 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, August 1999) p. 7.

Massachusetts: A "closed records" State

The Massachusetts Criminal History Systems Board (CHSB) was created in 1972 by the *Criminal Offender Record Information Act* (CORI) and is governed by a 17-member board comprised of representatives of the criminal justice community.

Criminal justice requests for criminal history records are handled electronically, while public access requests, which are restricted, are processed using the U.S. mail and email.

Public access requests must include the name and date of birth of the person who is the subject of the inquiry. There is a $25 fee for processing requests, which must be typed and accompanied by a self-addressed, stamped envelope. Not all criminal history records are available to the public. The determination of public access depends upon a number of factors, including the charge, the sentence, current status, and length of time that has passed since sentence completion. Specifically, in order for the information to be publicly accessible, the record subject must have been:

- Convicted of a crime punishable by a sentence of 5 years or more; or
- Convicted of any crime and sentenced to a term of incarceration.

In addition, at the time of the request for access to the individual's criminal history record, the record subject must:

- Be incarcerated; or
- Be on probation; or
- Be on parole; or
- Have been convicted of a misdemeanor, having been released from all custody (that is, incarceration, probation, or parole) or supervision for not more than 1 year; or
- Have been convicted of a felony, having been released from all custody (that is, incarceration, probation, or parole) or supervision within the last 2 years; or
- Have been sentenced to the custody of the Department of Correction, having finally been discharged therefrom, either having been denied release on parole or having been returned to penal custody for violating parole, for not more than 3 years.

CHSB estimates that it received 12,373 public access requests during 1999.

CHSB certifies applicants for access to non-publicly available criminal history information if the requestor: (1) qualifies as a criminal justice agency; (2) qualifies as an agency or individual authorized to have access by State law; and/or (3) it has been determined that the public interest in disseminating such information clearly outweighs individual privacy interests. There are approximately 6,700 noncriminal justice agencies in Massachusetts authorized to access criminal records. Parents, for example, can seek access to all conviction and pending case information on prospective day-care providers with the written, notarized consent of the record subject. Parents are prohibited from disclosing any results of the criminal history check to third parties. In addition, Massachusetts law prohibits a person from requesting or requiring a record subject to produce a copy of his or her record, unless authorized to do so by CHSB. In 1999, CHSB processed 659,808 requests for access to criminal history information that is not publicly available.

Sex offender information is subject to separate rules. Massachusetts makes information available about registered sex offenders classified by the Massachusetts Sex Offender Registry Board (SORB) as posing a moderate or high risk (after the offender has an opportunity for administrative evidentiary proceedings). Registry information may be obtained in person at local police departments or by requesting information from the SORB by mail.

The form of public inquiries is limited. If a member of the public makes an in-person request, he or she may:

1. Inquire whether a specifically named individual or a person described by sufficient identifying information to allow the police to identify the individual is a sex offender; **or**
2. Inquire whether any sex offenders live or work within the same city or town at a specific address, including, but not limited to, a residential address, business address, school, after-school program, daycare center, playground, recreational area, or other identified address; **or**
3. Inquire whether any sex offenders live or work at a specific street address within the city or town where the person is requesting sex offender information; **or**
4. Where the police department is located in a city or town with more than one ZIP code area, the inquiry may ask whether any sex offenders live or work within a specified ZIP code. In Boston, such inquiry may be made by specified police district.

Only option one (inquiries about named individuals) is available in the case of written requests to the SORB.

If an in-person request results in the identification of a sex offender, the requestor will be provided with the offender's name, home address, work address, age, sex, height, weight, eye and hair color, the sex offenses committed and the dates of conviction and/or adjudication, and a photograph of the offender, if available. If a written request is submitted to the SORB, the requestor will be provided with a report identifying whether the person is a sex offender with an obligation to register; the offenses for which he/she was convicted or adjudicated; and the dates of such convictions or adjudications. Responses to both personal and mail requests are provided free of charge and all information provided includes language cautioning that the misuse of sex offender information for purposes of harassment or discrimination is prohibited.

Sources:

- Massachusetts Criminal History Systems Board.
- Massachusetts Sex Offender Registry Board Internet site: **http://www.state.ma.us/sorb**

V. Change drivers and trend lines: The basis for a new look at privacy and criminal justice information

By the late 1990s, 10 interrelated and fundamental developments were outflanking the generation of privacy and information safeguards that emerged in the 1970s and the 1980s.

These trends and change drivers have overtaken traditional rules for access and use, arguably requiring new rules to re-establish the balance between privacy and disclosure of criminal justice information.[68] On one side of the equation, there is growing public concern about privacy in general, and the confidentiality of personal information in particular. On the other side, there are a number of cultural-, technological-, and policy-driven factors that tend to promote greater access to criminal justice information. The Task Force concludes that many of these change drivers are irreversible. What is not irreversible, however, is the degree to which these change drivers will inform future privacy standards for criminal justice information. By identifying the change drivers set forth below, the Task Force hopes to encourage effective debate as to a new generation of criminal justice information privacy standards.

- **Public concern about privacy**. In the late 1990s, the American public registers the strongest concerns ever recorded about threats to their personal privacy from both government and business. Ninety-four percent of respondents said in a 1999 survey that they are concerned about the possible misuse of their personal information. Of the concerned, 77% said they were "very concerned."[69]
- **The "Information Culture."** A new and emerging culture of information access and use facilitated by personal computers, browsers, search engines, online databases, and the Internet has helped to create a demand for, and a market in, information, including criminal justice information, while at the same time fostering in many a sense of lack of control over one's personal information and a loss of privacy.
- **Technological change**. Revolutionary improvements in information, identification, and communications technologies (including increasingly advanced software applications and Internet-based technologies), and the increased affordability of these technologies, fuels the appetite for information and creates new players in the criminal justice information arena.
- **System integration**. Initiatives to integrate criminal justice information systems operated by law enforcement, courts, prosecution, and corrections — as well as to integrate these systems with information systems maintaining other types of personal information — create powerful new information resources. At the same time, these integration initiatives may create uncertainty about the types of privacy laws and policies that apply to these new systems, and dilute existing policies designed to keep information separate.
- **New approach that closely resembles a "Business Model" for the criminal justice system**. Two fundamental changes in the way the criminal justice system operates — (1) a new, more cooperative,

[68] These trends and change drivers reflect elements of cause and consequence. It is, of course, not as important to assign degrees of causality to these developments as it is to identify and understand these developments and the nature of the challenge that they pose to established criminal justice information policy and privacy standards.

[69] *IBM Multi-National Consumer Privacy Survey*, October 1999, p. 71, available at **http://www.ibm.com /services/e-business/priwkshop.html**. Hereafter, IBM Consumer Privacy Survey.

community-based relationship between criminal justice agencies and citizens; and (2) added criminal justice agency responsibilities to provide information to surrounding communities, Federal, State, and local agencies, other police departments, and other organizations — have had a profound impact upon the approach that criminal justice agencies take to obtaining and using information. This new approach — a "data-driven, problem-solving approach" — also creates privacy risks through a wider circulation of criminal justice information.

- **Noncriminal justice demand**. A persistent and ever-increasing demand by noncriminal justice users to obtain CHRI has had a pervasive and important impact on the availability of information.
- **Commercial compilation and sale**. Changes in the information marketplace, which feature the private sector's acquisition, compilation, and sale of criminal justice information obtained from police and, more particularly, court-based open record systems, are making information similar to that found in criminal history records more widely available to those outside the criminal justice system.
- **Government statutes and initiatives**. A host of new government initiatives and laws, aimed at providing criminal justice information to broader audiences, on a more cost-effective and timely basis, has also fueled the availability of criminal justice information.
- **Juvenile justice reform**. Demands for juvenile justice records, particularly those involving violent offenses, which result in treating juvenile information in a way that very much resembles the handling of adult records, is also putting pressure on traditional information and privacy policies.
- **Intelligence systems**. Criminal justice intelligence systems are being automated, regionalized, and armed with CHRI and other personal information to create detailed personal profiles for law enforcement use.

Information privacy concerns at a historic high level

Today, concern about information privacy in the United States is at a high-water mark. This concern is evidenced in public opinion survey results, government attention to the privacy issue, and media treatment of government and private-sector initiatives that are viewed as an impingement on privacy or fair information practices.

— Public opinion survey results

Periodic surveys, including those conducted by Harris Interactive and Opinion Research Corporation in association with Dr. Alan F. Westin,[70] repeatedly indicate that the public is deeply concerned about privacy.

The growing traction of privacy as an issue can be illustrated by the following statistics from public opinion surveys concerning consumer privacy issues:

- A 1999 *Wall Street Journal*/NBC News survey asked respondents this question: "Which one or two issues concern them the most about the next century?" With 29 percent of respondents, the potential "loss of personal privacy" topped the list, finishing ahead of concerns about issues such as terrorism, overpopulation, world war, and global warming.[71]

[70]As previously noted, one of the responsibilities of the National Task Force was to provide advice with respect to the first-ever national opinion survey of the public's attitudes about privacy and criminal justice information. The results of that survey, which was developed and administered by Opinion Research Corporation concurrent to the preparation of this report and conducted once this report was largely finished, is being published separately by BJS as a companion report titled "Privacy, Technology and Criminal Justice Information: Public Attitudes Toward Uses of Criminal History Information, Summary of Survey Findings" (NCJ 187633).

[71]Albert R. Hunt, "Americans Look to 21st Century With Optimism and

- In the late 1990s, the American public registered the strongest concerns ever recorded about threats to their personal privacy from both government and business. In a 1999 survey, 94% of respondents said they are concerned about the possible misuse of their personal information. Of the concerned, 77% said they were "very concerned."[72]
- In that same 1999 survey, 72% of Internet users said they were "very" concerned about threats to their personal privacy today when using the Internet, and 92% said they were "very" or "somewhat" concerned. However, 66% believed that the "benefits of using the Internet to get information, send email, and to shop far outweigh the privacy problems that are currently being worked on today."[73]
- A mid-1990s survey indicated that although a narrow majority of survey respondents worried primarily about government invasions of privacy (52% in 1994 and 51% in 1995), a substantial minority expressed primary concern about activities of business (40% in 1994 and 43% in 1995). And, almost two-thirds of the public *disagreed* with the statement that "the Federal Government since Watergate has *not* been seriously invading people's privacy (64% in 1990 and 62% in 1995)."[74]
- Surveys suggest that the driving factors behind privacy attitudes, both in general and in specific consumer areas, are the individual's level of distrust in institutions and fears of technology abuse.[75]
- A large percentage of the public feels that consumers have "lost all control over how personal information about them is circulated and used by companies."[76]
- Seventy-two percent said they have read or heard a great deal or a moderate amount about invasion of privacy in the past year. One-quarter of the public (25% in 1991 and 1995) said they have *personally* been victims of what they felt was an invasion of their privacy,[77] and 29% (in 1999) said they had been victims of a business invasion of their consumer privacy.[78]
- There has also been a major increase in privacy-asserting behaviors by U.S. consumers. The percentage of people who said they have

Confidence," *Wall Street Journal* (September 16, 1999) p. A9. On the other hand, in 1995, when an Equifax/Harris survey gave respondents a list limited to nine *consumer* issues to rate in importance, privacy finished exactly in the middle (fifth) in terms of being "very important," at 61%. Rated higher in being very important were controlling the cost of medical insurance (84%); staying out of excessive debt (83%); reducing insurance fraud (74%); and controlling false advertising (71%). See, *infra*, note 74.

[72]IBM Consumer Privacy Survey, *supra* note 69, p. 71.

[73]Ibid., pp. 72, 77.

[74]Louis Harris and Associates, *Equifax-Harris Mid-Decade Consumer Privacy Survey* (1995) p. 9.

[75]Ibid., p. 12. The Harris/Westin Distrust Index, first used in 1978 and tested throughout the 1990s, combines measurement of distrust in institutions (government, voting, and business) with fear that technology is almost out of control. The surveys have found that a respondent's score on the Distrust Index correlates with a majority of that respondent's positions on privacy in general and the industry-specific questions on each survey.

The higher the Distrust Score, the more a respondent will express concern about threats to privacy, believe that consumers have lost all control over uses of their information by business, reject the relevance and propriety of information sought in particular situations, call for legislation to forbid various information practices, etc.

In 1995, for example, the American public divided as follows on the Distrust Index:

- High (distrustful on 3-4 questions): 29%
- Medium (distrustful on 2 questions): 42%
- Low (distrustful on 1 question): 23%
- Not (no distrustful answers): 6%

In 13 of the survey's 16 questions asking about general privacy concerns and measuring specific privacy attitudes, the strongest privacy positions were registered by the High Distrustful respondents; the next strongest by the Medium Distrustful; and so on through the Low to Not Distrustful. In survey terms, this is confirmation of the direct relationship between the Distrust orientation and positions on privacy issues. Ibid.

[76]IBM Consumer Privacy Survey, *supra* note 69, p. 70.

[77]Louis Harris and Associates, Inc., *1996 Equifax/Harris Consumer Privacy Survey* (1996) p. 4.

[78]IBM Consumer Privacy Survey, *supra* note 69, p. 74.

refused to give information to a business or company because they thought it was not needed or was too personal has risen from 52% in 1990 to 78% in 1999. Also in 1999, 53% of respondents said they have asked a company not to sell or give their name and address to another company, and 54% said they had decided not to use or purchase something from a company because they were not sure how their personal information would be used.[79]

— Activity at the Federal and State level to protect privacy

This high level of public concern about privacy issues has not gone unnoticed by the Federal government and States. Recent congressional activity suggests that Congress likely will be increasingly active on a range of privacy issues.[80] For example:

- Perhaps the most prominent piece of privacy legislation to be enacted during the 106th Congress was Title V of the *Gramm-Leach-Bliley Act* (G-L-B Act).[81] It requires that financial institutions take steps to protect the privacy of nonpublic financial information about consumers, including providing notice and an opportunity to opt-out of most disclosures of nonpublic personal information to nonaffiliated third parties. The enactment of the G-L-B Act, however, has not ended the debate. Many members of Congress believe that still stronger protections are needed.
- Senator Richard Shelby (R-AL) included language in the Department of Transportation Appropriations Act for fiscal year 2000[82] that requires the States to adopt an opt-in mechanism for use of personal information in motor vehicle records for marketing (excluding insurance rate setting), survey, or solicitation purposes, and for any use of driver's license photographs.
- Other domestic privacy issues receiving congressional attention include health information privacy issues, online privacy, the use and disclosure of the Social Security number, access to public record/government repository information, and the possible creation of a privacy study commission.

Privacy is an issue that cuts across political and ideological boundaries. On February 10, 2000, for example, Senator Shelby, Senator Richard Bryan (D-NV), Representative Ed Markey (D-MA), and Representative Joe Barton (R-TX) held a news conference to announce the formation of the bipartisan, bicameral Congressional Privacy Caucus (CPC). The purpose of the CPC is to: (1) educate Members of Congress and staff about individual privacy issues; (2) provide a forum for the discussion of individual privacy issues; and (3) advocate for personal privacy protections.

The State legislatures have also been active on privacy issues. During 2000, at least 1,622 consumer privacy bills (focusing on financial services, health, insurance, direct marketing, telecommunications, and online/Internet services) were introduced in State legislatures and 422 bills were enacted. Thirty-nine States enacted legislation, with health, finance, and insurance-related measures being the most common enactments.[83] In another example, groups as diverse as the American Civil Liberties Union (ACLU) and Phyllis Schlafly's Eagle Forum have supported health information privacy legislation.

[79]Ibid., p. 87.

[80]This is not to say that Congress also has not been criticized as being insensitive to privacy concerns. Congress, for example, passed legislation requiring a unique national health identifier for every American (to facilitate health care), as well as a requirement that all States use an individual's Social Security number as the person's driver's license number (to combat illegal immigration). Congress later reversed itself in both cases, following complaints about the adverse privacy implications of these measures.

[81]Pub. L. No. 106-102.

[82]Pub. L. No. 106-69, § 350.

[83]*Privacy & American Business*, "Privacy Legislation in the States – 2000" (January 2001).

At the same time, the Federal executive branch has launched numerous privacy protection initiatives. The Federal Trade Commission (FTC), the Federal Communications Commission, the U.S. DOJ, the U.S. Department of Health and Human Services, the Office of Management and Budget, the Office of the Vice President, the Federal financial regulatory agencies, the National Highway Transportation and Safety Administration (on intelligent vehicle-tracking systems), and the U.S. Department of Commerce have all published privacy-related regulations or guidelines; conducted privacy studies; initiated privacy-related, administrative actions; and/or promoted information privacy initiatives.

State officials have also been active on the privacy issue. The National Association of Attorneys General, for example, has voted to make privacy one of their top priorities and several Attorneys General have already taken legal action against companies they believe to be misusing consumer data.[84] In addition, the Governor of Washington issued an Executive Order requiring State agencies to implement a set of privacy protections for public records to the maximum extent permitted by State law.[85]

[84]Gail Appleson, "Drive to Protect U.S. Consumer Privacy, " Reuters (March 24, 2000, 3:47 PM ET).

[85]Governor Gary Locke, "Public Records Privacy Protections," Washington State Executive Order 00-03 (April 25, 2000).

— **Privacy issues are receiving increasing media attention, often requiring companies and government agencies to modify their practices**

Media coverage and its aftermath is also illustrative of increasing concern over information privacy issues. Typically, this cycle begins with media reports highlighting government or private-sector information practices that raise privacy issues. Once these practices become well-publicized, an ensuing firestorm of public pressure frequently forces the private- or public-sector entity responsible to modify or terminate the practices that offended public sensibilities. To date, although a few of the more prominent privacy firestorms have involved information that may have been used by law enforcement to some degree for intelligence or investigative purposes, the most notable of these "firestorms" have not involved criminal justice information.

Examples of private-sector privacy firestorms during the past 2 years include: Internet advertising giant DoubleClick; Image Data, a small New Hampshire company test marketing the use of DMV photographs for anti-fraud and identity theft prevention purposes; America Online (AOL); and supermarkets and pharmacies, such as Giant and CVS.

· **DoubleClick**. During its 4-year life, Internet advertising giant DoubleClick has collected clickstream information from its participating Web sites and then used that data to help those Web sites customize the banner and pop-up advertisements that visitors see. DoubleClick could not identify the visitor, only the visitor's computer. The privacy firestorm began in November 1999 when DoubleClick spent $1.7 billion to purchase Abacus Direct, the largest database of consumer catalogue activity. DoubleClick's plan, which drew intense criticism, was to marry its clickstream data with Abacus' offline data to identify specific consumers (not just their computers), and then create a profile of the consumer's interests and buying activity.

Not only did DoubleClick receive a torrent of adverse media coverage, it also received over 100,000 consumer complaints in response to an online protest organized by the Center for Democracy and Technology. In addition, the FTC, as well as the attorneys general of Michigan, Connecticut, New York, and Vermont, announced an investigation of DoubleClick's activities; several class-action lawsuits had been filed; and Internet-industry players, such as search engine AltaVista Co. and Internet home delivery

service Kozmo.com Inc., took steps to distance themselves from DoubleClick. If that had not been enough, the company's stock price fell by more than 25 percent during the firestorm, but rebounded somewhat following the company's announcement on March 2, 2000, that it would not go forward with the profile plan.[86]

- **Image Data.** One of the largest privacy firestorms of 1999 began in January 1999 when the *Washington Post* reported that Image Data, a small New Hampshire company, had developed a product designed to combat check and credit card fraud and identity theft, using State DMV photographs. Image Data had entered into contracts with several States, whereby Image Data was permitted to digitize DMV photographs of individuals and store the photographs in a database. Under Image Data's plan, merchants would be able to access this database, using a small screen installed near the merchant's cash register, to verify the identity of the purchaser when the customer presented the merchant with a check or credit card.

  Image Data had entered into agreements with South Carolina, Colorado, and Florida to obtain driver's license photographs and other information and was testing its program in South Carolina when the *Post* story broke. A public outcry ensued with State officials receiving a torrent of angry telephone calls protesting the plan (a class-action lawsuit was even filed in Florida). Public ire appears to have been a product of several factors. As one South Carolina woman described it: "We were livid [upon hearing about the Image Data program]. In my opinion, a South Carolina driver's license is a need, not a want. We have no choice but to give our information in order to have one. Then they turn around and sell it to a company, as personal as it is: my weight, my height, my address — my God, my image. There are endless possibilities as to what could be done with it."[87] As a result of the public outcry that ensued, all three States terminated their contracts with Image Data. South Carolina, the only State that had transferred photos before the story broke, sought to retrieve any photos already transferred. Image Data is reported to be moving forward with its program on an "opt-in" basis, giving consumers the option of having their driver's license photograph added to the Image Data database.

  In the months subsequent to the initial story, reports arose alleging that the Secret Service and other Federal agencies intended to use the Image Data database of photographs for counterterrorism, immigration control, and other law enforcement activities. Both the Secret Service and Image Data have denied this charge, stating that while Federal authorities expressed interest in the technology (and Congress "earmarked" funds for the program in 1997), the database developed by Image Data was never a part of these discussions.[88]

- **America Online.** America Online announced a new privacy policy incorporating

[86]"DoubleClick Cries 'Uncle' …Sam (Sort of)," *Privacy Times*, Evan Hendricks, ed., Vol. 20, No. 5 (March 3, 2000) pp. 5-6. See also, *Bloomberg News*, "DoubleClick in Settlement Discussions" CNET News (Mar. 23, 2000), available at **http://aolcom.cnet.com/news/0-1005-200-1582990.html**.

[87]Robert O'Harrow, Jr., "Drivers Angered Over Firm's Purchase of Photos," *Washington Post* (January 28, 1999) pp. E1, E8. See also, Robert O'Harrow, Jr., "Posing a Privacy Problem? Driver's License Photos Used in Anti-Fraud Database," *Washington Post* (January 22, 1999) pp. A1, A22; Robert O'Harrow Jr. and Liz Leyden, "Sale of License Photos Sparks Uproar, Colorado Governor Vows to Prevent Transfer to Private Firm," *Washington Post* (January 30, 1999) p. E1; Robert O'Harrow, Jr., "Gov. Cancels Sale of Fla. Driver License Photos to Private Firm," *Washington Post* (February 2, 1999) p. E3.

[88]See, David McGuire, "Feds Deny Alleged Misuse of Photo Database," *Newsbytes* (September 7, 1999), available at **http://www.infowar.com/class_1/99/class1_090899a_j.shtml**.

"Eight Principles of Privacy," following well-publicized reports of privacy breaches of AOL subscriber information, including the proposed sale of subscribers' home telephone numbers and the case of Timothy McVeigh (no relation to the convicted Oklahoma City bomber of the same name). McVeigh was discharged from the Navy for violating its policy on homosexuals as a result of personal information the Navy obtained from AOL about McVeigh, without a search warrant or McVeigh's consent.

- **CVS/Giant Pharmacies**. In February 1998, the *Washington Post* reported that two pharmacy chains — CVS and Giant — used, or planned to use, an outside contractor to send prescription refill notices and drug promotional materials to pharmacy patrons using prescription information supplied by the pharmacies. Within days of the initial media report, both companies took out full-page advertisements announcing the cancellation of the programs, amid a flurry of editorial criticism and customer complaints. CVS has since been sued, with the plaintiff alleging that CVS breached its fiduciary duty as well as its duty of confidentiality to its pharmacy customers. A State court rejected a motion to dismiss by the defendants, concluding that there is enough in the complaint for a jury to resolve, and the case is still pending.[89]

Media glare and public outrage over privacy missteps is not limited to the private sector. Examples of governmental privacy missteps over the past few years include the "Know Your Customer" proposal of the Federal Deposit Insurance Corporation (FDIC); the OASIS proposal of the Health Care Financing Administration (HCFA); a U.S. Postal Service proposal regarding private mailboxes; and a Social Security Administration initiative to provide individuals with online access to their Social Security earnings records.

- **Know Your Customer.** One of the most controversial Clinton Administration proposals, from a privacy perspective, was the FDIC's proposed "Know Your Customer" (KYC) regulations. The proposed KYC rule would have required all banks to develop a written program designed to enable the bank to "provide for identification and transaction monitoring procedures and identify transactions that would be subject to suspicious activity reporting requirements." According to the FDIC, the proposed regulation was intended to protect the integrity of the banking system and to "assist the government in its efforts to combat money laundering and other illegal activities that may be occurring through financial institutions. It is intended to detect patterns of illegal activity often characterized by large cash deposits and withdrawals that are outside the normal and expected activity." Some opponents characterized the measure as turning bank tellers into government informers and citizens into criminal suspects.

Opposition to the proposed KYC rule was widespread, including an Internet-based campaign against the measure. The FDIC was deluged with criticism about the proposal, including a flood of complaints from individuals. The agency received over 250,000 comments on the proposed rule; all but a small handful of the comments received were hostile to the proposal. Hostility toward the proposed KYC rule came not only from the grass roots level, but also on Capitol Hill where a half-dozen bills designed to prohibit the implementation of the rules were introduced. In March 1999, the FDIC and the other agencies that sponsored the measure announced they were withdrawing the measure in its entirety.

- **Outcome and Assessment Information Set.** The HCFA was caught in a privacy storm in the spring of 1999 as a result of its

[89] *Weld* v. *CVS*, Superior Court of Massachusetts (Suffolk) No. 98-0897.

planned "Outcome and Assessment Information Set" (OASIS) for home health care patients, which HCFA planned to have all home care facilities complete about their patients. Following adverse press coverage and criticism from privacy advocates, Vice President Gore, and numerous Congressmen, the agency postponed implementation of the project while it revamped the program. Changes were designed to ensure that: (1) only essential information would be collected; (2) the information gathered would be properly protected; (3) disclosures of the information would be limited to the minimum extent necessary to carry out the mission of HCFA; and (4) Medicare beneficiaries would be fully informed as to why information was being collected and how it would be used.

- **U.S. Postal Service.** In March 1999, the U.S. Postal Service issued a regulation requiring users of commercial mail receiving agencies (CMRAs), such as Mailboxes, Etc., to use the acronym "CMRA" in the address, thereby identifying that the address is at a CMRA (as opposed to a U.S. Postal Service post office box or a regular commercial or residential address). Mail not complying with this rule would not be delivered. The regulation was designed to help prevent the use of CMRAs as a tool for criminal activity. The regulation also required that CMRAs demand personal identification from all box renters and complete a form for submission to the Post Office, which included the box holder's Social Security number and other personal information. The Post Office would then make that form available to anyone who requested it.

  After complaints from citizens, privacy advocates, and several members of Congress, the Postal Service modified its regulation. It delayed the requirement that "CMRA" be included in the address. The post office also relaxed the registration requirements, announcing it would not make applications by small businesses publicly available and that it would advise CMRAs not to require Social Security cards as a form of identification. Some privacy advocates found these revisions insufficient and continued to oppose the regulation.

- **Social Security Administration (SSA)**. An April 1997 *USA Today* report that the SSA was making Personal Earnings and Benefit Estimates (PEBES) available to individuals over the Internet sparked another privacy furor. When the story broke on April 7, 1997, SSA initially defended the online disclosure of PEBES, which had begun approximately a month before, as a way to provide the information to taxpayers quickly and easily. SSA also noted there were severe penalties for fraudulently accessing SSA records and that in order to request a report, the individual had to supply five separate data elements: name, Social Security number, date of birth, place of birth, and mother's maiden name.

  This did not stem the criticism. Some privacy advocates, while supportive of the idea of online access, noted that all five of the data elements required for access were publicly available information, jeopardizing the security of the information and the privacy of taxpayers. Senators with key oversight responsibilities for SSA voiced reservations over the plan, and SSA was swamped with tens of thousands of calls from citizens complaining about threats to their privacy. On April 9, two days after the *USA Today* story first appeared, SSA "temporarily" suspended the online access initiative. Service has never been reinstated.[90] Instead, SSA has returned to its prior practice of allowing individuals to request PEBES statements using the Internet and mailing responses several weeks later.

[90]See, "SSA Pulls Plug on Web Page Offering Americans' Earnings," *Privacy Times*, Evan Hendricks, ed., Vol. 17, No. 8 (April 17, 1997) pp. 1-2.

— **Other indications of the importance of privacy concerns: The European Union Data Protection Directive, omnibus proposals in the United States, and self-regulatory initiatives**

The European Union Data Protection Directive

The European Union (EU) enacted the "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" (the Directive)[91] in 1995, and it became effective on October 25, 1998. The Directive is a comprehensive, omnibus privacy measure that regulates the processing of personal data.

The Directive places restrictions on the export of personal data to countries outside the EU that are deemed to lack "adequate" privacy protections.[92] European Union officials do not believe the United States has "adequate" privacy protections; therefore, U.S. companies wishing to move personal data across borders from EU countries to the United States have to negotiate contractual arrangements that satisfy the terms of the Directive or otherwise meet specific exceptions or tests (for example, consent of the data subject; important public interest test; protection of the vital interests of the data subject; or public information test).[93]

The U.S. Department of Commerce spearheaded the Clinton Administration's efforts to reach an understanding with the EU regarding the Directive's impact on transfers of personal data from the EU to the United States. In July 2000, the Commerce Department and the European Commission finalized and formalized the "Safe Harbor" agreement, after years of negotiations and several public discussion drafts.

Although the Safe Harbor accord explicitly states that it is not intended to have applicability beyond international trade, the Directive and the Safe Harbor process are having an impact on the domestic privacy debate in the United States. It is too soon to determine the extent of the impact; however, at least two factors are at work. First, the Directive and the Safe Harbor discussions have generated considerable media coverage, further raising the profile of privacy issues in the United States. Second, the Directive has increased the pressure on the United States to strengthen its privacy laws. Privacy advocates, for example, have questioned whether the Safe Harbor accord will result in two sets of privacy protections in the United States, one for information pertaining to citizens of the EU and a second, lower, standard for Americans.

Omnibus legislation

The EU Directive and growing public concern over information privacy is also evidenced in a growing trend at the State level: the active consideration of omnibus privacy legislation.

- In California, for example, State Senator Steve Peace (D-El Cajon) introduced Senate Bill 129, "The Personal Information and Privacy Act of 1999," which, as originally introduced, would have prohibited the collection, use, and disclosure of any type of personally identifiable information without the consent of the individual subject.
  - — The original bill also would have required organizations to inform individuals how and what type of information is collected and the purposes for which it is used; the types of organizations to which the information is disclosed; and the choices and means the organization offers to limit the use and disclosure of the information.
  - — The final version of the bill, which was signed into law by Governor Gray Davis in September 2000, was more

[91] Directive 95/46/EC.

[92] Under Article 2 of the Directive, "personal data" are broadly defined to include: "[A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[93] Directive, Article 26.

limited in scope than the original bill, creating a privacy ombudsman with various responsibilities, including, among others, accepting complaints about organizations from private citizens. The bill also imposes certain requirements on State agencies.[94]

- Similar efforts, while ultimately largely unsuccessful, were undertaken during the 1999-2000 legislative session in both Massachusetts and New York. The Massachusetts legislation, with the support of then-Governor Paul Cellucci and then-Lieutenant Governor (now Governor) Jane Swift, would have addressed a wide range of privacy issues ranging from how retailers and marketers handled personal information to surveillance of employees in the workplace. In New York, a package of over a dozen bills designed to safeguard the personal information of consumers, rather than a single bill, were introduced with the support of Assembly Speaker Sheldon Silver (D-Manhattan) and Attorney General Eliot Spitzer.

Self-regulatory initiatives

Finally, in part as a result of the pressure generated by media, advocacy group, and legislative and international scrutiny, and in part because consumers increasingly expect companies to provide adequate privacy, the private sector has launched several efforts to develop and implement voluntary privacy guidelines. The Individual Reference Services Group (IRSG), a trade association for companies that sell identification and location information products, has developed a set of self-regulatory principles for their member companies.[95] In another example, the Online Privacy Alliance has developed cross-sectoral privacy guidelines for companies that obtain personal information about consumers arising from online/e-commerce activity. BBBOnline and TRUSTe have developed privacy "seals" to be displayed by Internet sites adhering to certain privacy standards.

These self-regulatory programs and others require or encourage companies to provide consumers with notice about a company's information and privacy practices; a degree of choice in how much information the consumer wishes to provide or whether the consumer wishes to provide any information at all; some access and correction rights; data quality protections; security protections; and confidentiality safeguards. Increasingly, these voluntary programs also provide for verification of company compliance and some type of remedy for consumers who are aggrieved by a violation of these self-regulatory guidelines.[96]

The Information Culture

There is a considerable and growing public demand for a wide array of information, including criminal justice information. This demand is fueled by, and also fuels, technological advances that make it possible to gather and store increasingly larger amounts of information from an increasingly larger number of sources, in ever faster, more reliable, and more efficient ways. Information, including criminal justice information, also frequently marries traditional text with a variety of nontext formats including audio, video, and digital imaging.

As a practical matter, the public's exposure to criminal justice information was, for the most part, once confined to personal experience, media reports, and mugshots posted in the local post office. Today, large segments of the public expect to be able to use criminal justice information about individuals to better inform themselves about others, including their neighbors and their caregivers.[97] In addi-

[94]Codified at CAL. BUS. & PROF. CODE §§ 350-352 and CAL. GOV'T CODE § 11019.9.

[95]The IRSG is discussed in further detail in *infra*, p. 60.

[96]A comparison of the privacy protections provided by leading self-regulatory codes, certain Federal privacy laws, and the Federal justice information system privacy regulations (DOJ regulations) are included as Appendix 3.

[97]Approximately 90% of the public would allow some access to conviction records by potential employers, while 38% would favor access by individuals

tion, information, including criminal justice information, is increasingly searchable and accessible through the Internet or other electronic means.

The process builds upon itself. Technological advances make information available to the public in a new, more efficient way. Then, as the public becomes acclimated to the new technology, it comes to expect the benefits and comes to anticipate and expect new advances that will build further upon this technology, making even more information more readily available. The public increasingly expects information on demand and expects increasingly sophisticated databases and search engines to assist them in meeting their needs. This includes, but is not limited to, criminal justice information. Members of the public, while concerned about protecting their own privacy, expect to be able to access information to protect themselves and their children from risks that may be posed by offenders and others. As one commentator observed: "Given a choice between privacy and accountability, all of us can be relied upon to choose privacy for ourselves and accountability for everybody else."[98]

This shift in attitudes is apparent in the activities of business, government, and individuals and applies not only to criminal justice information, but also to information sectors throughout the economy. "If the shift to an information society means anything, it means thinking about information as one of the most important resources in society."[99] Businesses increasingly seek to gather information about their customers, storing this information electronically in "data warehouses" where it can be retrieved later for analysis for purposes ranging from inventory control to targeted marketing. Government, including the courts, criminal justice agencies, and noncriminal justice agencies, increasingly views personal information as a means to improve decisionmaking in areas ranging from child support enforcement, immigration control, and gun control, to bail decisions.

The Task Force views this move toward an "Information Culture" as an important factor in criminal justice information policy.

Changes in technology

Computers have been used to capture and manage criminal justice information since at least the late 1960s. Until recently, however, computerized criminal justice information systems merely created what amounted to an automated "file cabinet." Whoever owned the automated file cabinet had responsibility for managing the system; as a practical matter, the "owner" enjoyed substantial discretion in setting rules for the collection, retention, use, and disclosure of information maintained in that automated file cabinet. Today's powerful and nimble information systems, however, facilitate a far different environment. Users can access information from remote locations and from multiple databases. In doing so, users can create their own multidimensional, cross-sectoral, customized, personal information reports. Today, those who maintain these databases are less able to control how information in them are used. With the ability to draw and assemble information from the various databases, information users may be able to create customized, comprehensive information products for use in various settings.

These customized reports could include a mix of criminal justice and noncriminal justice information about an individual. These reports could support criminal justice applications, but could also be deployed in noncriminal justice settings. The evolution of these types of personal reports will be influenced and shaped by current and future law governing information collection, use, and disclosure.

This information management revolution is occurring contemporaneously with a revolution in

wanting to learn if a neighbor has a criminal record. Privacy Survey Report, *supra* note 4, p. 5.

[98]Chris Gaither, "Big Brother is Your Friend," *Wired News* (September 20, 1999) (quoting science fiction author David Brin).

[99]James Boyle, *Shamans, Software, and Spleens: Law and the Construction of the Information Society* (Boston: Harvard University Press, 1996) p. 174.

identification technology — such as DNA, livescan, and Automated Fingerprint Identification Systems — that gives users the potential not only for a richer, customized information product, but also for a product with a much higher degree of reliability and integrity (that is, an assurance the information truly relates to the person who is the intended subject of the inquiry).

The Internet is a dramatic and new feature on the information landscape. The Internet is an inexpensive and relatively user-friendly technology, which not only provides robust information management capabilities, but also does so on a real-time, communications platform. Furthermore, the Internet creates remarkable opportunities for national and international publication — and remarkable risks to privacy. Recently, several States have placed all or parts of their sexual offender databases on the Internet. A few States, including Texas and Washington, make conviction information available over the Internet.

These information technology advances hold enormous promise for criminal justice users and authorized, noncriminal justice users to obtain comprehensive, reliable, and customized information about individuals on a near-instantaneous basis. These advances, however, also create or, at a minimum, exacerbate privacy risks. The online availability of an individual's criminal history and criminal justice record information, along with the potential to obtain juvenile justice information, combined with information about educational background, financial status, medical information, immigration, and citizenship status is certain to ignite a new privacy debate about who should get access to this kind of information; for what purposes; and subject to what privacy safeguards and restrictions.

It is a cliché to say we are living in the "Information Age" or in an "information society" or that we are in the midst of an "Information Revolution." Nevertheless, it is undeniable that technological advances in computing and communications are significantly impacting the way in which information is viewed by the public, by the courts and criminal justice agencies, and by government agencies generally.

One way to conceptualize the manner in which technology is received and integrated by society is to think of a new technology as a physical object moving into a steel web representing society's existing rules and arrangements.

> "Technology never breaks through this social web, which is an extremely dense intertwining of economic, legal, organizational, social, and cultural constraints. Rather, a new technology makes a slow and gradual passage through the web. In the process, both the technology is shaped in its forms of application and accepted capabilities and the strands of the web are altered. Sometimes the strands open fairly widely to accommodate new forms of technological use; sometimes, they hold fairly firm to block certain uses of the technology or substantially alter its application."[100]

The strands of the "steel web," representing the way information is viewed by society, are being reshaped by the new information technologies.

One of the most significant technologies that has been making its way through the "steel web" of society is the computer. Today, the computer is a central fixture in American life. Computers are used for everything from word processing, to data storage, to inventory control at supermarkets, to advanced mathematical research. The centrality of computers is just as applicable in the criminal justice recordkeeping arena. As recently as 1986, the then-Director of the Federal Bureau of Prisons was able to refer to computers as "the ultimate status symbol."[101] Today, in

[100]Alan F. Westin, preface to Donald A. Marchand, *The Politics of Privacy, Computers, and Criminal Justice Records: Controlling the Social Costs of Technological Change* (Arlington, Va.: Information Resources Press, 1980) p. vi. Hereafter, The Politics of Privacy.

[101]Norman A. Carlson, "The Federal Bureau of Prisons and Data Quality," in *Data Quality Policies and Procedures: Proceedings of a BJS/SEARCH Con-*

contrast, it is the rarest of office worker who is without a computer on his or her desktop. In addition, advances in computing and telecommunications technologies have acclimated the public to automatic teller machines, credit cards, electronic commerce over the Internet, and a host of other innovations that depend on the ready transfer of information.

Increases in the speed of computers and communications technologies are also having an effect. While speed "for its own sake is hardly impressive," it "is important because is allows men to do things they otherwise would not have done, for lack of will, time, or energy. The development of computers signifies not just an increase in the speed of calculation, but offers as well a quantum leap in the amount and kinds of things that can be done within a human framework."[102]

This ability to do things that otherwise would not have been done due to "lack of will, time, or energy" has important implications for the privacy of criminal justice information. Technological innovations have removed (and are removing) many of the *de facto* protections — the nondiscoverability — that once protected the privacy of an individual's criminal justice information, not by any intentional design, but because there was a "lack of will, time, or energy" to obtain it.

Court records and police blotter information, for example, traditionally have been public documents available (with the exception of certain sealed records) to anyone who went to the courthouse to view them. In the past, this imposed a number of barriers and "transaction costs" on someone seeking to obtain arrest or conviction information:

- First, it was necessary to know in which of the Nation's thousands of courts or police stations to look for the record.
- Second, it was necessary to actually go to the courthouse or police station (which might be across the street or across the country) to view the records.
- Third, it took time to determine if the court or police station had a record.
- Fourth, it took time for police or court staff to retrieve the record.
- Fifth, if there was a record, further research might be necessary elsewhere to determine whether the case was prosecuted, or how the case was resolved on appeal.

In addition to the time involved, there were additional costs, which could be significant, for copying the records. Thus, while the records technically were *open* to the public, accessing the information imposed transaction costs that had the effect of *limiting* public access.

Advances in technology, however, are eliminating these barriers to access and the *de facto* privacy protections that they once afforded to those with arrest or conviction records. Courts and police departments are automating their records, and many are making this information available in an electronic format on a wholesale basis. Thus, in doing so, they permit private companies to assemble databases of criminal justice information that include information from jurisdictions across the country — "one-stop shopping" for criminal justice information. Some States go further. Texas and Washington, for example, make conviction information (and some arrest information) available to the public over the Internet. As of May 1999, 15 States allow the public to access sex offender databases over the Internet as well.[103] These databases allow

ference, NCJ 101849 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, November 1986) p. 46. Hereafter, Data Quality Policies and Procedures.

[102]Marchand, The Politics of Privacy, *supra* note 100, p. 10 (quoting Kenneth C. Laudon, *Computers and Bureaucratic Reform* (New York: Wiley, 1974) p. 6).

[103]Devron B. Adams, *Update 1999: Summary of State Sex Offender Registry Dissemination Procedures*, Fact Sheet series, NCJ 177620 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, August 1999). In addition to the 15 States that grant public access to searchable sex offender databases via the Internet, 10 States have Internet sites that are either accessible only to law enforcement or are limited information about the reg-

the public to search not only by name, but also by geographic location, such as ZIP code, so that it is possible to identify sex offenders in a neighborhood, whether the party conducting the search knows their names or not.

With the reduction of the "transaction costs" for such inquiries, it is possible to conduct background checks in an increased number of circumstances and by a wider number of people. Background checks, while once largely the province of licensing boards, banks, securities firms, and government agencies screening for sensitive national security positions, are now possible (or even required) for a much larger, and continually growing, roster of positions, including bus drivers, school janitors, daycare workers, nursing home workers, volunteer coaches, and Boy Scout troop leaders.[104] In the case of sex offender registries, there need not be an employment or volunteer relationship at all.

This trend is reflected not only in the increasing commercial sale of such information but also in the law. Employers may be found liable under common law theories of negligent hiring if they hire an individual without conducting a background check and the individual then commits an on-the-job crime.[105] Increasingly, State and Federal statutory law authorizes State central repositories to disclose CHRI for background checks for positions involving financial responsibility or for the interaction with potentially vulnerable populations, such as children and the elderly.[106]

It has been said the "strains that technology places on our values and beliefs, finally are reflected in economic, political, and ideological conflict. That is, they raise questions about the proper goals of society and the proper ways of pursuing those goals."[107] That is true of the way in which the Information Revolution is affecting the collection, use, and disclosure of criminal justice information. The fact that technology has reduced the transaction costs involved in accessing criminal justice information, removing traditional *de facto* barriers that once created protections, raises difficult questions about the proper use of criminal justice information in this new environment, including spawning a debate as to whether we should reexamine our approach to "public record information."[108] In 1998, Congress, recognizing the vital role criminal justice information, identification, and communication technologies must play, enacted the *Crime Identification Technology Act of 1998* (CITA).[109] CITA authorizes $1.25 billion over 5 years for grants to the States to upgrade criminal justice and criminal history record systems; improve criminal justice identification; promote the compatibility and integration of national, State, and local systems for a variety of purposes; and capture information for statistical and research purposes to

istry itself rather than individual offenders; 5 States without Internet sites are planning to develop them, and the remaining 20 States and the District of Columbia report having no sex offender registry site on the Internet and provided no information as to whether one was planned. Ibid.

[104]See, for example, Valerie Strauss, "Ackerman Orders Volunteer Screening," *Washington Post* (October 8, 1999) pp. B1, B4.

[105]See, *infra*, p. 53 (more public access/demand).

[106]See, *infra*, p. 61 (Federal and State initiatives).

[107] Marchand, The Politics of Privacy, *supra* note 100, p. 15 (quoting Emmanuel G. Mesthene, "The Role of Technology in Society" in *Technology and Man's Future*, Albert H. Teich, ed. (New York: St. Martin's Press, 1972) p. 148).

[108]While court records and other original records of entry have traditionally been publicly available, not all information held by the Federal and State governments is publicly available. CHRI contained in the State repositories, for example, is only available for certain purposes in many, although not all, States. In addition, the *Federal Privacy Act*, *Freedom of Information Act*, and other Federal and State laws restrict public access to a variety of information held by government agencies, including sensitive personal information, such as tax returns and health information. In May 1998, President Clinton issued an order to the heads of executive departments and agencies to review their compliance with the *Federal Privacy Act* to account for changes in technology. See, William Jefferson Clinton, "Memorandum for the Heads of Executive Departments and Agencies. Subject: Privacy and Personal Information in Federal Records," (May 14, 1998).

[109]Pub. L. No. 105-251, §§ 101-102 (October 9, 1998), 112 Stat. 1871 (to be codified at 42 U.S.C. § 14601).

improve the administration of criminal justice.[110]

The areas identified in CITA are reflective of a re-shaping of criminal justice information environment. The important theme of CITA — the integration of State, Federal, and local systems, so that the criminal justice information systems will be compatible — is discussed in detail later in this report.

— Information technologies

The importance of information technologies in the collection, organization, and dissemination of information, including criminal history information, can hardly be overstated. The increased power, utility, and affordability of computer power have revolutionized the way information is handled in the United States.

In recent years, the price of computer memory and other hardware has decreased,[111] making computers accessible not only to the largest members of the criminal justice community, but now also to the smallest.[112] Where the criminal justice community's exposure to the computer was once limited to mainframes maintained by the FBI and central State repositories, today computers can be found in even the smallest of local police departments and in patrol cars as well.

Technological advances have made computers smaller, faster, and capable of storing ever-increasing amounts of data in seemingly ever-decreasing amounts of space. Disk drive capacity now doubles at least once a year and, according to experts, this time frame is shrinking significantly.[113] The ready availability of computers at all levels of law enforcement, as well as society at large, has spurred advances in computer programming and data retrieval, making it possible for users to customize systems to meet their own institutional needs.

This increased programming and search flexibility, in turn, has supported the creation of "data warehouses" where large amounts of information are accumulated and available to be searched on the basis of a multitude of discrete selection criteria. Today, it is possible to gather and store large amounts of data about data subjects and to enrich that data with information obtained from outside sources to create detailed information profiles about individuals. It is also possible to search those profiles to identify files on the basis of almost any common characteristic. Although it once may have been possible to search a database using only an individual's name or identification number, for example, today databases can be searched using addresses, telephone numbers, or even random words. In addition, data-matching programs permit the comparison of multiple databases for overlapping data.

This was, of course, not always the case. The criminal history record system, while predating the computer, is a relatively new innovation. At the beginning of the 20th century there was hardly such a thing as a criminal history record, let alone a criminal history record system.[114] In 1924, criminal history record-keeping and fingerprinting took a step forward when Congress directed the FBI to create an "identification division" to acquire, maintain, and use fingerprint information.[115] This new identification division began

[110]Pub. L. No. 105-251, §§ 102(a), (e).

[111]Owen M. Greenspan, et. al., *Report of the National Task Force on Court Automation and Integration*, NCJ 177601 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Assistance, June 1999) p. 24. Hereafter, Task Force on Court Automation. "In 1975 an IBM mainframe cost approximately $10 million and provided 10 million instructions per second (MIPS), or about $1 million per MIPS. In 1998, a Pentium® personal computer cost approximately $2,500 and provided roughly 300 MIPS, at a cost of $6-$10 per MIPS." Ibid., at n. 26.

[112]While the cost of memory and other computer hardware has declined, technology costs incurred by courts and criminal justice agencies may not have declined overall. Agencies have shifted from an environment where there was only a mainframe, or perhaps no computers at all, to the current environment where there must be a computer of some sort at practically every workstation. In addition, as the volume of users and workstations increase, the need for technical support has also increased.

[113]Task Force on Court Automation, *supra* note 111, p. 35.

[114]"Use and Management of CHRI, *supra* note 22, p. 20.

[115]Ibid. p. 21.

with 800,000 fingerprints obtained from various sources, and maintained on manual fingerprint cards.[116] Over the succeeding years, the FBI accumulated paper fingerprint cards and information files by the millions. Each individual's file was fingerprint-supported and also retrievable by name or FBI number.[117] These records occupied huge warehouses and required armies of clerks to maintain and update.

By the 1960s, the early computer brought the first movement toward the automation to criminal history records. The expense of early computers restricted their use to only the largest institutional players, such as the FBI. Computers proliferated slowly to include State repositories and the largest of police departments. These early systems, however, were little more than automated file cabinets, with manual input requirements and limited retrieval capabilities. Automated systems were used for new entrants into the criminal justice system, while records on offenders whose records pre-dated the inauguration of the computer system were still maintained in the traditional paper format.

In addition to changing the manner in which State repositories organize and maintain criminal justice information, advances in information technologies have affected the way information is reported to the repositories by the courts and law enforcement agencies. Until recently, the automation of arrest and disposition reporting to State repositories has lagged behind the automation of disclosures from the State repositories in response to inquiries from law enforcement and the courts. Increasingly, however, computer technology is being used to automate the reporting process, thereby speeding the reporting process and saving resources.[118]

Historically, arrest information has been reported to the repositories and the FBI on fingerprint cards that also included space for textual information about the record subject. State law frequently requires that cards for reportable offenses be submitted within 24-48 hours of arrest or "promptly" or "without undue delay." However, even if these laws are complied with, mail delays and normal data processing resulted in a delay of a week or more from the date of arrest until the information was entered into the repository systems. Increased automation at the local level and direct computer-to-computer transmissions now create the potential for real-time transmission of data from the local law enforcement agency to the State repository. The same is true of disposition reporting information from the courts, which is increasingly automated with the advent of automated case management systems, particularly in high-volume jurisdictions.[119]

— Identification technologies

Means of identification

Technological advances have had a profound impact on identification capabilities. People are identifiable in many ways, including name, Social Security number, or other account number, and by physical characteristics. With the exception of physical characteristics, all of these identification methods are inherently unreliable in the criminal justice context. Names can be shared by many people and Social Security numbers can be falsified; this makes reliance on such names and numbers unreliable in many instances, which opens the door to fraud, mistake, and abuse. Physical characteristics, called "biometric identifiers," are unique characteristics for purposes of personal identification.[120] Examples of biometric identifiers include fingerprinting, DNA, retinal scanning, voice spectrography, and hand geometry scanning.[121] Although biometric identification is a

[116]Ibid.

[117]Ibid., p. 22.

[118]Ibid., p. 43.

[119]Ibid., p. 44.

[120]Robert R. Belair and Robert L. Marx, *Legal and Policy Issues Relating to Biometric Identification Technologies* (Sacramento: SEARCH Group, Inc., 1990) p. 1. Hereafter, Biometric Identification Technologies.

[121]Ibid. There are many other potential biometric identifiers including, for example, vein prints, poroscopy (pore prints), cheiloscopy (lip prints), otoscopy (ear prints), dentition prints, and sweat prints. Ibid., pp. 39-42.

more reliable means of personal identification, virtually none of the identification documents used in the United States is supported by biometric identifiers.[122]

Identification cards are the most common form of identification device. In recent years, efforts have been made to reduce the ability to falsify or counterfeit identification documents and to increase their utility to law enforcement. Some of these changes simply involve the use of inks and other materials that are more difficult to alter or counterfeit. Other innovations include MICR lines or magnetic strips, which contain identification information and are more difficult to tamper with than paper identification. It is also possible to include digitized fingerprints and other biometric identifiers on the magnetic strip or in an embedded chip, to further enhance reliability. These magnetic strips, as well as bar codes, can also be "swiped" or "scanned" through reading devices by law enforcement to quickly access the stored data.

Biometric identifiers are used in the criminal justice field not only to link suspects to crime scenes, but also as a reliable means of verifying identity for background checks. There is increasing pressure, however, to move to a name-only identification regime to produce both faster and less-expensive background checks. Such a move to name-only checks, however, is not without potential privacy and accuracy problems. First, name-only checks can result in multiple hits for individuals with common names, such as John Smith. Second, as noted previously in discussing traditional identification documents, falsification is a problem. If an individual assumes a false identity (identity fraud is an increasingly common crime), it is possible that the identity in question is that of a real person, not an identity that was simply made up by the applicant.[123] If this is true, and the applicant commits a crime, it could lead to the issuance of an arrest warrant and other problems for an innocent person.

Fingerprinting

Fingerprinting is the best-known and most widely used means of biometric identification. Attempts to use fingerprints for identification purposes, while first the subject of scientific inquiry in the 17th century, can be traced back to ancient China and Egypt.[124] Today, fingerprinting is a critical tool for law enforcement efforts to solve crime and fingerprinting criminal suspects is commonplace. The FBI, for example, receives approximately 50,000 fingerprints per day, about one-half of which come from criminal matters.[125] Outside the criminal justice setting, fingerprints are also the most widely used and recognized means of biometric identification. Children are frequently fingerprinted. In addition, job applicants and applicants for many types of licenses are fingerprinted, not only as a means of identification, but also to facilitate reliable criminal background checks.

In the criminal justice context, Automated Fingerprint Identification Systems (AFIS), which first emerged in the late 1960s, are an example of the power of information technology advances.[126] In an early AFIS, manual fingerprint records were scanned into a computer system, converted into digital records, and stored. In order to search the AFIS database, the fingerprint that is the subject of the search was digitized and compared to the existing fingerprints already digitized and on file. If the system made a potential match, a fingerprint examiner compared the fingerprints and made an actual identification determination. This technology was complemented in the 1980s by the emergence of automated, direct-read fingerprint devices. Direct-read fingerprint devices take an inkless photograph of an

[122]Ibid.

[123]In addition to the use of biometric identification, information products, frequently drawing from information contained in public records, can also assist in detecting identity fraud.

[124]Biometric Identification Technologies, *supra* note 120, p. 13.

[125]Vicki Smith, "FBI Touts Fingerprint Database: Says Police Will Get ID and History within Two Hours," The Associated Press (August 10, 1999), available at **http://www.abcnews.go.com/sections/us/dailynews/fbi990810.html**.

[126]Biometric Identification Technologies, *supra* note 120, p. 2.

individual's finger or thumb and convert that fingerprint or thumbprint into a digital record. These inkless photographs take only seconds to produce and result in a clearer image than the traditional method of "rolling" the finger on a fingerprint card to create an inked impression.[127]

The impact of AFIS, further enhanced by the increased efficiency and clarity of direct-read technology, has been substantial. In San Francisco, for example, prior to AFIS, police made approximately 60 identifications of crime scene prints each year by manually searching fingerprint files.[128] In slightly less than 4 years from San Francisco's implementation of an AFIS, police had searched over 12,000 crime scene fingerprints and made 2,500 criminal identifications, a dramatic increase.[129]

Potential privacy concerns also result from the increased efficiency brought by this new information technology. Although fingerprint searches used to be a time-consuming process, today large databanks can be searched in a very short time and with little or no additional effort by staff. This means law enforcement can conduct "cold searches" (that is, searches where there are no suspects or leads, other than fingerprints found at the scene).[130] Another result of AFIS is an increasing demand from law enforcement to expand the pool of fingerprints on file and accessible to an AFIS, thereby increasing the possibility of a match. Some criminal justice sources have argued in favor of expanding AFIS systems to include juvenile fingerprints.[131] Other potential expansions of source records for AFIS searches include child fingerprinting programs, fingerprints taken for professional licensing, fingerprints taken for security clearance applications, and employment background checks, to name a few.

The FBI launched the next generation of AFIS technology in July 1999: the Integrated Automated Fingerprint Identification System (IAFIS). Under IAFIS, fingerprint images (rather than traditional fingerprint cards) will be taken at local law enforcement agencies by livescan or cardscan equipment, processed by a local AFIS, and then transmitted electronically to the State repository for processing. If a positive identification is not made at either the State or local level, the fingerprint data and any relevant textual data will be transmitted electronically to the FBI for processing and the FBI, in turn, will electronically transmit a response to the local booking station. It is estimated the entire process can be completed in 2 hours or less, permitting local law enforcement to identify prior offenders and fugitives, even if they have provided false identification information, prior to their initial bail hearing or release from booking.[132]

Retinal scans, voice spectrography, and hand geometry

While fingerprinting is, by far, the best known and most widely used biometric identifier, there are other techniques, although they are more likely to be used for controlling an individual's access to information or locations than for criminal investigations. Retinal scans record the unique vasculature (blood vessels) in the fundus, or posterior orbit of the eye. In voice spectrography, a spectrograph produces a graphic representation of the sound emitted by a human voice. Hand geometry systems, another means of biometric identification, measure characteristics, including finger lengths, finger density, hand width, the silhouette of the entire hand, a profile view of the knuckles and back of the hand, and skin translucency. These results can then be digitized and

[127]Ibid. The appendix to the 1990 report contains a detailed and technical analysis of AFIS.

[128]Ken Moses, "Maintaining and Using Juvenile Fingerprints," in *Juvenile and Adult Records: One System, One Record? Proceedings of a BJS/SEARCH Conference*, NCJ 114947 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, January 1990) p. 50. Hereafter, Juvenile and Adult Records.

[129]Ibid.

[130]U.S. Congress, Office of Technology Assessment, *Criminal Justice, New Technologies, and the Constitution, Special Report*, OTA-CIT-366 (Washington, D.C.: U.S. Government Printing Office, May 1988) p. 19.

[131]Moses, Juvenile and Adult Records, *supra* note 128, p. 51.

[132]Use and Management of CHRI, *supra* note 22, p. 47.

stored for future identification.[133]

DNA testing

Although fingerprinting is the traditional and most widespread method of biometric identification, with a long pedigree and years of public acceptance in the criminal justice system, Deoxyribonucleic Acid (DNA) testing is a newer and, in many ways, more versatile, biometric identification innovation. DNA is unique among biometric identifiers: unlike fingerprints and other biometric identifiers, DNA can reveal more about an individual than simply his or her identity. This fact therefore raises unique privacy concerns. DNA has been called "the single greatest advance in the search for truth since advent of cross-examination."[134] That comment was made in 1988, shortly after the first time DNA testing was used, in a 1987 British case involving the rape and murder of two young girls.[135]

Since then, DNA has exploded onto the public scene, not only for its vast potential as an identification and crime-solving tool, but also as the key to advances in medicine and cloning. In the dozen years since DNA was first used to solve a crime, its stock as an identifier has risen. A 1990 SEARCH report on biometric identifiers recognized the potential of DNA testing as "enormous."[136] Policymakers have agreed, with State after State (led by the General Assembly of Virginia in 1988) establishing DNA testing laboratories and databases.

As with fingerprinting, DNA testing is not an effective means of identification unless there is an identified sample to compare with the unidentified DNA. Standards for collecting and maintaining these samples raise civil liberties and privacy concerns. The potential uses of DNA beyond identification raise additional concerns because, unlike fingerprints, DNA can be used to identify familial relationships as well as potential genetic defects or a genetic disposition for disease.[137] The information privacy concept of minimizing the information collected and retained about an individual to that which is necessary to the task can be put at risk unless DNA testing systems are carefully designed to capture only the information necessary for identification purposes (or other purpose for which the sample was originally collected). Privacy issues also arise from the retention of the underlying biological sample (rather than the digitized results of DNA identification analysis), because the biological sample could be analyzed subsequently for disease traits or other purposes beyond the original identification purpose for which the sample was collected.[138]

Civil libertarians are particularly concerned about the privacy risks posed by DNA databases. Barry Steinhardt of the ACLU, when asked to comment on efforts to perfect a chip that could be used to quickly produce a unique genetic profile from DNA discovered at a crime scene, expressed the concern this way: "Anything that makes it easier and cheaper to create a DNA databank is dangerous because it will increase the impetus to DNA test… . We don't oppose specific technologies, but what we are concerned about is the creation of the databanks."[139]

---

[133]SEARCH Group, Inc., "Biometric Technologies are Promising for Criminal Justice," *Interface* (Spring 1991) p. 33.

[134]Biometric Identification Technologies, *supra* note 120, p. 27 (quoting a 1988 comment by New York State Judge Joseph Harris).

[135]Ibid.

[136]Ibid., p. 26.

[137]Despite the identification benefits, there is some public apprehension about being voluntarily tested. In Florida, for example, a free DNA-identification pilot program for school children was not well received, despite the fact that parents, not the State, would receive and control the sample. Jeffrey McMurray, "Florida Police Find Mystery in Parents' Snub of DNA Testing," *Washington Post* (March 14, 1999) p. A22.

[138]Destruction of the underlying samples has been "met with harsh criticism from law enforcement representatives," arguing that by destroying the samples law enforcement would, as one official put it, "be destined to start over every time there's a technological change." Declan McCullagh, "What to do with DNA Data?" *Wired News* (November 18, 1999) available at **http://www.wired.com/news/politics/0,1283,32617,00.html**.

[139]Robin Lloyd, "Lab on a Chip May Turn Police Into DNA Detectives," *Washington Post* (March 1, 1999) p. A9.

States are building DNA databases, typically by requiring felons, particularly those convicted of violent crimes, to submit DNA samples to the State database. In December 1998, then-New York City Police Commissioner Howard Safir recommended that DNA samples be taken of all arrestees, declaring "The innocents have nothing to fear… . Only if you are guilty should you worry about DNA testing."[140] Safir's proposal has been adamantly opposed by the New York Civil Liberties Union, which argues that mere arrest is insufficient grounds for collection of a DNA sample.[141] This debate is also taking place on the national level, as the Federal government considers whether to develop such a comprehensive DNA database. The National Commission on the Future of DNA Evidence, which was appointed by the Attorney General to study issues related to the evidentiary use of DNA, has concluded that the practice is currently impractical due to a lack of staffing and other resources in crime laboratories nationwide and a backlog of samples currently awaiting analysis.[142]

[140]"DNA Samples in All Arrests?" *Washington Post* (December 15, 1998) p. A16. The International Association of Chiefs of Police has also called for the collection of DNA samples from all arrestees. J.D. Abolins, "International Police Group Wants DNA Sample From ALL Suspects," 2 *ISPI Privacy Reporter* (Summer 1999).

[141]Ibid., *Post* article, p. A16.

[142]National Institute of Justice, "Recommendation of the National Commission on the Future of DNA Evidence to the Attorney General Regarding Arrestee DNA Sample Collection," available at **http://www.ojp.usdoj.gov/nij/dna/arrestrc.html**. Some States are moving forward with additional testing. New York State, for example, passed a law in 1999 increasing the number of offenses with a DNA sample requirement upon conviction from 21 to 107, a change the Governor estimated would increase the number of samples collected in New York each year from 3,000 to 30,000. Gary Tuchman, "New York to expand DNA testing of convicts," CNN (October 20, 1999) available at **http://www.cnn.com/US/9910/20/dna.database/index.html**.

— Communication technologies, including the Internet

The communications revolution

The third area in which advances are generating both benefits to criminal justice and risks to privacy is communications technology. The past decade has witnessed an explosion of new technologies that allow people (and systems) to communicate faster, easier, and from more locations than ever before.[143] These changes are affecting the way criminal justice information is communicated between various criminal record repositories, between the courts and the repositories, between repositories and law enforcement, and with other criminal justice agencies. Then-Senate Minority Leader Thomas Daschle (D-SD) summarized the importance of improved communications this way: "Revolutionary technological improvements in communications systems allow localities separated by great distances to share information instantaneously. This communication between law enforcement agencies can make the difference between locating suspects and getting them off the streets, or leaving them free to commit more crimes."[144]

Information distribution is no longer tied to a fixed distribution point, such as where a telephone wire has been run. Laptop computers outfitted with wireless communications packages now permit law enforcement officers to access a wide array of Federal, State, and local databases from remote locations, without the assistance of dispatchers.[145]

Electronic mail, or "email," is another part of the communications revolution. Data can now be transmitted around the world almost instantly. Users can send one another not only directly

[143]These developments can be attributed, at least in part, to the explosion in competition between telecommunications companies as a result of deregulation. Another factor in this arena is the growing competition between telecommunications companies, cable system operators, and Internet Service Providers as applications of these technologies become increasingly interrelated.

[144]144 *Cong. Rec.* S3,943 (April 30, 1998) (statement of Senator Tom Daschle, D-SD).

[145]Kelly J. Harris, *Law Enforcement Mobile Computing: Armed with Information*, Technical Bulletin series (Sacramento: SEARCH Group, Inc., 1997, No. 1) p. 1.

keyed-in messages, but also attach files, thereby allowing potentially privacy-sensitive information to be externally distributed in a matter of keystrokes. Communications advances also make it increasingly possible for systems to share larger volumes of data electronically and to do so at faster rates. In addition, while data was once primarily processed in text format, it is increasingly possible to easily transmit, process, store, and integrate audio, video, and digital data, creating a richer and more complete data environment.

Increased speed and high-quality fiber-optic networks allow such tasks as automated arrest and disposition reporting to take place more quickly and easily than before. It also permits larger quantities of data to be transferred from one computer system to another because data entry (by keystroke or scanning) now only needs to be done once, thereby relieving "downstream" recipients of the need to determine whether some of the data received is of enough value to make the data entries.

The widespread maintenance and dissemination of information in electronic form has raised a host of concerns about how to best protect the confidentiality, accuracy, and integrity of information in electronic form. This is typically accomplished through a combination of physical, administrative, and technical measures designed to control access to data and to control the ability of authorized users to access and disseminate information. When information is transferred between systems over the Internet or other nonsecure means, there is added potential that the transmission would be intercepted. Encryption is one means to protect the confidentiality of information at risk of being intercepted by an unauthorized party. Encryption is the "transformation of plaintext into an apparently less readable form (called ciphertext) through a mathematical process. The ciphertext may be read by anyone who has the key that decrypts (undoes the encryption of) the ciphertext."[146]

Federal and interstate communications systems: National Crime Information Center, National Law Enforcement Telecommunications System, and other resources

The National Crime Information Center (NCIC) is an automated database of criminal justice and justice-related information maintained by the FBI, including "hot files" of missing or wanted persons, stolen vehicles, and identifiable stolen property. Communications components of the NCIC permit access to NCIC files through central control terminal operators in each State that are connected to the NCIC via dedicated telephone lines maintained by the FBI. Local law enforcement agencies and officers can access NCIC through the State law enforcement network. In July 1999, the FBI inaugurated the next generation of the NCIC — a project known as "NCIC 2000." NCIC 2000 upgrades the NCIC's telecommunications system and its hardware to permit the paperless exchange of information. In addition, NCIC 2000 is able to handle graphic information in paperless imaging format, including material such as mug shots, tattoos, and the signatures of offenders.[147]

The National Law Enforcement Telecommunications System (NLETS) is a high-speed message system maintained by the States through a not-for-profit corporation. NLETS permits the interstate exchange of criminal justice information between local, State, and Federal criminal justice agencies. NLETS supports inquiries into a variety of State files, including criminal history files, motor vehicle registration files, driver's license files, and other databases maintained by the States. NLETS also interfaces with the NCIC, the Royal Canadian Mounted Police, the National Insurance Theft Bureau, the National Center for Missing and Exploited Children, and other national-level files.[148]

Among the funding priorities designated in CITA are multiagency, multijurisdictional communications systems among

[146]RSA Laboratories, "Frequently Asked Questions About Today's Cryptography: Glossary," available at **http://www.rsasecurity.com/rsalabs/faq/B.html**.

[147]Federal Bureau of Investigation, Press Release, July 15, 1999.

[148]Use and Management of CHRI, *supra* note 22, p. xi.

the States to share routine and emergency information among Federal, State, and local law enforcement agencies. "A 1997 incident along the Vermont and New Hampshire border underscored the need for multijurisdictional systems. During a cross-border shooting spree that left four people dead, including two New Hampshire State Troopers, Vermont and New Hampshire officers were forced to park two police cruisers next to one another to coordinate activities between Federal, State, and local law enforcement officers because the two States' police radios could not communicate with one another."[149] As a result of this incident, officials from Vermont, New York, New Hampshire, and Maine have developed the "Northern Lights" proposal, which would allow these northern-border States to "integrate their law enforcement communications systems to better coordinate interdiction efforts and share intelligence data."[150]

The Internet

Perhaps the most important technological development underpinning the need for a reassessment of the privacy landscape — the Internet — is actually a by-product of the other advances in communications and information technology already discussed. The number of American Internet users in 1998 was approximately 47 million.[151] It is estimated that, as of September 2000, nearly 148 million Americans had access to the Internet, over 89 million of whom were active users.[152] This explosive growth has caught everyone's attention. The public is "surfing" the Internet in large and increasing numbers, business is enthralled by the promise of electronic commerce, and Congress and the State legislatures are paying close attention to developments to determine what legislation is necessary to regulate everything from Internet privacy to Internet decency to Internet taxation.

The Internet is a growing means for law enforcement to interact with the public and a valuable research tool. The FBI and other law enforcement organizations, such as the Los Angeles Police Department, post their "most wanted" lists on the Internet.[153] Other law enforcement agencies allow citizens to use the Internet to make anonymous tips, report nonemergency crimes, and file initial police reports in certain matters, including burglary, theft, and vandalism.[154]

As of May 1999, 15 States have posted sex offender and sexual predator registration information from State sex offender registries on the Internet in a format accessible to and searchable by the public.[155] These sites commonly include the offender's name, address, vital statistics, offense (sometimes including case number), and sometimes a photograph as well.[156] These sites allow individuals to search by name or geographic area (typically city, county, or ZIP code).[157] States are not the only ones to sponsor sex offender sites on the Internet. Local police also maintain sex-offender sites either on their own or in concert with local newspapers.[158]

---

[149]144 *Cong. Rec.* S12,042 (Oct. 8, 1998) (statement of Senator Patrick Leahy, D-VT).

[150]Ibid.

[151]About.com, Internet Industry, "How many people use the Internet?" (August 1, 1999), available at **http://internet.about.com/industry/internet/library/archivebl/stats/blstats2a.htm**.

[152]Nielsen//Netratings, "Average Web Usage, September 2000," available at <www.nielsen-netratings.com.

[153]See, for example, **http://www.fbi.gov/mostwant/fugitive/fpphome.htm**; and **http://www.lapdonline.org/**.

[154]See, for example, **http://www.cji.net/sierraso/index.html** (Office of the Sheriff of Sierra County, California); and **http://www.placer.ca.gov/sheriff/** (Sheriff's Department of Placer County, California).

[155]See, *supra* note 103.

[156]See, for example, **http://www.dps.state.ak.us/nSorcr/asp/** (Alaska); **http://www.fdle.state.fl.us/Sexual_Predators/index.asp** (Florida); **http://www.state.in.us/serv/cji_sor** (Indiana); **http://www.ink.org/public/kbi/kbiregoffpage.html** (Kansas); **http://sex-offender.vsp.state.va.us/cool-ICE/** (Virginia); and **http://www.statetroopers.com/sexoff/sexoff.shtml** (West Virginia).

[157]Ibid.

[158]See, for example, **http://www.ccspd.org/search_output .html** (Cook County, Illinois); and

In addition to interacting with the public, law enforcement is also using the Internet to interact with fellow law enforcement officers and to do law enforcement work. Internet sites such as **www.officer.com** and **www.leolinks.com** provide law enforcement officers with access to a wide array of information on everything from hate groups and terrorism, to computer crime, traffic enforcement, statutes, other law enforcement organizations, police unions, and educational and training opportunities.

Trend toward integrated systems

Traditionally, each of the four components of the criminal justice system — law enforcement, prosecutors, courts, and corrections — maintained a discrete information system designed to meet that component's particular information needs. There was little, if any, linkage between these systems, and certainly no system architecture that provided one system for all components. In recent years, however, the criminal justice system has worked toward integrating these systems, using a multipurpose architecture.

— Definition of integration

The BJA/SEARCH National Task Force on Court Automation and Integration defines integration of justice information systems to mean, "the electronic sharing of information by two or more distinct justice entities within a system. The degree to which information systems are considered 'integrated' depends upon who participates, what information is shared or exchanged, and how data are shared or exchanged within the system."[159]

It is also important to understand what integration is not. Integration is not the mere linkage or connection of distributed or dispersed databases. Nor is integration the amalgamation of private data in a particular information system.

Participants

Participation in integrated systems can occur in three principal configurations: vertical integration of criminal justice users, horizontal integration of criminal justice users, and the integration of criminal and noncriminal justice databases.

Vertical integration refers to the linkage of systems operated by the same type of criminal justice organization at various levels of government; city police systems are linked with county police systems that are linked with State police systems, which are linked with Federal systems, and so forth. *Horizontal integration* refers to the linkage of different components of the criminal justice system on a particular level — the State police system, the State court system, the State prosecutors' system, and so forth. Indeed, local and municipal agencies have been leaders in pioneering horizontal integration.

Information exchanged

The information exchanged by integrated systems varies. "Some systems may include only adult criminal justice data, whereas others may include juvenile, family, domestic relations, and social service data. Some systems may address all operating requirements, such as … revenue management systems, whereas others may limit the database to case management information requirements. However, 'information' is increasingly more than just raw data elements: it may include images, audio, video, substance abuse test results, DNA profiles, and fingerprint minutiae."[160]

Method of information exchange

The underlying technology of an integrated system may also vary. Information may be exchanged through a common database that is shared by participating agencies. Information may also be shared by a coordinated system, with data maintained in separate databases and exchanged via standardized messages. In addition, hybrid systems exist, which allow

http://oakparkjournal.com/sexoffend-op.htm (Oak Park, Illinois).

[159]Task Force on Court Automation, *supra* note 111, p. 2. Although some members of the Privacy Task Force believed that this definition was too narrow, the Task Force used this definition as the basis of its discussions.

[160]Ibid., p. 3.

agencies to maintain separate databases while using a central database that controls the level of access afforded to different users in the system.[161]

— Benefits and privacy risks of integration

Integration has numerous benefits. Integration may reduce labor costs and operating expenses by eliminating the need for agencies to undertake duplicative data entry and collection, eliminating the need to maintain duplicate records, and increasing efficiency. Furthermore, the data in an integrated system may be more accurate because it was only entered once. The information may also be available on a more timely basis because information collected early in the process is available for later processes even before those later processes begin. This information availability can improve the performance of the courts and criminal justice agencies, and thereby improve public safety. Finally, and perhaps most importantly, data may be more complete because the responsibility for collecting and reporting each data element is firmly fixed with a particular agency.[162]

Integration, however, also poses privacy risks. First, there is the potential that integrated systems may propagate inaccuracy if the data are entered incorrectly in the first instance. Second, an integrated system may make sensitive data about an individual, which is important to one part of the criminal justice system, readily available to other parts of the system, where that information is not necessary or useful to the needs of that institutional player. The corrections system, for example, gathers large amounts of detailed information concerning the lives of inmates over the course of their incarceration. An inmate's correction record might include breaches of discipline and resulting disciplinary action; information about sexual activity; sensitive medical information, such as HIV status; drug use and rehabilitation information; mental health information; and educational or employment information. Although this may be important information for the corrections facility where the inmate is held, it is not necessarily relevant to law enforcement officials or others with access to the integrated system.

A third privacy risk arising from integration is that there will be more information and increasing demands for its use. As systems are integrated, the data in those systems become richer and, therefore, more valuable to a wider pool of potential users. Although a system may have been integrated to increase its utility to law enforcement, corrections, prosecutors, and the courts, "function creep" becomes a real possibility and privacy concern. How widely should the information in these integrated systems should be made available is a key question. Access by law enforcement, courts, prosecutors, and corrections are common suggestions. Should the list be expanded to include the defense bar or the public defender's office? What about access for those outside the system, such as child support enforcement and welfare agencies?

A fourth privacy risk arises when information subject to strict rules in one sector is captured by an integrated system operating in a more accommodating privacy environment. Data coming from the privacy-sensitive central repository environment, for example, may be captured in an integrated system subject to the relatively privacy-lenient environment in the courts. This raises a question as to which privacy rules apply to information in an integrated system. Do the standards for the integrated system reflect the policies of the most privacy-protective participating agency, the least privacy-protective, or is a new privacy standard developed for the integrated system? Or, in the alternative, do privacy rules vary depending upon the source of the information or the purposes for which the information is accessed?

---

[161] Ibid.

[162] Ibid., p. 29. For a more extensive discussion of the benefits of integration, see, ibid., pp. 29-34. See also, Robert L. Marx, *System Integration: Issues Surrounding Integration of County-Level Justice Information Systems*, NCJ 156841 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Assistance, November 1996) p. 29.

A new approach that closely resembles a "Business Model" for the criminal justice system

In recent years, there has been a shift in the way courts and criminal justice agencies view their mission. Increasingly, agencies focus on their interaction with the public and seek to accomplish their missions through active crime prevention efforts in addition to the more traditional approach of reacting to crimes once they occur. In addition to the well-known "community policing" model, there "are literally hundreds of examples of this trend, from offender-victim reconciliation projects in Vermont and Minneapolis to 'beat probation' in Madison, Wisconsin; from neighborhood-based prosecution centers in Portland, Oregon, and New York City, to community probation in Massachusetts."[163] These programs come in a variety of forms; the term "community courts," for example, encompasses a wide range of specialized courts, including: teen courts, drug courts, misdemeanor courts, and family courts.[164]

These programs rely, in part, on the ability to exchange information with the community about crimes, suspects, and criminals in a quick, accurate, and efficient manner. The importance of information to the new criminal justice model has been described this way:

> The new age of community justice is made possible by the power of information. Using geo-coded data, crime control services are organized around locations of crime events, offenders, and victims. Data, both official data about crimes and offenders and qualitative data that come from interaction with offenders, victims, and neighborhood residents, drive problem-solving and action. Information will also provide evaluative feedback about the successes of strategies. The imaginative use (and production of information) is one of the factors that sets aggressive community safety strategies apart from the more mundane concept of the local constable.[165]

A number of community organizations throughout the Nation use the information-sharing aspects of community policing to fight crime in their communities. Turn Around America, for example, mobilizes neighborhoods in an effort to stop drug trafficking. The group, which is led by neighbors in conjunction with law enforcement and others, is designed to address the economics of the drug trade — separating the buyer from the seller.[166] This "separation" of buyer and seller is accomplished by marches through, and vigils at, locations believed to be venues where drug dealing occurs. These activities are designed to spotlight venues where drug trafficking occurs and discourage buyers who fear public exposure. Turn Around America views positive relations and information-sharing with law enforcement as an important element of their ability to succeed.[167] Much of the building of positive relations between such community groups and the police can be achieved without the disclosure of personal information. Although Turn Around America claims to have drastically lowered crime in areas it

[163]Todd R. Cleary and David R. Karp, "The Community Justice Movement," in *Community Justice: An Emerging Field*, David R. Karp, ed. (New York: Rowman & Littlefield, 1998) p. 3. Hereafter, Community Justice.

[164]Ibid., p. 9.

[165]Ibid., p. 18.

[166]See, **http://www.drugfighters.com**.

[167]As noted in an article about the Turn Around effort in Waxahachie, Texas, "The relationship between the community and police depends on trust, shared information, cooperation, support, mutual respect and social interaction. If you try this approach in your community, make every effort to keep law enforcement officials aware of your group's concerns, goals and activities. Ask that a representative from the police attend each of your planning sessions. Make certain they understand that your intentions are to enhance and not replace the role of law enforcement within the community. Look at contact with local police as an education that will ultimately benefit everyone." Nathan Bickerstaff, "Community Anti-Drug Group Development Shows Community and Police Teamwork," available at **http://www.communitypolicing.org/artbytop/w4/w4bicker.htm**.

has targeted,[168] civil liberties organizations, such as the ACLU, have criticized the group's practices as harassment and an invasion of privacy of individuals who have not been charged with a crime.[169] Concern has also been raised over the propriety of law enforcement organizations sharing information about suspected drug traffickers with these groups.[170]

In addition to more community interaction, courts and criminal justice agencies are interacting with one another and noncriminal justice agencies in new ways to process offenders, rehabilitate offenders, and prevent future crimes. Criminal justice agencies and the courts frequently recognize new obligations that make them responsible to, and/or dependent upon, other agencies. The Midtown Community Court in Manhattan, which specializes in misdemeanor cases, is one example. "Contained in one building, the Midtown Community Court makes concrete use of a social services center, a community service program, community mediation services, and a sophisticated information network that tracks and relays cases as they travel between departments."[171]

This kind of interactivity and accountability often means that CHRI is being widely shared by criminal justice agencies, not only with other law enforcement agencies, but also with social welfare agencies, educational institutions, and the public. These new relationships and initiatives are increasing the amount and expanding the scope of recipients of criminal history information.

In Texas, for example, law enforcement agencies, prosecutors, and probation officers are required to notify the school district where a student is believed to be enrolled of the student's arrest for designated offenses. In addition, the school district must be apprised of whether the matter is prosecuted or adjudicated, as well as the final disposition of the matter.[172] This information may serve as the basis for the transfer of that student from the general student population into an "alternative education program" that provides instruction in core subjects as well as self-discipline, supervision, and counseling.[173]

Other examples of these changes, including the publication of sex offender information, reporting of child protection orders, and expanded disclosure of CHRI for background checks in the employment and firearms purchasing contexts, are discussed at length elsewhere in this report. One Task Force member characterized these new information flows as a "data-driven, problem solving approach" to crime and other social problems. These mechanisms are designed with prevention in mind: prevention of sex offenses, of child abuse and endangerment, of poor hiring decisions that could endanger people and create liability for employers, and of firearms purchases by those whom society deems a risk.

Another distinct development is the privatization or outsourcing of criminal justice information functions. Privatization introduces a new player into the information equation — often a private, for-profit company or service bureau. Private contractors, however, can be contractually bound to observe the same standards that are applicable to government agencies.

In September 1999, the U.S. DOJ published a final rule amending its regulations to permit the criminal justice

[168]Turn Around America cites the following statistics: "The … process has proven effective all over the country with all types of communities in ridding neighborhoods of drug trafficking and drastically lowering crime and violence, for example: Taylor, Texas, 80% crime reduction in targeted area; Waxahachie, Texas, 93% clearance for major crime cases; East Palo Alto, California, 86% drop in crime; and Red Oak, Georgia, 98% drop in 911 calls." See, **http://www.drugfighters.com**.

[169]See, Victoria Loe, "ACLU Scrutinizing Effort by Authorities to Shame Drug Dealers" *Dallas Morning News* (July 2, 1996) p. 1A; John Moritz, "Morales Backs Disclosure of Drug House Locations; Anti-Drug Activists Want Addresses to Put Pressure on Dealers, Customers," *Ft. Worth Star-Telegram* (December 24, 1996) p. 2.

[170]Ibid.

[171]Community Justice, *supra* note 163, p. 9.

[172]TEX. CRIM. PROC. CODE § 15.27. This article imposes certain confidentiality requirements on the school district personnel receiving the information.

[173]TEX. EDUC. CODE § 37.008.

agencies, subject to certain controls, to grant private entities access to CHRI for the purpose of providing services for the administration of criminal justice.[174] Criminal justice agencies will be required to include a security addendum approved by the Director of the FBI to their agreements with the private-sector contractor to "authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require."[175] The regulations also authorize criminal justice agencies to outsource certain dispatching, data processing, and information service functions to other government agencies pursuant to executive order, statute, regulation, or interagency agreement.[176]

The new prevention model poses potential privacy risks. Sex offender registries, for example, have been criticized by civil libertarians on numerous grounds, including the potential harm to registrants from the public disclosure of their status as registrants. One potential risk is that registrants may be the targets of vigilantism and physically harmed.[177] Another risk is that offenders will lose their jobs. In September 1999, Oregon voluntarily placed its plans to provide public access to sex offender registry information over the Internet on hold pending an ACLU-assisted lawsuit, in which 10 sex offenders each claimed that "[i]f his name, photograph, and identity is broadcast over the Internet as a sex offender, he will readily and immediately lose his employment." [178] Accuracy of registry information is also a concern.[179] In one instance, a Kansas family was subjected to scorn, and rocks thrown at their mobile home, after local officials posted notices that a sex offender lived at their address. In reality, the sex offender had lived at the address previously and moved without notifying authorities.[180]

More public access, demand for criminal justice records

Beginning in the late 1970s, policymakers grew increasingly interested in capturing, maintaining, and sharing criminal justice and criminal history record information and grew less interested in providing privacy safeguards for arrestees and offenders. During this same period, as noted earlier, the Supreme Court found that information about arrests and convictions relates to public events and is, therefore, not subject to constitutional privacy protections.[181] The result, throughout the 1980s and 1990s, was a steady expansion of statutory and regulatory provisions permitting the use and disclosure of CHRI.

Today, criminal justice and criminal history record information is available from State central repositories not only for criminal justice purposes, but

[174]64 *Federal Register* 52223 (September 28, 1999).

[175]Ibid., at 52223 – 52224.

[176]Ibid., at 52224.

[177]Examples of vigilantism against sex offender registrants reported by the ACLU include the firebombing of a registrant's car in California, the beating of a man believed to be a paroled sex offender in New Jersey, and the destruction of the homes of registrants in New Jersey and Washington by arson. ACLU, "Names Removed From Missouri Sex Offender List," Press Release (August 27, 1997), available at **http://aclu.org/news/n082897a.html**.

[178]Robert Ellis Smith, "In the Courts: Sex Offenders," *Privacy Journal* Vol. 25, No. 11 (September 1999) p. 7.

[179]Accuracy concerns, of course, are not limited to sex offender registries. Inaccurate criminal justice information can have serious repercussions for the individual, including loss of employment. A Maryland woman, for example, reportedly lost her job as a child-care director at a Maryland YMCA, when, during a background check, her name and Social Security number erroneously appeared during a search of a Baltimore County computer in connection with four child protective services cases. Although Baltimore County family services later acknowledged and corrected the error, the woman was not reinstated by the YMCA. Evan Hendricks, "Maryland Woman Victimized by Inaccurate Criminal Data," *Privacy Times*, Vol. 17, No. 23 (December 15, 1997) pp. 9-10.

[180]Robert Ellis Smith, "Inevitable," *Privacy Journal*, Vol. 23, No. 7 (May 1997) p. 4.

[181]See, for example, *Paul* v. *Davis*, 424 U.S. 693, 713 (1976).

also for a wide variety of non-criminal justice purposes authorized by law or regulation. In particular, these purposes include employment background screening, licensing eligibility checks, and a wide array of noncriminal justice, governmental purposes.

Demand continues to grow. This is particularly true of employers and volunteer organizations, such as the Boy Scouts, which increasingly seek access to CHRI for pre-employment background checks. There are two driving forces behind this increased demand for access: (1) a desire to make informed hiring decisions that assess the potential risk prospective employees may pose to the hiring organization, its employees, or its clients; and (2) a desire to minimize potential legal exposure that could result from hiring individuals without conducting a criminal history check.

The potential for both harm to individuals and resulting employer liability is illustrated by recent negligent hiring cases.[182] In one instance, a home health care company in Boston hired a home health care aide without conducting a background check, which would have revealed the aide had six larceny-related convictions, and that he did not have the education or work experience stated on his employment application.[183] Several months later, the employee murdered a 32-year-old quadriplegic man in his care and the man's 77-year-old grandmother, allegedly in order to cover up ongoing theft from the man. The man's parents sued, alleging that the company was negligent in allowing a convicted felon to care for their son. A jury found for the parents and awarded $26.5 million in punitive and compensatory damages.[184]

Negligent hiring cases are not limited to positions that are typically viewed as being sensitive either because of the trust the position requires or the vulnerable nature of the population served. A jury held a Florida furniture store that did not conduct a background check liable for $2.5 million in damages for a person who was assaulted by a store employee with a prior criminal record.[185] In another set of cases, a pizza delivery chain reportedly paid a total of $375,000 to settle two lawsuits by parents of young boys who were allegedly molested by a pizza delivery man who, unknown to the pizza company, had a prior record for burglary and grand theft.[186] In addition to the employer liability question, these cases also raise policy questions about the reintegration of convicted persons into society after their sentence is complete, and if background checks are expected not only of persons in sensitive positions, but also of those in positions traditionally viewed as being less sensitive, such as pizza delivery persons.[187]

It is a rare legislative cycle, however, that does not see the enactment of new State laws authorizing access to criminal history information for non-criminal justice purposes, either for specified noncriminal justice users or the public at large. Unlike some negligent hiring cases, however, most legislative authorizations focus on positions that involve a particular

[182]Under the tort of negligent hiring, an employer can be held liable for wrongful acts of an employee if the wrongful act was a cause-in-fact of the plaintiff's injury, provided that the failure of the employer to exercise due care in the hiring, training, or supervision of the employee was a cause-in-fact of the act of the employee who caused the injury. See, for example, *Miller* v. *Wal-Mart Stores, Inc*., 580 N.W.2d 233 (1998).

[183]See, *Ward* v. *Trusted Health*, No. 94-4297 (Suffolk Super. Ct., Mass. February 1999). See also, Mayer & Riser, PLLC, "Worker Murders Man and His Grandmother: Employer Liable for Negligent Hiring," available at **http://www.mayer-riser.com/Articles/ap/liability/neghiring0599.htm**.

[184]Ibid.

[185]See, *Tallahassee Furniture Co.* v. *Harrison*, 583 So.2d 744 (4 Fla. App. 1991), *rev. denied* 595 So.2d 558 (Fla. 1992). In addition to failing to conduct a background check on the man, who worked for the company's owner as a part-time laborer for several months prior to being hired as a full-time deliveryman, the furniture store also failed to conduct a job interview, request references, or request that the man complete an application form. Ibid.

[186]See, Employment Data Services, "Negligent Hiring the New 'Entitlement,'" available at **http://users.javanet.com/~empdata/negligent.html**.

[187]In addition to concerns about reintegrating the former offender into society, there is also the related risk that the former offender will be unable to obtain gainful employment and will be consigned to a permanent underclass.

trust or regular interaction with vulnerable populations, such as the sick, the elderly, and children.[188] In the 105th Congress, for example, the Senate held hearings on the need for access to criminal history data for nursing home workers; the Congress enacted legislation strengthening the *National Child Protection Act*, which authorizes background checks for employees providing services to children, the elderly, and the handicapped; and the Congress amended the *Fair Credit Reporting Act* to permit consumer reports to include conviction information, regardless of how long ago the conviction occurred.

The FBI has reported that the number of criminal history record access requests it receives from noncriminal justice requesters now exceeds the number of requests from criminal justice. Noncriminal justice requests include not only private employers, but also other government agencies not associated with the criminal justice system. An Office of Technology Assessment (OTA) survey in 1979 of criminal history record system managers in 35 States found 20.6 percent of the total number of access requests received by these repositories were by noncriminal justice agencies.[189] As long ago as 1981, a BJS/SEARCH report, *Privacy and the Private Employer*, recognized that increased access to criminal history information, particularly for employment purposes, was a nascent trend. At that time, however, there was little data regarding the number of criminal history information requests made to criminal justice agencies by private employers.[190] The report recognized that one means by which employers could obtain criminal history information about applicants — in addition to asking the applicant directly or using a third party such as a consumer-reporting agency — was "to request the data directly from criminal justice agencies, usually local police departments."[191] The role of local police departments was highlighted in the report, which noted that many State statutes regulating the disclosure of criminal history information regulated only disclosures by the State repositories, not local law enforcement.[192]

A 1998 survey determined that approximately 35% of the fingerprint cards submitted by the States to the FBI and processed during fiscal year 1997 were for noncriminal justice purposes.[193] The survey found that in eight States — Delaware, Florida, Idaho, Massachusetts, Nevada, New Jersey, Oregon, and Washington — and the District of Columbia, the number of requests for noncriminal justice purposes exceed the number of requests made for criminal justice purposes.[194] A similar 1993 study found that only approximately 9% of the fingerprint cards the FBI received from the States that year were for noncriminal justice purposes, with no States submitting more noncriminal justice requests than criminal justice requests.[195]

There are several State law patterns and similarities in the treatment of criminal history record dissemination for noncriminal justice purposes. Most States treat conviction information and open-arrest information less than 1 year old (arrests with no record of disposition) differently from nonconviction information. Typically, States place few or no restrictions on the dissemination of conviction records, and a number of States do not place restrictions on open-arrest information less

[188]Other policy considerations are the basis for permitting access to noncriminal justice users. Manufacturers, distributors, and dispensers of controlled substances are prohibited from hiring individuals convicted of felonies related to controlled substances, and are expected to screen employees in other circumstances. See, 21 C.F.R. §§ 1301.76, 1301.90, 1301.93.

[189]Gary R. Cooper and Robert R. Belair, *Privacy and the Private Employer*, Criminal Justice Information Policy series (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, 1981) p. 14 (citing *An Assessment of the Social Impacts of NCIC and CCH*, prepared by the Bureau of Governmental Research and Service, University of South Carolina, for the U.S. Congress' Office of Technology Assessment (1979) p. 227). Hereafter, Privacy and the Private Employer.

[190]Privacy and the Private Employer, p. 14.

[191]Ibid.

[192]Ibid., pp. 34-35.

[193]Compendium, *supra* note 60, p. 8.

[194]Ibid.

[195]Ibid, pp. 8-9.

than 1 year old. Nonconviction records are restricted to a greater degree, with dissemination frequently limited to specified types of noncriminal justice users for specified purposes.[196] The different approaches reflect the fact that the widespread dissemination of nonconviction information makes it more difficult for an innocent arrestee to be reintegrated into society.[197] Finally, the widespread reporting and dissemination of nonconviction data may exacerbate the potentially disproportionate adverse impact of the criminal justice system on minority populations.[198]

Some States authorize the use of conviction information for any occupational licensing or employment purpose, while other States limit authorization for background checks using conviction and, particularly, nonconviction information to applicants for specific high-risk occupations, such as child care, sensitive government positions, elder care, care of the disabled, health care, banking, firefighters, and police.[199] Similarly, the "Bible Rider" authorized the FBI to exchange conviction information with officials of federally chartered or insured banking institutions and certain segments of the securities industry and with nuclear power plants.[200]

Another area where the States are authorizing access to CHRI, or even actively disclosing the information, relates to sex offenders. As noted earlier, 15 States now post sex offender registration information on the Internet. Other States, such as New York and California, offer a "900 number" for citizens to call to find out if an individual is a registered sex offender.[201]

This trend, spurred primarily by public reaction to high-profile abductions, rapes, and murders of young children, is discussed in more detail in the subsequent discussion of Federal legislation in this chapter.

The growing number of users authorized to access CHRI for various purposes is one that the Task Force expects will continue to grow.

Changes in the marketplace: Growing commercialization of records as private companies sell criminal justice records compiled from public record information

— The changing marketplace

In the last few years a new marketplace has emerged to meet the burgeoning noncriminal justice demand for criminal history data and to take advantage of changes in information technology. Today, private companies routinely "harvest" public record information, including arrest and conviction information, from newly automated court dockets and, to a lesser extent, police blotter systems.[202] These

[196]State statutes vary in their level of detail. Many States rely upon executive orders, regulations, and written and unwritten repository policies to supplement and elaborate on their statutes. Ibid., p. 8.

[197]A Maryland woman, for example, is reported to have lost her job running a daycare center at a military housing complex because a background check revealed that the woman was arrested for burglary and assault. According to reports, the woman had been erroneously arrested in 1985. Her superiors subsequently acknowledged that there was a discrepancy, but did not offer to rehire her. See, *supra* note 179.

[198]See, *supra* note 47. See also, Michael A. Fletcher, "Criminal Justice Disparities Cited," *Washington Post* (May 4, 2000) p. A2; Leadership Conference on Civil Rights and Leadership Conference Education Fund, *Justice on Trial: Racial Disparities in the Criminal Justice System* (Washington, D.C.: May 4, 2000), available at **http://www.civilrights.org/policy_and_legislation/pl_issues/criminal_justice/.**

[199]Compendium, *supra* note 60, p. 9.

[200]This measure is popularly referred to as the "Bible Rider" because it was originally sponsored by then-Senator Alan Bible (D-NV), who attached the authorization for such exchanges of information as a rider to an appropriations bill. Regulations have since been published at 28 C.F.R. § 50.12.

[201]Robert Teir and Kevin Coy, "Approaches to Sexual Predators: Community Notification and Civil Commitment," 23 *New England Journal on Criminal and Civil Confinement* (Summer 1997) pp. 405, 409, n. 18.

[202]Court records contain far more information than simply indexes of charges leveled against a criminal defendant and the disposition of those charges. Criminal court records may also include transcripts of preliminary hearings and court proceedings, voir dire information, exhibits submitted into evidence, deposition information, motions and pleadings, and other in-

companies then sell the criminal history profiles to employers, insurers, and other noncriminal justice users. In addition, individual reference services "provide critical assistance to Federal, State, and local government agencies to carry out their law enforcement and other missions."[203] Further, these companies or their customers may merge criminal record information with an individual's education, employment history, credit history, and other records, as well as with putative data to create informal but, nonetheless, powerful and comprehensive reports.

Although court records have always been in the public domain, these records were maintained on a court-by-court basis, and were organized either chronologically or by docket number, or by name, sometimes with a date of birth in an index available to the public. In addition, these records were manual, paper-boxed records requiring a researcher to travel to the court to physically access and inspect the records. All of this had the practical impact of limiting the accessibility of these records to those who had reason to believe that a particular individual had appeared in a particular court at a particular time, and had the resources and motivation to conduct this kind of a search.

The automation of court records and, to a lesser extent, of police blotters and the emergence of companies that harvest and disseminate arrest and conviction records have changed the criminal justice information privacy landscape. These companies, frequently referred to as "individual reference services companies," gather not only CHRI, but also other types of personal and public record information. The companies make this information available to corporate and professional users, as well as government agencies and individuals.

This information, compiled from a variety of sources, can be used for a wide range of purposes, which may or may not be regulated by statute.[204] Information obtained from public record sources, for example, is used for preventing fraud; promoting child support enforcement; locating witnesses for civil and criminal cases, and missing children, heirs, and beneficiaries; protecting consumers from unqualified "professionals" or potential predators; locating and apprehending individuals eluding law enforcement; supporting media research; and increasing the ease with which the public can access public records.[205]

---

formation generated as a case advances through the criminal justice system. These records can easily include sensitive personal information about the defendants, victims, and witnesses in a particular case. This information can be generated not only as paper records, but also in the form of computer-aided transcription, videotaped depositions, and in some jurisdictions, televised trials. Court systems are increasingly aware of the sensitive nature of the information contained in court records. In Washington, for example, the State Judicial Information System Committee is conducting public meetings around the State to discuss the impacts and effectiveness of its data dissemination policy as part of its review of the policy. "The policy review will focus on the major issues that the requests for information have raised over the last four years and will revisit the extent to which compiled information on individuals needs protection." See, "Data Dissemination Policy Review," available at **www.courts.wa.gov /datadis/policy.cfm**.

[203]Federal Trade Commission, *Individual Reference Services: A Report to Congress* (December 1997) p. 9.

[204]Over a dozen State constitutions contain language protecting personal privacy rights, usually from government interference. See, Fred H. Cate, *Privacy in the Information Age* (Washington, D.C.: Brookings Institution Press, 1997) pp. 66-68. Some State constitutional provisions, such as Article 1, Section 1 of the California Constitution, have been interpreted to apply to both the public and private sector. The California Supreme Court has held that a plaintiff alleging an invasion of privacy in violation of the State constitutional right to privacy must establish "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy." Even if the plaintiff proves all three of these elements, the defendant has an affirmative defense if the invasion of privacy "substantially furthers one or more countervailing interests" and the plaintiff is unable to show there are "feasible and effective alternatives to [the] defendant's conduct which have a lesser impact on privacy interests." *Hill* v. *National Collegiate Athletic Association*, 865 P.2d 633, 657 (Cal. 1994). To date, however, application of these State constitutional privacy protections has not resulted in significant information privacy protections beyond those derived from the U.S. Constitution. Cate, *Privacy in the Information Age*, p. 68.

[205]Piper & Marbury, L.L.P., *White Paper: Individual Reference Services* (Washington, D.C.: Individual References Services Group, December 1997) p. 2. Hereafter, IRSG White Paper,

One member of the IRSG , the Online Professional Electronic Network (OPEN), for example, makes a relatively comprehensive criminal arrest and conviction record search product available to its business and professional subscribers that "searches millions of online arrest records submitted by county jail facilities from an ever-growing [sic] number of States. Arrest record data includes booking time, inmate ID, arresting agency and charge code with description. Also available through this search is the ability to place orders for on-site searches for conviction information in any U.S. County."[206] For this product, arrest records can be searched using name or Social Security number, while conviction information searches require name, Social Security number, date of birth, and county to be searched.[207]

Another reference services company, identifying itself on the Internet as the "Global Information Network," offers several CHRI products, including: a "county criminal court record report," from a potential pool of 3,300 counties; a "Statewide criminal repository record report," from approximately 30 State repositories (a release form from the subject may be required); and a "Federal criminal court record report" for actions in the Nation's 94 Federal District Courts.[208] Typically, county record searches are completed within two business days, Federal court searches within three business days, and State repository requests "usually take considerably longer … the turn around varies by State."[209] This vendor accepts orders via a toll-free telephone number; other companies selling background checks permit ordering online.[210]

In addition to the commercial sale of CHRI to the public, a number of commercial vendors also sell identification and location products that are used by law enforcement agencies ranging from the U.S. Marshals to local sheriff's departments for the apprehension of fugitives.[211] U.S. Marshals, for example, were able to apprehend two fugitives using a system offered by CDB Infotek, a member of the IRSG. The Marshals entered the names of two fugitives and the system returned information indicating a nearby location. DBT, another member of the IRSG, reports that its products are used by more than 1,000 law enforcement agencies and that law enforcement has used its products to apprehend criminals ranging from child kidnappers to bank robbers to jewel thieves.[212]

— The *Fair Credit Reporting Act*

The *Fair Credit Reporting Act of 1970* (FCRA), as amended, regulates the use of CHRI by consumer-reporting agencies for employment, credit, and certain other purposes.[213] Consumer-reporting agencies are organizations that, for a fee or on a cooperative, nonprofit basis, are in the practice of assembling or evaluating personally identifiable information obtained from third parties and bearing upon a consumer's credit worthiness, character, reputation, personal characteristics, or mode of living. This, of course, includes criminal history information,

available at **http://www.irsg.org/html/white_paper.htm**.

[206]"OPEN Products," available at **http://www.openonline.com/productguide.htm#criminalacrcmvoc.htm**.

[207]Ibid.

[208]See, for example, **http://www.searchinfo.com/criminal.html**.

[209]Ibid.

[210]Ibid. For an example of a firm permitting online ordering, see, **http://www.1800ussearch.com**.

[211]IRSG White Paper, *supra* note 205, p. 12.

[212]See, **http://www.dbtonline.com**. A special agent of the Bureau of Alcohol, Tobacco and Firearms characterized the value of such services as "a tremendous benefit to our law enforcement mission and a real time saver … . The spontaneous retrieval of accurate data maintained in [the database] contributed to effectively directing and positioning our surveillance teams that resulted in the surrender of two suspects. When one of the suspects was believed to be in a large apartment complex, your … system was able to provide us complete drivers license information for every driver in the complex which totaled over 700 and did so in less than 10 minutes. [It] is an incredible tool for law enforcement providing us with a capability to assimilate information from your uniquely cross referenced records." Letter from Robert J. Creighton, Special Agent in Charge, Miami Field Division, Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms, to Database Technologies, Inc. (September 14, 1995).

[213]15 U.S.C. § 1681 *et seq.*

such as arrest and conviction information.

Under the FCRA, a consumer-reporting agency may only provide a consumer report to a party when the agency has reason to believe that the party will use the report to make a credit determination, an employment determination, an insurance underwriting determination, or otherwise in connection with a legitimate business need in a transaction involving the consumer or pursuant to written instructions of the consumer.[214]

As substantially amended in 1997, the FCRA includes all of the safeguards expected in a comprehensive, fair information practice/privacy statute, including notice to consumers; consent, including opportunities for opt-in/opt-out; accuracy, relevance, and timeliness standards; confidentiality and use safeguards; security expectations; consumer access and correction rights; content restrictions; and remedies, including administrative sanctions and private rights of action. More specifically, the FCRA provides consumers with the following privacy rights:

- A consumer-reporting agency that furnishes a consumer report for employment purposes containing public record information, including criminal history records, which is "likely to have an adverse effect upon a consumer's ability to obtain employment," must either provide the consumer with notice at the same time that the information is reported to the potential employer or "must maintain strict procedures" to ensure that the information is complete and up-to-date.[215]
- A consumer must be notified when information is used to take an action against him or her, such as the denial of employment. In such cases, the party denying the benefit must provide the consumer with information on how to contact the consumer-reporting agency that provided the information.
- Consumer-reporting agencies must, upon request, provide a consumer with a copy of that consumer's file, as well as a listing of everyone who has requested it recently. The cost to the consumer of obtaining the report cannot exceed $8, and may be free if requested in connection with a recent denial of benefits or other specified circumstances.
- Consumers are permitted to request a correction of information they believe to be inaccurate. The consumer-reporting agency must investigate unless the dispute is frivolous. The consumer-reporting agency must also send a written investigation report to the individual and a copy of the revised report, if changes were made. The consumer may also request that corrected reports be sent to recent recipients. If the dispute is not resolved in the consumer's favor, the consumer has the option of including a brief statement to the consumer's file, typically for distribution with future reports.
- Consumer-reporting agencies must remove or correct unverified or inaccurate information from its files, typically within 30 days after the consumer disputes the information.
- In most cases, a consumer-reporting agency may not report negative information that is more than 7 years old

[214] Consumer-reporting agencies, however, are forced to rely on the representations of permissible purposes made by their customers. Therefore, if a customer makes a false representation, he or she can obtain a consumer report without actually having a permissible purpose. Although making such a misrepresentation is punishable under the FCRA, the penalty may not always be sufficient to discourage the conduct. Such appears to have been the case in *WDIA* v. *McGraw-Hill*, C-1-93-448 (December 1, 1998, S.D. Ohio). In *WDIA*, a consumer-reporting agency sued the parent company of *Business Week* after a *Business Week* reporter obtained a consumer report on then-Vice President Dan Quayle for an article, after falsely representing that he had a permissible purpose to receive the report. WDIA sought $75,000 in actual damages and $45 million in punitive damages. However, the court, which ruled in WDIA's favor on the merits, awarded only $7,500 in actual damages and no punitive damages at all, noting that the news coverage was a "vital public interest" and *Business Week* promised not to engage in such conduct in the future. The reporter is reported to have claimed the ruling was a "vindication." Robert Ellis Smith, "In the Courts: Business Week" *Privacy Journal*, Vol. 25, No. 3 (January 1999) p. 7.

[215] 15 U.S.C. § 1681k (FCRA § 613).

(including arrest information); 10 years for bankruptcies. A 1998 amendment to the FCRA permits the inclusion of criminal conviction information, without time limitations.

- Consumers can sue for violations or seek assistance from the FTC and other Federal agencies responsible for the enforcement of the FCRA.

— The Individual Reference Services Group

In 1997 the major companies in the individual reference services industry, joined by the three national consumer-reporting systems, established the Individual Reference Services Group (IRSG). Companies in the individual reference services industry provide public record information, including CHRI (obtained primarily from the courts), to government agencies, companies, law firms, private investigators, and, in some instances, the public. The IRSG adopted self-regulatory principles (IRSG Principles) that became effective at the end of 1998.[216] The IRSG Principles require signatory and complying companies to:

- Make efforts to educate their customers and the public about their services, the privacy issues associated with those services, the IRSG Principles, and the societal benefits from the responsible flow of information.
- Acquire individually identifiable information from only reputable sources in the public and private sector and take measures to understand the information collection practices of those sources.
- Take reasonable steps to ensure the accuracy of the information in their products, and to either correct inaccurate information or refer the individual to the agency that created the information.
- Limit the distribution of nonpublic information according to specified criteria based on the nature of the information requested and the intended use of that information.
- Maintain systems and facilities to protect information from unauthorized access by means of physical, electronic, and administrative safeguards.
- Have an information practices policy statement notifying individuals of their information practices.
- Provide individuals with a means for limiting the general public's access to nonpublic information. The companies may also provide individuals with the ability to limit access to other information in their databases.
- Provide individuals with information about the types and sources of the public record and publicly available information that the companies include in their information products and services.
- Limit the distribution of information about individuals identified as being less than 18 years of age.

— Privacy risks posed by changes in the marketplace

Changes in the marketplace, particularly the emergence of sophisticated private-sector networks providing CHRI, raise a number of privacy issues:

- First, of course, private-sector resellers of criminal histories encourage and facilitate the availability of criminal history information to the public or to non-criminal justice business users in a way that is fast, convenient, and inexpensive.
- Second, the commercial marketplace for criminal histories may exacerbate the

[216] Individual Reference Services Group, "Individual Reference Service Industry Principles" (December 15, 1997), available at **http://www.irsg.org/html/industry_principles_principles.htm**. The IRSG Principles apply to information products that assist users to identify individuals, verify identities, and locate individuals for various purposes. These identification and location products are beyond the scope and protections of the FCRA because they do not bear on one of the seven characteristics (credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living) set forth in the FCRA definition of "consumer report," which is set forth at 15 U.S.C. § 1681a(d).

risk of communicating incomplete or inaccurate records. Records obtained from police blotters or from court sources are customarily less complete than records held by the State criminal record repositories.

- Third, there is certainly the potential that the commercial-sector records will keep and disclose records, regardless of how long ago the underlying offense occurred. Although the FCRA provides a 7-year limitation for disclosures of arrest information by consumer-reporting agencies, nonconsumer-reporting agencies are subject to no such restriction. In addition, as noted, the FCRA was amended in 1998 to permit the disclosure of conviction information, regardless of the date of the conviction. As a result, it is legally possible to create a private criminal history database that will forever record and report an individual's interactions with the criminal justice system.

  Thus, private databases may outflank State sealing and expungement laws. Once a criminal record has been captured in a private database or published in the newspaper (now also electronically searchable and available on the Internet) or published on the Internet, court or other legal directives to seal or expunge those records have limited effect.

- Finally, because private databases seldom are supported by fingerprints or other biometric identifiers, they run a risk of misidentification and of attributing erroneous information to an individual. On the other hand, Task Force participants are aware of few examples of misidentification arising from name checks used in commercial criminal history reporting systems.

Although commercial harvesting and reporting of criminal histories may pose a privacy risk, it should also be noted that commercial systems meet a burgeoning noncriminal justice demand and facilitate use of these records for numerous important public safety, anti-fraud, and other economically and socially important purposes.[217]

Federal and State initiatives

The Federal government is spearheading numerous initiatives aimed at providing authorized users with better and more timely criminal justice information. One inevitable effect of such efforts is to create at least the potential for new and significant privacy risks. This report describes several initiatives.

Perhaps the most important of the new Federal initiatives is the National Instant Criminal Background Check System (NICS), which became operational in November 1998. NICS, as authorized in the 1993 *Brady Handgun Violence Prevention Act*, provides firearms dealers with instantaneous information about whether an individual has a criminal history record background that makes the individual ineligible to obtain a firearm. The NICS draws on three Federal databases that include CHRI, information on wanted persons, and certain other kinds of sensitive information, including mental health information, information on individuals who have received dishonorable discharges from the military, and citizenship status information. The sensitivity and breadth of this information, combined with its availability on a name-only basis, seems certain to add fuel to the criminal justice information privacy debate.

In 1998, as noted, Congress amended the FCRA to remove a provision that prohibited consumer-reporting agencies from reporting "obsolete" conviction information (that is, convictions more than 7 years old).[218]

[217] IRSG White Paper, *supra* note 205, p. 1. "Individual reference services provide important societal benefits. They help a broad range of people, from welfare mothers seeking to enforce child support orders, to pension beneficiaries and heirs, to fraud victims. These services also assist in important governmental functions, such as tracing fraud, apprehending criminals, and locating witnesses to crimes." Ibid.

[218] *Consumer Reporting Employment Clarification Act of 1998*, Pub. L. No. 105-347, § 5. It has been suggested that a similar FCRA obsolescence requirement for arrest information also be eliminated.

— The *Security Clearance Information Act of 1985*

The *Security Clearance Information Act of 1985* (SCIA)[219] opens virtually all CHRI to the Central Intelligence Agency, the Office of Personnel Management, the U.S. Department of Defense, and the FBI for background checks for security clearances and for placement of people in national security duties. This Act eliminated wide disparities between State laws; some gave the security agencies broad access and others provided no access at all.[220]

SCIA, however, does not provide unlimited access. The General Accounting Office (GAO), in a February 1999 report on the military's criminal history screening practices, noted that SCIA does not require States or the FBI to provide the military with access to criminal history records for determining whether an individual is suitable for mere enlistment in the military.[221] In addition, Federal agencies cannot obtain sealed data, thereby preserving State prerogatives in the area. Furthermore, Federal agencies must obtain the written consent of the individual, and the information obtained may only be used for national security purposes.

— Sex offender statutes

In 1989, Jacob Wetterling, then 11, was abducted at gunpoint by a masked man, never to be seen again.[222] In 1994, 7-year-old Megan Kanka was raped and murdered by a repeat sex offender who lived next door to her, after he lured her inside with promises to let her play with a puppy. Polly Klaas and Ashley Estelle suffered similar fates at the hands of offenders in California and Texas, respectively. These crimes brought repeat sex offenders to the forefront of the national consciousness and led to a flurry of State and Federal legislation.[223]

Texas State Senator Florence Shapiro (R-Plano), who spearheaded the drive for sex offender legislation in Texas following the abduction, rape, and murder of 7-year-old Ashley Estelle, summed up the importance of such legislation this way: "Legislatures and justice agencies must remove barriers that prevent the free flow of information between agencies so criminal justice professionals are not reluctant to do their job out of fear of liability. Information is critical to our systems. Secrecy is the sex offender's best friend, so we must shine a light on everything they do."[224] A string of recent Federal statutes seeks to turn on that light.

The *Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act*, named after Jacob Wetterling, requires States to establish effective registration systems for convicted child molesters and other sexually violent offenders. The most dangerous of these offenders, "sexually violent predators" are subject to more stringent registration standards. The Act requires States to require designated sex offenders to register and provide law enforcement with a current address for 10 years, with sexually violent predators required to provide more extensive registration information. The Act also requires that this information be retained by the State central repository and made public in certain public safety circumstances.[225]

---

[219]Pub. L. No. 99-169 (1985), codified in part at 5 U.S.C. § 9101.

[220]Robert R. Belair, "Public Availability of Criminal History Records: A Legal Analysis," in *Open vs. Confidential Records, Proceedings of a BJS/SEARCH Conference*, NCJ 113560 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, 1988) p. 16.

[221]*Military Recruiting: New Initiatives Could Improve Criminal History Screening*, GAO/NSIAD-99-53 (Washington, D.C.: U.S. General Accounting Office, February 1999) p. 11. Hereafter, Military Recruiting Report. According to this report, the U.S. Department of Defense has proposed legislative changes to "give it the authority to readily obtain access to State and local criminal history information at reasonable costs for the purpose of accepting or retaining individuals into service." Ibid., p. 12, n. 12.

[222]Patty Wetterling, "The Jacob Wetterling Story," in *National Conference on Sex Offender Registries: Proceedings of a BJS/SARCH Conference*, NCJ 168965 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, May 1998) p. 3. Hereafter, Sex Offender Registries Conference.

[223]See, Teir and Coy, *supra* note 201, p. 405.

[224]Florence Shapiro, "The Big Picture of Sex Offenders and Public Policy," in Sex Offender Registries Conference, p. 94.

[225]42 U.S.C. § 14071.

The Federal *Megan's Law*, named after Megan Kanka, builds on the *Wetterling Act*.[226] While the *Wetterling Act*, as originally enacted, gave law enforcement the option to release information about sex offenders who were perceived as a threat to public safety, *Megan's Law*, like many of its State counterparts, *requires* States to release information about sex offenders when it is required for public safety. This "mandatory community notification" is designed to inform parents and members of the community when a sex offender, who is perceived to be a threat to public safety, moves into a neighborhood. Megan's parents said after their daughter's rape and murder that they had been unaware that her killer, who was their neighbor, was a previously convicted sex offender, and that they would have been especially vigilant if they had known a convicted sex offender lived in their midst.

The third of the Federal sex offender statutes, the *Pam Lychner Sexual Offender Tracking and Identification Act*,[227] establishes a national database for the tracking of sex offenders. The Act also requires the FBI to administer sex offender registration programs in States that fail to have "minimally sufficient" programs. Finally, the Act changes the *Wetterling Act* requirement that offenders register for 10 years to a lifetime registration requirement for aggravated offenders, recidivists, and sexually violent predators.[228]

— The *Brady Handgun Violence Prevention Act*

The 1993 *Brady Handgun Violence Prevention Act*[229] established the NICS for the purpose of determining if an individual is disqualified from the purchase of a firearm on the basis of: indictment for or conviction of a felony; being a fugitive from justice; being an unlawful user of, or addicted to, a controlled substance; having been adjudicated as mentally defective or committed to a mental institution; being an illegal alien; having renounced U.S. citizenship; being dishonorably discharged from the military; having been convicted of a misdemeanor of domestic abuse; or being subject to a protective order.[230]

When a Federal firearms licensee conducts a NICS check, a name search is conducted in three different databases at the national level to determine the eligibility status of an applicant to purchase a firearm: the NCIC, III, and the NICS index. The NICS index "contains about 940,000 records of prohibited persons, as outlined in the *Brady Act*, such as individuals who have received dishonorable discharges from the armed services, individuals who have renounced their citizenship, mental defectives, illegal/unlawful aliens and others."[231]

Recognizing the potentially sensitive nature of the information that would be used by the NICS, the *Brady Act* requires establishment of security and privacy safeguards: "After 90 days' notice to the public and an opportunity for hearing by interested parties, the Attorney General shall prescribe regulations to ensure the privacy and security of the information of the [NICS] system."[232] Further, the Act prohibits gun dealers from disclosing nonpublic information received as a result of a background check except to the purchaser or to law

[226] 104 P.L. 145, 100 Stat. 1345.

[227] The Lychner Act was named in memory of victims' rights activist Pam Lychner, who founded the victims' rights organization Justice for All after she was brutally attacked by a twice-convicted felon. She later died, along with her two daughters, in the crash of TWA flight 800 in July 1996.

[228] 42 U.S.C. § 14072.

[229] Pub. L. No. 103-159 (November 30, 1993).

[230] 18 U.S.C. § 922(g) (Supp. 1997).

[231] *National Instant Criminal Background Check System (NICS): The First Seven Months (November 30, 1998-June 30, 1999)* (Washington, D.C.: Federal Bureau of Investigation, Criminal Justice Information Services Division) pp. 2-3. The 940,000 records in the NICS index, which concern mental defectives, the dishonorably discharged, etc., are currently only a small portion of the overall number of records checked as a part of a Federal NICS check, when compared to the approximately 34.7 million criminal history records in the III and the 700,000 records on wanted persons and protective orders in the NCIC. Ibid., p. 3.

[232] 18 U.S.C. § 922 Historical and Statutory Notes, National Instant Criminal Background Check System § (h) (Supp. 1997).

enforcement authorities, or pursuant to a court order. The Act also addresses the retention and destruction of background check records and firearms purchaser applications. Further, the *Brady Act* gives purchasers a right to review denials and correct erroneous information, and prohibits the establishment by Federal agencies of firearms registration systems.

On October 30, 1998, the U.S. DOJ issued final regulations for the NICS.[233] The final rule included provision for an "audit log" that would be retained on a temporary basis "solely for the purpose of satisfying the statutory requirement of ensuring the privacy and security of the NICS and the proper administration of the system."[234] During 1999, NICS' first full year of operation, NICS processed about 8.6 million inquiries. The FBI conducted about one-half of the presale background checks for which these inquiries were made, with the other half being handled by State and local agencies. In 1999, approximately 2.4% (204,000) of applications for firearm transfer were rejected. The FBI's rejection rate was 1.8% (81,000 applications) and the rejection rate for checks handled by State and local agencies was 3% (123,000 applications). In over 70% of the cases where an application for firearms transfer was rejected, a current felony indictment or prior felony conviction was the reason.[235]

— The *National Child Protection Act*

The *National Child Protection Act of 1993* (NCPA)[236] authorizes States to make nationwide background checks (based upon fingerprint-based identification) to determine if a care "provider has been convicted of a crime that bears upon the provider's fitness to have responsibility for the safety and well-being of children, the elderly, or individuals with disabilities."[237] The NCPA, as originally enacted, permitted use of the national system only as authorized by State law and approved by the U.S. Attorney General.[238] This, as might reasonably be expected, resulted in inconsistencies among State laws. National volunteer organizations, such as the Boys and Girls Clubs of America, found themselves with State-authorized access in only six States, yet with volunteers in all 50 States.[239] As a result of these concerns, Congress amended the NCPA in 1998 to permit qualified entities, such as schools or youth-serving nonprofit organizations, to conduct fingerprint-based background checks using the national system regardless of whether State law specifically authorizes them to conduct such checks, provided that certain criteria are met.[240]

The number of people/positions potentially covered by the NCPA is staggering. In the area of child care alone, for example, State criminal record check statutes frequently cover day-care, foster and adoptive homes, schools, social service/welfare agencies, school bus/ transportation services, juvenile detention/residential facilities, those with supervisory or disciplinary power over children, youth organizations, youth camps, public recreation, or youth programs.[241] The American Bar

[233]63 *Federal Register* 58303 (October 30, 1998), to be codified at 28 C.F.R., Part 25.

[234]Ibid. On November 30, 1998, the same day NICS became operational, the National Rifle Association filed suit in Federal district court arguing that the FBI's audit log, even if intended to be "temporary," was a violation of Section 103(I) of the *Brady Act* (prohibiting Federal agencies from establishing a national gun registry). Both a Federal district court and the Court of Appeals for the District of Columbia Circuit have held in favor of the government. See, *National Rifle Association of America* v. *Reno*, 216 F.3d 122 (D.C. Cir. 2000).

[235]Lea Gifford, et. al., *Background Checks for Firearm Transfers*, Bulletin series, NCJ 180882 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, June 2000), pp. 1-3.

[236]Pub. L. No. 103-209 (Dec. 20, 1993).

[237]42 U.S.C. § 5119a(a).

[238]Ibid.

[239]Testimony of U.S. Representative Mark A. Foley (R-FL) before the House Judiciary Subcommittee on Crime regarding H.R. 2488, the *Volunteers for Children Act* (April 30, 1998).

[240]*Volunteers for Children Act*, Pub. L. No. 105-251, §§ 221-222 (October 9, 1998), 112 Stat. 1885 (amending 42 U.S.C. § 5119a).

[241]Noy S. Davis, "Authorized Record Checks for Screening Child Care and Youth Service Workers," in *National Conference on Criminal History Records: Brady and Beyond, Proceedings of a BJS/SEARCH Group Conference*, NCJ 151263 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, 1995) p. 85, figure 2. Hereafter, Brady Conference.

Association Center on Children and the Law estimates that nearly 35 million adults have contact with children through these kinds of programs.[242] The NCPA also covers elder care and care of the disabled. The potential workload implications and the potential numbers of access requests for and disclosures of criminal history information are staggering.

Juvenile justice reform

Concerns regarding the frequency of juvenile crime, its periodic violence and recidivism have combined to generate pressure to open juvenile records to greater use within both the criminal justice and the non-criminal justice communities. Concomitantly, these same forces have generated pressure to improve the quality of juvenile history records, including making the records fingerprint-supported and assuring appropriate disposition reporting. Recent Federal legislation has focused attention on the privacy issues associated with juvenile records by including initiatives to rework the juvenile justice information system to make it look much more like the adult system. The effort to improve juvenile history records and to make juvenile history records more available is controversial and adds to the emerging debate over privacy and criminal justice.

— A brief history of the philosophy of the juvenile justice system

The juvenile justice system was one of the products of the "Progressive Movement" of the late 19th and early 20th centuries. "To the Progressives, crime was the result of external forces, not of the exercise of an individual's free will. Their goal was to reform the offender, not punish the offense."[243] The Illinois State Legislature established the Nation's first independent juvenile court system in 1899, to be a system in which "children were not to be treated as criminals nor dealt with by the process used for criminals."[244] The Illinois juvenile court, and those subsequently created in other States, adopted the British notion of *parens patriae* (the State as parent) and the State came to see its role as stepping in when parents failed to carry out their supervisory responsibilities.

The U.S. Supreme Court, in a 1967 decision, characterized the juvenile justice system this way: "The early conception of the Juvenile Court proceeding was one in which a fatherly judge touches the heart and conscience of the erring youth by talking over his problems, by paternal advice and admonition and in which in extreme situations, benevolent and wise institutions of the State provided guidance and help, to save him from a downward career."[245] The child was seen as impressionable and malleable, not truly responsible for his or her actions, and should not be saddled with responsibility for his or her actions in the same manner, and with the lifelong impact, as adult offenders.

The juvenile justice record-keeping system was also designed with the protection of the child in mind. A law review commentary in 1909 stressed that the importance of confidentiality for juvenile records was to "get away from the notion that the child is to be dealt with as a criminal; to save it from the brand of criminality, the brand that sticks to it for life; to take it in hand and instead of first stigmatizing and then reforming it, to protect it from the stigma — this is the work which is now being accomplished (by the juvenile court)."[246]

[242]Kimberly Dennis, "Report on National Study of Existing Screening Practices by Child Care Organizations," in Brady Conference, p. 90, figure 1.

[243]Robert R. Belair, *Privacy and Juvenile Justice Records: A Mid-Decade Status Report*, Criminal Justice Information Policy series, NCJ 161255 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, 1997) p. 6. Hereafter, Privacy and Juvenile Justice Records Status Report.

[244]Robert R. Belair, *Privacy and Juvenile Justice Records*, Criminal Justice Information Policy series (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, 1982) p. 12 (quoting Eldefonzo, *Law Enforcement and the Youthful Offender*, 3rd ed. (New York: John Wiley & Sons, 1978) p. 147).

[245]*In re Gault*, 387 U.S. 1, 25-26 (1967).

[246]Mack, "The Juvenile Court," 23 *Harvard Law Review* 104, 109 (1909).

During the 1950s and 1960s this view of the juvenile justice system came into question, with the Supreme Court noting in 1966 that "While there can be no doubt of the original laudable purpose of juvenile courts, studies and critiques in recent years raise serious questions as to whether actual performance measures well enough against the theoretical purpose to make tolerable the immunity of the process from the reach of constitutional guarantees applicable to adults."[247] The Court answered its own question in the negative, extending to juveniles much the same right to adversarial-style due process as adults.[248]

The following year the Court went further, rejecting *parens patriae* and extending to juveniles the four basic elements of due process: the right to notice, the right to counsel, the right to cross-examine witnesses, and the right against self-incrimination.[249] In that same case, *In re Gault*, the Court questioned the confidentiality of juvenile records, noting "the summary procedures of Juvenile Courts are sometimes defended by a statement that it is the law's policy 'to hide youthful errors from the full gaze of the public and bury them in the graveyard of the forgotten past.' This claim of secrecy, however, is more rhetoric than reality."[250]

Although the Supreme Court's extension of "adult" rights to juveniles broke down one of the walls around the juvenile justice system, increased juvenile crime (and increased media attention to juvenile crime) created additional pressures for changes in the juvenile justice system. Public attitudes toward youthful offenders hardened over the years, with ever-decreasing tolerance for youthful offenders, particularly violent offenders. While the public might agree that shoplifting was a "youthful error," youth gangs, and random violence by juveniles are unlikely to be included in that category.

A vigorous debate began as to the extent to which the juvenile recordkeeping system should be integrated with that of the adult system by either unifying the records or at least linking the adult and juvenile records.[251] Those arguing for the maintenance of separate record systems believe the juvenile system should continue to adhere to its Progressive traditions with respect to juvenile justice records. As one commentator observed: "The juvenile justice system should open its records to the criminal justice system and the public only if it is in the best interest of the child, and I have serious doubts that it ever would be."[252]

The statistical growth of violent juvenile crime during the late 1980s and early 1990s, and the media attention accompanying it, created a powerful counter-argument for many. As Reggie B. Walton, formerly the presiding judge of the criminal division of the District of Columbia Superior Court put it: "To the crime victim, and society as a whole, it matters not whether the offender is 16 or 17, or has just turned 18. What is important is that a crime has been committed, an injury has been sustained, and protection against further acts by the perpetrator are taken if and when the offender is apprehended … greater utilization of juvenile records is warranted, so long as measures have been taken to guard against abuses."[253]

Although the solution to the problem is debatable, Judge Walton's assessment of public opinion and the public's fear of crime, particularly juvenile crime, appears right on the mark. Anecdotal evidence of youth violence is plentiful, including a recent string of school shootings by juveniles. This

[247] *Kent* v. *United States*, 383 U.S. 541, 555 (1966).

[248] Ibid.

[249] *In re Gault*, 387 U.S. 1 (1967).

[250] Ibid., at 24.

[251] See generally, Juvenile and Adult Records, *supra* note 128.

[252] Howard N. Snyder, "Thoughts on the Development of and Access to an Automated Juvenile History System," in Juvenile and Adult Records, *supra* note 128, p. 56.

[253] Reggie B. Walton, "Utilization of Juvenile Records in Adult Proceedings, A Judge's Perspective," in Juvenile and Adult Records, *supra* note 128, p. 43. Others, such as the National Council of Juvenile and Family Court Judges, have argued that the confidentiality surrounding juvenile justice *proceedings* should be "reexamined and relaxed to promote public confidence" in juvenile courts. See, Hon. Gordon A. Martin Jr., "Open the Doors: A Judicial Call to End Confidentiality in Delinquency Proceedings," 21 *New England Journal on Criminal and Civil Confinement* (Summer 1995) 393, 410.

series of school shootings is a tragic, well-publicized manifestation of juvenile crime, which rose significantly during the late 1980s and early 1990s before beginning to decline.

Despite a series of high-profile juvenile crimes, including the high school shootings, the "substantial growth in juvenile violent crime arrests that began in the late 1980s peaked in 1994."[254] In 1998, for the fourth year in a row, the total number of juvenile arrests for Violent Crime Index offenses — murder, forcible rape, robbery, and aggravated assault — declined.[255] Even with these declines, however, the number of juvenile Violent Crime Index arrests remained higher than the 1988 level.[256]

— Recent legal trends

State legislatures took note of media and public concerns. Beginning in the late 1970s, they have instituted a number of reforms that have radically impacted the functioning of the traditional juvenile justice system, including revising the circumstances under which juveniles can be transferred for trial in the adult system, increased centralization of juvenile records, increased availability of juvenile records outside the juvenile system, increased fingerprinting, and, most recently, DNA testing of juveniles.

First, the States have made it easier to transfer juveniles from the juvenile system to the adult system by establishing a system of discretionary and mandatory circumstances under which youth are transferred from the juvenile system to the adult system to be "tried as adults." A 1995 GAO report found that since 1978, 44 States and the District of Columbia had amended their statutes addressing the circumstances under which juveniles could be tried in criminal court. The GAO found that in 24 States, these changes have increased the population of juveniles subject to transfer to adult courts (primarily by decreasing the age at which juveniles may be transferred or by increasing the number and types of offenses subject to transfer); in three States, these changes have decreased the population of juveniles subject to transfer; and in 17 States, changes in the law have neither increased nor decreased the population subject to transfer.[257] The criminal history records relating to an offense for which a juvenile is charged as an adult typically are maintained in the adult CHRI system and treated the same as other adult records, a largely uncontroversial practice.

Second, juvenile justice records are being maintained on an increasingly centralized basis. Juvenile justice records were traditionally maintained on a dispersed and local basis; however, the centralization trend that reshaped the maintenance of adult records in the 1960s and 1970s has had an increasing impact on juvenile records as well. In 1988, only 13 of the 50 State repositories for adult records maintained juvenile record information. By 1995, 27 States had expressly authorized a central repository for the collection and maintenance of juvenile criminal history information, either by the adult repository or a special juvenile repository.[258] In addition, in 1992, the Attorney General authorized the FBI to begin accepting State-reported data concerning serious juvenile offenses.[259] The FBI decided to disseminate this juvenile information under the same standards applicable to adult records.[260]

A third trend in recent years is the increasing availability of juvenile justice record information outside of the juvenile system. In contrast to the situation in the early 1980s, by the end of 1995 juvenile justice information is almost fully available to adult courts for sentencing and

[254]Howard N. Snyder, *Juvenile Arrests 1997*, Juvenile Justice Bulletin series, NCJ 173938 (Washington, D.C.: U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, December 1998) p. 1. Hereafter, Juvenile Arrests 1997.

[255]*Crime in the United States, 1998 Uniform Crime Reports* (Washington, D.C.: U.S. Department of Justice, Federal Bureau of Investigation, 1999) p. 209.

[256]Juvenile Arrests 1997, *supra* note 254, p. 1.

[257]Privacy and Juvenile Justice Records Status Report, *supra* note 243, pp. 8-9.

[258]Ibid., p. 23.

[259]Use and Management of CHRI, *supra* note 22, p. 23.

[260]Ibid.

most other purposes.[261] "In roughly one-half the States, prosecutors have a statutory right of access to juvenile record information and a BJS survey indicates that prosecutors, in most States, have little difficulty in obtaining access."[262] There are also signs that juvenile records are becoming available outside the justice system. According to a 1996 Navy survey, three States release the juvenile records of applicants for enlistment to the military.[263] Access to these records is of interest to the military because "juvenile crime records are likely to be a major source of criminal history information for the population targeted by military recruiters — men and women generally 17 to 21 years old."[264]

A fourth trend in the juvenile system that has privacy implications is increased fingerprinting, photographing, and obtaining DNA samples from juveniles. Traditionally, photographs and fingerprinting were undertaken only for the most serious of offenses likely to go before a juvenile judge; however, by 1995, 40 States had expressly authorized police to take fingerprints when arresting a juvenile.[265] Twenty-two States limited the fingerprinting to offenses that would have been a felony if committed by an adult, five States authorized fingerprinting for offenses that would be either felonies or misdemeanors if committed by an adult, and 13 States made no reference to the type of offense.[266] With the advent of DNA testing in the late 1980s, State legislatures have rushed to add new statutes authorizing the collection of DNA samples of juveniles, with at least 25 having done so by mid-1998.[267] These statutes typically, but not always, limit the collection of DNA samples to juveniles who have committed specified offenses, typically sexual offenses, violent crimes, and other felonies.[268]

All of these recent trends have seriously eroded the Progressive Model for the juvenile justice system. The turn of the century system, which still has substantial support, envisioned its role as a firm hand that could provide an errant child with rehabilitation and a fresh start, with sealed records being one means of meeting that goal.[269] Other

[261]Privacy and Juvenile Justice Records Status Report, *supra* note 243, p. 28.

[262]Ibid.

[263]Military Recruiting Report, *supra* note 221, p. 12. 18 U.S.C. § 5038 limits the disclosure of Federal juvenile records to judicial inquiries, law enforcement needs, juvenile treatment requirements, positions raising national security concerns, and certain victim inquiries. Ibid.

[264]Ibid.

[265]Privacy and Juvenile Justice Records Status Report, *supra* note 243, p. 28.

[266]Ibid.

[267]See, for example, ALA. CODE § 12-15-102 (Michie Supp. 1997); ALASKA STAT. § 44.41.035 (Michie 1996); ARIZ. REV. STAT. ANN. § 13-4438 (West Supp. 1997); ARK. CODE ANN. § 12-12-1109 (Michie Supp. 1997); CAL. PENAL CODE § 290.2 (West Supp. 1998); FLA. STAT. ANN. § 943.325 (West 1996 & Supp. 1998); IDAHO CODE § 19-5506 (Michie 1997); KAN. STAT. ANN. § 21-2511 (Supp. 1997); LA. REV. STAT. ANN. § 15:601 (West Supp. 1998); ME. REV. STAT. ANN. tit. 25, § 1573 (West Supp. 1997); MICH. COMP. LAWS ANN. § 28.173 (West Supp. 1998); MONT. CODE ANN. § 44-6-103 (1997); N.H. REV. STAT. ANN. § 632-A:21 (Michie Supp. 1997); N.J. STAT. ANN. § 53:1-20.20 (West Supp. 1998); N.M. STAT. ANN. § 29-16-3 (Michie 1997); OHIO REV. CODE ANN. § 2151.315 (West Supp. 1998); OR. REV. STAT. § 181.085 (1997); 35 PA. STAT. ANN. § 7651.306 (Purdon Supp. 1998); S.C. CODE ANN. § 23-3-620 (West Supp. 1997); TEX. GOV'T CODE § 411.150 (Vernon's Supp. 1998); UTAH CODE ANN. § 53-5-212.1 (1998); VA. CODE ANN. § 16.1-299.1 (1998); WASH. REV. CODE § 43.43.754 (West Supp. 1998); and WIS. STAT. ANN. § 165.76 (West 1997).

[268]See, for example, MONT. CODE ANN. § 44-6-103 (1997) (applies to youth found to have "committed a sexual or violent offense"); 35 PA. STAT. ANN. § 7651.306 (Purdon Supp. 1998) (applies to a "person who is convicted or adjudicated delinquent for a felony sex offense or other specified offense"); ALASKA STAT. § 44.41.035 (Michie 1998) (applies to minors age 16 and above, "adjudicated as a delinquent for an act that would be a crime against a person if committed by an adult").

[269]There are a number of initiatives around the country, such as Juvenile Drug Courts, that attempt to rehabilitate youthful offenders, under the watchful eye of a judge, through innovative, integrated social service programs for the offender and his or her family. See, for example, Robin J. Kimbrough, "Treating Juvenile Substance Abuse: The Promise of Juvenile Drug Courts," *Juvenile Justice* Vol. V, No. 2 (Washington, D.C.: U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, December 1998) pp. 11-19. Such programs may trigger additional privacy protections depending on the entities involved and the subject matter. Certain substance abuse treatment records are subject to

societal concerns have weighed against that model and in favor of treating juveniles convicted of violent crimes the same as, or more like, adults. First and foremost was the rise in juvenile crime (now somewhat mitigated), particularly violent crimes. These crimes make it difficult for the public to accept the notion that the perpetrator should get a fresh start rather than life imprisonment.

Some have argued that the majority of those juveniles in the juvenile system desist from future criminal acts (or what would be criminal acts if committed by adults), and that perhaps the test for access to the juvenile's records by the adult system and the public should be whether the juvenile offender comes within the purview of the adult system within a certain number of years of having reached the age of majority.[270] Others have raised concerns that it is unfair to a first-time adult offender with no juvenile record to be treated the same way as an adult who had a juvenile record, which is kept from the court so that offender could get a "fresh start."

Although the trend in recent years has been toward greater access to juvenile records, the debate is ongoing and the central policy questions surrounding the juvenile recordkeeping system remain largely unresolved. Final resolution of these and other policy questions are likely to be influenced by juvenile crime statistics and the public's reaction to the crimes those statistics represent, as well as the success of rehabilitation efforts directed at youthful offenders.

Criminal intelligence information systems

Innovations in the development and operation of criminal intelligence systems are another change driver encouraging a reexamination of privacy protections for criminal justice information.

The terms "criminal investigative information" and "criminal intelligence information" are often used interchangeably. They relate, however, to two distinct, although related, concepts.[271] *Criminal investigative information* is defined to mean "information on identifiable individuals compiled in the course of an investigation of specific criminal acts."[272] *Criminal intelligence information*, in contrast, is defined as "information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity."[273] Criminal intelligence and investigative systems may gather the same types of information about individuals; the principal difference is the purpose for which information is gathered.[274] Criminal intelligence information-gathering efforts are frequently the more controversial, as they involve collection of information not about a person's connection with an actual crime, but rather a person's possible connection to criminal activities.

Both the importance and sensitivity of this information have long been recognized. Criminal intelligence information, for example, is an essential tool in controlling organized crime activity, as well as gang activity, drug trafficking, and terrorism. At the same time, the privacy sensitivity of criminal intelligence information and its potential impact on freedom of association rights has been recognized. The growth of criminal intelligence-gathering efforts slowed during the 1970s following a series of congressional

Federal confidentiality protections. See, 42 C.F.R. Part 2. In addition, if educational institutions are involved, privacy protections in the *Family Educational Rights and Privacy Act of 1974*, Pub L. No. 93-380 (codified at 20 U.S.C. § 1232g), requires educational institutions to grant students or parents access to student records and establishes limits on disclosure to third parties.

[270]Mark H. Moore, "The Public Policy Considerations of A Merged Record," in Juvenile and Adult Records, *supra* note 128, p. 48.

[271]Intelligence and Investigative Records, *supra* note 26, p. 9.

[272]Technical Report No. 13, 3rd ed., *supra* note 8, Standard 2.1(d).

[273]Ibid. at Standard 2.1(e). Federal regulations define "criminal intelligence information" to mean "data which has been evaluated to determine that it: (i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) Meets criminal intelligence system submission criteria." 28 C.F.R. § 23.3(b)(3).

[274]Intelligence and Investigative Records, *supra* note 26, p. 10.

hearings chaired by then-U.S. Senator Frank Church (D-ID). These hearings exposed a number of criminal intelligence system abuses that occurred during the civil unrest of the 1960s and early 1970s, as well as during the Watergate period. In 1975, LEAA issued regulations governing the gathering of criminal intelligence information that covered any criminal intelligence system receiving funding through the *Omnibus Crime Control and Safe Streets Act of 1968*.[275] The LEAA criminal intelligence regulations require that information be "relevant" and that the individual or organization in question be "reasonably suspected of involvement in criminal activity."[276] Since this congressional and regulatory activity, a number of salient developments have occurred with important privacy implications:

1. First, criminal intelligence and investigative information systems have become automated. Traditionally, criminal intelligence and investigative information systems consisted of little more than notebooks and other manual files. In the past 25 years, however, the automation of this information has expanded at a rapid rate, so that today, virtually all large and important criminal intelligence systems are automated. This, in turn, has encouraged the establishment of more criminal intelligence systems, with more data, about more people.
2. Second, criminal intelligence systems have become far more textured and robust. Today there are a multitude of data sources, allowing intelligence files to be compiled and supplemented using personal information obtained from other criminal intelligence information systems, newspapers, commercial vendors, and other information sources. This information may include financial data, medical information, family data, and other very sensitive types of information.
3. A third important change is the increased sharing of criminal intelligence information among jurisdictions. Traditionally, criminal intelligence information was maintained locally, with little sharing of information outside of the host agency. During the late 1960s, attempts to create regional criminal intelligence information compacts failed.[277] Today, fueled by automation and with increased Federal funding, this information is increasingly shared between jurisdictions and agencies, both in terms of "vertical sharing" between local police, State police, and the FBI, and "horizontal sharing" between States and between local law enforcement organizations.

The Task Force recognizes that the analysis and structuring of privacy policies for criminal intelligence data is complex and raises issues that are substantially different than the privacy issues raised by changes in CHRI and other criminal justice information systems. Accordingly, the Task Force recommends that the U.S. DOJ sponsor an initiative exclusively dedicated to the examination of the privacy implications arising from a new generation of criminal intelligence information systems.

[275]See, 28 C.F.R. Part 20.

[276]28 C.F.R. § 23.3(b)(3)(i).

[277]Intelligence and Investigative Records, *supra* note 26, p. 20.

VI. Task Force recommendations

Background

The National Task Force on Privacy, Technology and Criminal Justice Information brought together representatives from the academic community, State and Federal government, law enforcement, the courts, commercial compilers of criminal justice information, the privacy advocacy community, and others who have expertise in criminal justice information and privacy and who are national leaders in the debate about criminal justice information privacy. Task Force members cover the privacy spectrum from those favoring high levels of privacy protection for criminal justice information to those favoring high levels of public use and disclosure.

As this report indicates, the Task Force has identified a series of "change drivers" that are profoundly changing the traditional balance between criminal justice information access and privacy. Without intervention by policymakers, those change drivers inevitably will create an environment favoring enhanced public access and use, with no assurance that the resulting balance between access and privacy will be satisfactory.

Although constituted to examine "privacy, technology, and criminal justice information," the Task Force made an early determination to focus its time and resources on the complex issues associated with access to CHRI. Accordingly, the Task Force report does not address, in any depth, the broad range of other issues arising from the increasing demand for public access to other types of criminal justice information, such as intelligence and investigative data, and the accompanying privacy risks associated with making that data more widely available.

Task Force recommendations comprise a range of proposals for handling CHRI. Recommendation I reflects the Task Force's conclusion that change drivers are creating a pattern of essentially making ad hoc policy at the local, State, and national level. The Task Force believes there is a need, at least in the short term, for an institutionalized entity responsible for making considered public policy recommendations with respect to all issues associated with the increasing demand for criminal justice information and the privacy risks associated with that demand.

Recommendations and commentary

The National Task Force on Privacy, Technology and Criminal Justice Information adopts the following 14 recommendations in three broad areas: privacy protections, data quality and security, and data integration and amalgamation.

Action is necessary to ensure appropriate privacy protection

Recommendation I: The Task Force recommends that a body be statutorily created to consider and make policy recommendations to the Federal and State legislative, executive, and judicial branches of government as they work to balance the increasing demand for all forms of criminal justice information and the privacy risks associated with the collection and use of such information. The Task Force recommends that the body look at information and privacy issues arising from all types of criminal justice information, including criminal history record information, intelligence and investigative information, victim and witness information, indexes and flagging systems, wanted person information, and civil restraining orders. The Task Force further recommends that such a body be comprised of public and private stakeholders; that the body be limited to an advisory role; and that it have neither rulemaking nor adjudicatory authority. Finally, the Task Force recommends

that the body sunset after not more than 3 years, unless statutorily reauthorized.

Commentary:

- The Task Force believes that without the establishment of a body to study and provide guidance on criminal justice privacy issues on an ongoing basis, the change drivers identified in chapter V of this report will result, essentially, in a pattern of ad hoc policymaking at the local, State, and national level.
- The Task Force believes that the establishment of a body dedicated to the detailed examination of issues relating to the privacy, confidentiality, and security of criminal justice information is necessary to build upon the work of the Task Force and provide advice and guidance to local, State, and Federal agencies, courts, and policymakers on the many issues surrounding the collection, use, maintenance, and dissemination of criminal justice information.
- The Task Force believes there is a need, at least in the short term, for an institutionalized entity responsible for making considered public policy recommendations with respect to all issues associated with the increasing demand for criminal justice information and the privacy risks associated with that demand. Although the Task Force has made a number of recommendations, the Task Force believes that additional, detailed work is necessary, particularly when the discussion moves from general principles to more specific policy issues.
- The body would not have adjudicatory or rulemaking authority. The Task Force envisions an advisory body, available to consult and advise Federal, State, and local officials, as well as the public, on criminal justice privacy issues. The Task Force believes this approach respects the nature of our Federal system, while providing a mechanism to provide guidance at all levels of government.
- The Task Force believes the new body should include representatives of public- and private-sector organizations that create, use, compile, or sell criminal justice information. Examples of categories of entities that the Task Force believes should be represented in the new body include: law enforcement, the courts, prosecutors, corrections, criminal history repositories, academics, privacy advocates, commercial compilers, and the media. Public-sector representation should include Federal, State, and local officials, as appropriate.
- The Task Force believes that a short-lived body will be sufficient to guide the formulation of a new generation of criminal justice information privacy laws, regulations, and policies. If a longer period of time proves necessary, an extension permitting the body to continue its work could be considered.

Recommendation II: The Task Force recommends the development of a new generation of criminal justice information and privacy law and policy, taking into account public safety, privacy, and government oversight interests. This law and policy should be broad in scope, so as to address the collection, maintenance, use, and dissemination of criminal justice record information by law enforcement agencies, including State central repositories and the FBI, the courts, and commercial compilers and resellers of criminal justice record information.

Commentary:

- When the first criminal history record privacy principles were developed in the mid-1970s, they were designed to regulate the actions of a relatively limited number of entities. Today, CHRI is collected, maintained, used, and disclosed by numerous types of entities, including, in particular, law enforcement agencies (local police, State central

repositories, and the FBI); courts; and commercial compilers and resellers. Thus, it makes little sense and achieves little purpose to fashion privacy and confidentiality policy and law that applies to only one of these sectors.

- On the other hand, certainly there can be differences in standards for collection, maintenance, use, and disclosure based upon special considerations pertaining to each of these sectors. Notwithstanding these differences, any law or policy should at least take into account and, where possible, synthesize or rationalize standards among the various sectors that collect, maintain, use, and disclose CHRI.
- Any standards established for private actors, such as the media and commercial compilers, should carefully consider the first amendment interests of these entities.

Recommendation III: The Task Force recommends that the adequacy of existing legal remedies for invasions of privacy arising from the use of criminal history record information should be reexamined by legal scholars, State legislatures, Congress, State and Federal agencies, and the courts.

Commentary: Individuals who are aggrieved by privacy violations arising from their arrest and/or conviction information face substantial legal hurdles if they are to obtain any type of relief. The outcome of a judicial privacy challenge pivots on the nature of the privacy complaint (was the information incomplete or inaccurate? old or otherwise not relevant? subject to a seal or purge order? used without the individual's knowledge or opportunity to respond?); the identity or category of the defendant (was it a Federal or State law enforcement agency? a court? the media? a commercial information broker?); as well as the nature of the alleged harm (can the individual/plaintiff demonstrate tangible harm or "merely" intangible harm, such as stigma or embarrassment?). These factors, as well as the victim's legal theory (tort, statutory rights, or constitutional rights) and the interplay of these legal theories with the defendant's legal and constitutional rights to obtain, use, and disseminate CHRI, determine the outcome of most criminal history privacy claims. In the new information era where CHRI — even aged or purged information — remains not just available, but easy and inexpensive to use and disseminate, the question arises whether traditional judicial remedies remain meaningful.

Recommendation IV: The Task Force recommends the development of a new generation of confidentiality and disclosure law and policy for criminal history record information, taking into account the type of criminal history record information; the extent to which the database contains other types of criminal justice information (victim and witness information, or intelligence or investigative information) and sensitive personal information (medical or financial information, and so on); the purpose for the intended use of the information; and the onward transfer of the information (the redissemination of the criminal history information by downstream users).

Commentary:

- In assessing the privacy risk posed by CHRI, the source of the information is unlikely to be a compelling consideration. If the source is a central repository, for example, as opposed to a court, why does this affect the privacy impact on the individual?
- On the other hand, the *type* of criminal history information seems far more likely to create a privacy impact. Arguments can be made, for example, that:
  - — Juvenile justice record information should be treated differently than adult CHRI.

— Witness and victim information should be treated differently.

- Further, arguments can be made that the purpose of the intended use should be a criterion for shaping privacy policy. Relevant questions as to use include the following:
  - — Should the traditional distinction between criminal justice uses and noncriminal justice uses be retained?
  - — Should there be any distinctions among criminal justice uses?
  - — Should governmental, noncriminal justice be treated differently than private, noncriminal justice uses?
  - — Should national security use continue to receive a high priority?
  - — Is there a meaningful distinction between licensing uses and employment uses?
  - — Should the identity (as opposed to the purpose) of the prospective user be a criterion for imposing restrictions?

Recommendation V: The Task Force recommends that intelligence and investigative information also be addressed by new privacy law and policy, but that this process should begin with the establishment of a Task Force dedicated exclusively to a review of intelligence and investigative systems, and the law and privacy issues related to those systems.

Commentary:

- Task Force members agree that intelligence and investigative information systems are growing in number and size. Moreover, these systems sometimes contain CHRI and other types of sensitive personal information.[278] The ubiquity and importance of these systems appear to be having an impact upon the information culture, and appear to pose privacy risks.
- Task Force members also agree that intelligence and investigative information should be addressed as part of any new generation of privacy policy. The Task Force recommends, however, that prior to crafting proposed law or policies for intelligence and investigative information and information systems, a separate Task Force or initiative examine both the privacy risks and the important public safety interests relating to these systems. The sources, requirements for confirmation (accuracy) of data, retention, dissemination, purpose, and usage policies for criminal intelligence and investigative data are different than those policies as they relate to CHRI and should be separately examined by a Task Force with greater representation from the intelligence and investigative community than was present on this Task Force.[279]

[278]The RISS.NET (Regional Information Sharing Systems) and its compatible components — Western States Information Network's (WSIN) Statewide Integrated Narcotic System (SINS), the California Bureau of Investigation's Automated Criminal Intelligence File (ACII), and the Southwest Border States — are among the most important criminal intelligence systems. Both the SINS and ACII have developed integrated data submission capabilities between investigations and criminal intelligence. Each operates under file guidelines (CFR 28, part 23 governs Federal systems, and the ACII follows the California Attorney General's Criminal Intelligence File Guidelines).

[279]It bears emphasis that criminal intelligence and investigative systems, while both different than criminal history systems, are also very different from each other:

Criminal Intelligence Information vs. Investigative Information

- Proactive vs. Reactive
- Prevention vs. Identification
- Not intended for court vs. Intended for court
- "Soft" information vs. "Hard" information
- Not necessarily crime-related vs. Must be crime-related

Organizations that have extensive experience in these arenas, and which would need to be represented in any review of the privacy implications of intelligence and investigative systems, include: the RISS, the Law Enforcement Intelligence Unit (L.E.I.U.), and the Board of Directors for the Association of State Criminal Investigative Agencies (ACIA).

Data quality and security are important

Recommendation VI: The Task Force recommends that legislators and criminal history record information system managers develop, implement, and use the best available technologies to promote data quality and data security.

Commentary: Data security and data quality are fundamental fair information practices. The Task Force believes that it is vital that the system managers in the criminal history information community continue to promote the quality and security of data through the use of new technology.

Recommendation VII: The Task Force recommends that criminal history record information, whether held by the courts, by law enforcement, or by commercial compilers and resellers, should, subject to appropriate safeguards, be supported by and accessible by fingerprints to the extent legally permissible and to the extent that technology, cost, and the availability of fingerprints to both database managers and users make this practicable.

Commentary:

- Use of fingerprints when conducting record checks is a means of enhancing data quality and data accuracy, by reducing the potential for identification errors that may result in a false positive or false negative response to a background check or other type of inquiry.
- Requesting or requiring fingerprints to compare to existing criminal history records gives the individual notice and, if optional, the opportunity to consent to the records check. Name-only checks, by contrast, can be conducted without the individual's knowledge or consent. On the other hand, several Task Force members noted that obtaining fingerprints is more intrusive than a name-only check.
- Changes in technology (livescan and IAFIS) may soon make fingerprinting just as quick, convenient, and inexpensive as "name-only" checks.
- Relying on "name-only" checks inevitably means that requesters must collect and use more demographics, such as Social Security numbers. This carries its own privacy risk and provides a further argument in favor of fingerprinting.
- Mismatched information (applying the wrong CHRI to the wrong person) is a major privacy risk and is associated with name-only checks. This also provides a basis for the use of fingerprinting. In some jurisdictions a "name-only" check is used as an initial screen and is then followed by a fingerprint check only if the name check indicates a potential record match. Although this reduces the potential for a false positive, it does not reduce the potential for a false negative.
- The use of aliases creates a risk that name-only checks will not retrieve available criminal histories, thus creating a public safety risk. This also provides a basis for fingerprint-based searches.
- Commercial compilers and resellers of CHRI and their customers seldom have access to fingerprints. Future changes in technology, however, may make the use of fingerprints more practical and cost-effective. The Task Force encourages the use of fingerprints when practical.
- The collection and use of fingerprints should be accompanied by appropriate safeguards to ensure the accuracy, security, and confidentiality of the fingerprints collected. In cases where fingerprints are requested (such as in the employment context) rather than required (such as in arrest context),

individuals should receive notice prior to the collection of fingerprints of the collecting entity's information practices, including whether the fingerprints will be retained or databased for future use.

Recommendation VIII: The Task Force recommends that criminal history record information should be sealed or expunged (purged) when the record no longer serves an important public safety or other public policy interest. A sealed record should be unsealed and available for criminal justice and/or public use only when the record subject has engaged in a subsequent offense or when other compelling public policy considerations substantially outweigh the record subject's privacy interests. During the period that a criminal history record is sealed, use and disclosure should be prohibited.

Commentary:

- At present, laws in 40 States provide for the purging of nonconviction information and in 26 States for the purging of conviction information. Also at present, laws in 31 States provide for the sealing of nonconviction information and in 30 States for the sealing of conviction information. The standards for a purge or seal order vary substantially among the States, but turn on the type of offense, the number of previous offenses, and the establishment of a "clean record" period. The methods for obtaining a seal or purge order also vary substantially among the States and include statutory or automatic sealing or purging mechanisms, as well as record subject-initiated and court-ordered purging and sealing.
- Sealing standards should apply not only to criminal history records at the central State repository, but also to original records of entry and to commercially maintained CHRI.
- Several Task Force members supported the position that expunging a criminal history record from all levels of the criminal justice system should not be done because it effectively "rewrites history" and creates the potential for confusion. They argued that this confusion is exacerbated by the fact that the media and commercial compilers of information increasingly retain a record of the underlying event. Although it may be advisable from a privacy standpoint to regulate future disclosures of a particular record, the record itself should not be destroyed. The Task Force as a whole, however, declined to adopt this position, noting that expungement could serve important privacy interests and should be available to the courts and criminal justice agencies, particularly in the case of individuals who have been falsely accused.
- The Task Force recognizes that while it is inefficient for all levels of the criminal justice system to retain all criminal history records in perpetuity, records should be retained permanently by at least one agency, such as the FBI at the Federal level and the State repositories at the State level, unless expungement has been ordered by a competent court or authority.
- The Task Force recommendation pertains to the criminal history record of living persons. The Task Force does not believe all records need to be retained or sealed in perpetuity. There may be some records, however, that should be retained beyond the death of the record subject for academic or government oversight purposes. In addition, it may be appropriate to unseal some records following the death of the subject (or some reasonable duration thereafter) for academic or government oversight purposes.

Recommendation IX: The Task Force recommends that individuals who are the subject of criminal history record information be told about the practices, procedures, and

policies for the collection, maintenance, use, and disclosure of criminal history information about them; be given a right of access to and correction of this information, including a right to see a record of the disclosure of the information in most circumstances; and enjoy effective remedies for a violation of any applicable privacy and information standards. In addition, the Task Force recommends that States establish meaningful oversight mechanisms to ensure that these privacy protections are properly implemented and enforced.

Commentary:

- This recommendation promotes transparency in the collection, use, disclosure, and retention of CHRI. The Task Force believes that requiring the publication and distribution of notice of the system's data practices will promote a continued dialogue and review of privacy issues and policies.
- Increasingly, notice is a fundamental part of every information privacy law and standard. In addition, providing record subjects with a right of access is also a means of improving data accuracy.
- Although individuals may not have a choice about being arrested, once the individual is arrested, he or she has some choice about the disposition of the charges. This choice may affect the type of information that becomes a part of a criminal history record. For example, if the individual enters a drug court or into a particular type of diversion or probation program, the consequences of that choice include different information consequences.
- At present, the law in 43 States requires the creation and maintenance of transaction logs (records describing the use and disclosure of criminal history records), and requires that record subjects be given access to the logs. These laws provide a significant privacy benefit. The Task Force believes that courts and commercial providers of CHRI should be required to maintain these types of logs, and provide access to record subjects as well. Access to information contained in these logs may, however, need to be restricted in certain instances if disclosure would implicate attorney-client privilege, attorney work product privilege, or where disclosure would interfere with ongoing investigations either by law enforcement or employers.
- In part as a result of pressure from the European Union, U.S. policymakers have recently taken a new look at the availability and practicality of remedies for violation of privacy law and regulations. Most States provide for both civil remedies and criminal penalties in the event of a violation of their criminal history record statute. It is not clear, however, whether these remedies are practicable or convenient for record subjects. Furthermore, there is reason to believe that these remedies are seldom invoked. Finally, these remedies do not apply to courts or commercial compilers and resellers.
- The Task Force noted, however, that a number of laws provide at least some of the types of protections called for by this recommendation. The *Fair Credit Reporting Act*, for example, provides individuals with rights regarding the use of CHRI in the employment context.

Recommendation X: The Task Force recommends that where public safety considerations so require, the record of a juvenile offender who commits an offense which, if committed by an adult, would be a felony or a violent misdemeanor, be treated in the same manner that similar adult records are treated. Even if a State opts to retain stronger privacy and confidentiality rules for these

types of juvenile records, these records should be fingerprint-supported and should be capable of being captured in an automated, national system.

Commentary:

- Juvenile justice record policy is currently the subject of debate in the Congress and many State legislatures. Legislation currently before Congress would grant greater access to juvenile justice information arising from offenses that would be considered a felony, or in some bills a violent felony, if committed by an adult. These bills would create incentives for States to disseminate information on juvenile violent felonies on the same basis as records relating to adult felonies. In most instances, however, the legislation would restrict access to information about juvenile offenses to the courts, law enforcement agencies, and schools.
- The Task Force recognizes that State law and State practice with respect to the administration of juvenile justice systems and record-keeping varies substantially. Implementing this recommendation will likely require greater cooperation and coordination among the States to ensure that the type and quality of data collected are similar across the States.
- The Task Force discussed the question of whether there should be a minimum age requirement incorporated into this recommendation. Although most Task Force members agreed that age is a relevant factor, a consensus age was not reached. Broadly speaking, Task Force members were more comfortable applying the recommendation to older juveniles than to younger juveniles. Several Task Force members suggested 14, although others found that age to be too low. Another Task Force member observed that focusing on the age of the offender, rather than the crime committed, is a flawed approach, citing cases, particularly in the narcotics trafficking context, where adults and older juveniles use young children to commit crimes, knowing that the child will face only limited repercussions.
- Even if States opt to retain a juvenile justice record information policy that provides more confidentiality and privacy protections than is provided for adult records, States should: require fingerprinting so as to be able to reliably identify the juvenile; and require that these records be captured in a manner that at least creates the capability to share these records on a national basis.
- The Task Force believes that in certain circumstances, juveniles deserve a "second chance," and, therefore, these juvenile records warrant greater privacy protection than adult records. On the other hand, the Task Force also believes that juvenile adjudications for serious offenses should be available for public safety purposes on the same basis as adult adjudications. Public safety purposes include law enforcement uses, court uses, uses by the military, uses for background checks for security clearances, screening firearms purchasers, and uses for background checks for sensitive public and private employment positions.

Data integration and amalgamation issues are important

Recommendation XI: The Task Force recommends that criminal justice record information law and policy should restrict the combining of different types of criminal justice record information into databases accessible to non-criminal justice users and should restrict the amalgamation of criminal justice record information in databases with other types of personal information, except where necessary to satisfy public policy objectives.

Commentary:

- As a matter of law and custom, CHRI has been limited to subject identification information; a history of arrests and dispositions; and, occasionally, other types of information, such as juvenile record information, special felony conviction flags, or pretrial release information.
- The law in over a dozen States restricts CHRI from being integrated or combined with intelligence and investigative information. Even more States have adopted law or standards that prohibit combining CHRI with juvenile record information.
- In recent years, a number of studies and reports have called for expanding criminal history records to include information about victims, witnesses, and certain other third parties. Amalgamation, therefore, potentially implicates the privacy and safety interests of those other than offenders and arrestees.
- There are instances when the amalgamation of various types of criminal justice information or the amalgamation of criminal justice information with other personally identifiable information may be necessary to further public policy goals, such as public safety. The Task Force notes that public policy need not be expressed in terms of legislation, but may also result from judicial decisions or executive branch policies.
- This recommendation would restrict the creation of profiling databases that would combine CHRI with other types of personal information. This is a forward-looking recommendation, as the Task Force is unaware of the existence of any such database at present. What is customary, and would remain unchanged by this recommendation, is the ability of commercial compilers and investigators to gather both CHRI and other types of personal information from disparate sources as part of an investigation, consumer report, background check, or similar inquiry.

Recommendation XII:

The Task Force recommends that where public policy considerations require amalgamation of information, systems be designed to recognize and administer differing standards (including dissemination policies and standards) based upon differing levels of data sensitivity, and allow the flexibility necessary to revise those standards to reflect future changes in public policy.

Commentary:

- Advances in information, identification, and communications technologies and related software pose challenges to existing criminal justice record privacy and information law and policy. At the same time, advances in these technologies create opportunities to use these technologies to improve the accuracy of criminal justice record information; improve the security of this information; and improve the ability of criminal record managers to distinguish among varying types of criminal justice information and manage this information with different policies for retention, use, and disclosure.
- The Task Force gave strong emphasis to the role that information, identification, and communications technologies play as a change driver and as a threat to traditional privacy protections.
- These technologies, however, can also be used to enhance and protect privacy. New technologies, including, in particular, new software technologies, are both robust and nimble and make it far easier, cheaper, and faster to apply different disclosure and other information policies to different types of criminal justice record information and other personal information, even when the information is maintained in the same database or system. These technologies make it much

easier than it once was, for example, to distinguish between conviction and nonconviction data or to combine juvenile justice information with adult criminal justice information, while retaining the ability to provide enhanced confidentiality protections for juvenile justice information.

Recommendation XIII:

The Task Force recommends that the integration of criminal justice information systems should be encouraged in recognition of the value of integrated systems in improving the utility, effectiveness, and cost efficiency of information systems. Prior to establishing integrated systems, however, privacy implications should be examined, and legal and policy protections in place, to ensure that future public- and private-sector uses of these information systems remain consistent with the purposes for which they were originally created. In addition, once an integrated system is created, any future uses or expansions of that system should be evaluated to assess the privacy implications.

Commentary:

- Privacy risks that arise from integration should be managed and minimized.
- Integration can serve a variety of socially beneficial purposes. Integration, for example, can help move accused offenders more quickly, efficiently, and cost-effectively through the criminal justice system, thereby reducing the amount of time the accused spends in jail awaiting trial and the amount of time victims must wait to have their day in court.
- Some types of integration — such as integrating criminal history record systems with intelligence and investigative systems, or with systems that contain medical, financial, or other very sensitive personal information — are especially privacy-sensitive and should be subject to appropriately strong privacy protections.

Recommendation XIV:

The Task Force recommends that new criminal justice privacy law and policy should continue to give weight to the distinction between conviction information and nonconviction information. The Task Force recognizes, however, that there are certain instances in which disclosure of nonconviction information may be appropriate.

Commentary:

- The distinction between conviction information and nonconviction information ("nonconviction information" is customarily defined to mean "an arrest which is over 1 year old without a disposition, as well as acquittals and other dispositions which do not involve a conviction"[280] has long been a cornerstone of criminal history record privacy policy. Conviction information is not only available to the criminal justice system, but is widely available to governmental, noncriminal justice agencies and to many types of employers and other noncriminal justice users. Nonconviction information, even in the late 1990s, remains largely unavailable to the general public (at least from State central repositories) and only partly available to private-sector employers and other users.
- Valid arguments exist for States to treat nonconviction information with more confidentiality and privacy protections than conviction information, given that nonconviction information carries a presumption of innocence; that its dissemination frustrates efforts to reintegrate arrestees into society; and that dissemination of nonconviction information exacerbates the

[280]See glossary of criminal justice information terms included as Appendix 2.

disproportionate impact that CHRI oftentimes has upon minorities.

- The fact that a State repository may not have a disposition within 1 year of arrest, which is the traditional standard, should not necessarily preclude the repository from disclosing any information. In such circumstances, the State repository should be able to point a requestor to the court in question so the requestor can inquire as to the disposition status. In responding to some inquiries, such as those made pursuant to the *National Child Protection Act*, the State is affirmatively required to track down dispositions.
- Examples of appropriate disclosure of nonconviction information most frequently cited by Task Force members involved sex offenses against young children and rape arrests where the victim failed to testify. Several Task Force members pointed out that parents would want to know that a prospective child-care worker had been arrested for child molestation, even if this individual was never convicted.
- Some Task Force members also noted that arrest information, regardless of disposition, is of historical and social interest and is a valuable government oversight tool. It was observed, for example, that information concerning the arrest of Dr. Martin Luther King, Jr., for loitering and an array of other offenses during the civil rights movement of the 1960s is a valuable record illustrating improper government action. Information concerning false arrests resulting not from malice, but from error or negligence also serves a valuable oversight function.

VII. Conclusion

This report and the Privacy Task Force's other efforts come at a critical juncture. Fundamental reassessments and changes regarding the rules for the handling of personal information are under way not only in the criminal justice information community, but also in many other information sectors, including medical information, financial information, the online collection of information, and public record information of various types.

Many of the same change drivers identified in this report (such as the Information Culture, new technology, new Business Models, and so on) have also impacted other information sectors and have fueled the reassessments and changes under way. There are differences, however, between the criminal justice sector and other sectors where reassessments are under way. These differences could have an impact on how change in the criminal justice information sector proceeds. First, as the public opinion survey data in the companion report indicate, the criminal justice system may benefit from a higher overall level of public trust than other sectors that use personal information. Second, the public safety value associated with access to, and disclosure of, criminal justice information is more frequently seen to outweigh other interests, including personal privacy, than is the case in other information sectors.

These differences between the collection and use of criminal justice information and other types of personal information do not mean that changes in the safeguards afforded to criminal justice information are unnecessary or that changes will not take place. These differences suggest, however, that any eventual changes will likely require a delicate and difficult-to-achieve balance to preserve the robust use of criminal justice information for socially beneficial purposes while finding ways to protect personal privacy.

The recommendations of the Task Force are a first step — but only a first step — in the development of a new generation of criminal justice information law and policy that achieves an important, nuanced balance between the use of criminal justice information and the privacy interests of those to whom the information pertains.

Appendix 1:

Task Force participants

Task Force participants

Chair

Robert R. Belair
Mullenholz, Brimsek & Belair; SEARCH General Counsel

Members

Kathy T. Albert
Global Network Coordinator, Global Justice Information Network,
U.S. Department of Justice

Dr. Ann Cavoukian
Commissioner, Office of Information and Privacy Commissioner, Ontario, Canada

Hon. Thomas M. Cecil
Judge, Sacramento Superior Court, California

Col. Timothy J. DaRosa
Deputy Director, Division of Administration, Illinois State Police

James X. Dempsey
Senior Staff Counsel, Center for Democracy and Technology

Dr. David H. Flaherty
Principal Officer, David H. Flaherty Inc., Privacy and Information Consultants

Dr. Charles M. Friel
Professor, College of Criminal Justice, Sam Houston State University, Texas

David Gavin
Assistant Chief of Administration, Crime Records Service,
Texas Department of Public Safety

Roger W. Ham
Chief Information Officer, Los Angeles Police Department, California

Ronald P. Hawley
Assistant Director, Division of Criminal Information,
North Carolina State Bureau of Investigation*

Hon. Catherine D. "Kitty" Kimball
Associate Justice, Supreme Court of Louisiana

Prof. Jane E. Kirtley
Silha Professor of Media Law and Ethics, School of Journalism and Mass Communications, University of Minnesota

Linda Lightfoot
Executive Editor, *The Advocate*

Anthony S. Lowe
Senior Legislative Counsel, Subcommittee on Antitrust, Business Rights, and Competition, U.S. Senate Judiciary Committee

Dr. Barry Mahoney
President, Justice Management Institute

Prof. Kent Markus
Visiting Professor, Capital University Law School, Ohio

Hon. Gordon A. Martin, Jr.
Associate Justice, District Court Department, Massachusetts Trial Court

Thomas R. McMahon
General Counsel, Illinois Department of Human Services

Iris Morgan
Senior Management Analyst II, Criminal Justice Information Services, Florida Department of Law Enforcement

Deirdre Mulligan
Staff Counsel, Center for Democracy and Technology

Ron Oldroyd
Assistant Juvenile Court Administrator, Utah

Lawrence F. Potts
Director, Administrative Group, Boy Scouts of America

Jack H. Reed
Chairman, I.R.S.C., Inc. and Confidential Business Resources, Inc;
Vice President, DBT Online, Inc.

Jack Scheidegger
Chief Executive Officer, Western Identification Network, Inc.

James F. Shea
Assistant Director of Systems, New York State Division of Criminal Justice Services

Harold M. "Hal" Sklar
Attorney-Advisor, Criminal Justice Information Services Division,
Federal Bureau of Investigation

Prof. George B. Trubow**
Director, Center for Information Technology and Privacy Law,
The John Marshall Law School, Illinois

Donna M. Uzzell
Director, Criminal Justice Information Services, Florida Department of Law Enforcement

William C. Vickrey
Administrative Director of the Courts, Administrative Office of the California Courts

Dr. Alan F. Westin
Professor Emeritus of Public Law and Government, Columbia University, New York

Dr. John Woulds
Director of Operations, Office of the Data Protection Registrar, United Kingdom

Bureau of Justice Statistics, U.S. Department of Justice

Dr. Jan M. Chaiken‡
Director

Carol G. Kaplan
Chief, Criminal History Improvement Programs

General Counsel's Office, Office of Justice Programs, U.S. Department of Justice

Anne Gardner
Attorney-Advisor

Paul F. Kendall
General Counsel

SEARCH, The National Consortium for Justice Information and Statistics

Sheila J. Barton
Deputy Executive Director
Law and Policy Division

Gary R. Cooper
Executive Director

Eric C. Johnson
Policy Research Analyst
Law and Policy Division

* Mr. Hawley is now Chief Information Officer, North Carolina Office of Information Technology Services
** Prof. Trubow has since retired
‡ Dr. Chaiken's tenure as BJS Director ended in January 2001

Participants' biographies

Robert R. Belair

Robert R. Belair is a partner with the Washington, D.C., law firm of Mullenholz, Brimsek & Belair and is General Counsel to SEARCH, The National Consortium for Justice Information and Statistics. He also serves as Chief Executive Officer of Privacy and Legislative Associates, a legal and policy consulting firm. The principal emphasis of Mr. Belair's practice is privacy and information law involving administrative, legislative, and litigation activity. His practice includes counseling in all aspects of privacy and information law, including credit, financial, educational, criminal, juvenile, medical, and employment records and telecommunications; defamation; intellectual property, including software copyright; constitutional law; and criminal justice administration.

As General Counsel to SEARCH, Mr. Belair has participated in SEARCH's privacy and security programs and has authored many studies in the area of criminal justice information law and policy. He was actively involved in the development of SEARCH's revised standards of criminal history record information, *Technical Report No. 13: Standards for the Security and Privacy of Criminal History Record Information* (Third Edition).

Mr. Belair has served as consultant to numerous Federal agencies and commissions on information policy and law. He is former Deputy General Counsel and Acting Counsel of the Domestic Council Committee on the Right of Privacy, Office of the President.

Mr. Belair is a graduate of Kalamazoo College (Michigan) and Columbia University School of Law.

Dr. Ann Cavoukian

In May 1997, Dr. Ann Cavoukian was appointed Information and Privacy Commissioner, Ontario, Canada. As Commissioner, Dr. Cavoukian oversees the operations of Ontario's freedom of information and protection of privacy laws, which apply to both provincial and municipal government organizations. She serves as an officer of the legislature, independent of the government of the day.

Dr. Cavoukian joined the Information and Privacy Commission in 1987, during its start-up phase, as its first Director of Compliance. She was appointed Assistant Commissioner in 1990. Prior to her work at the Commission, Dr. Cavoukian headed the Research Services Branch of the Ministry of the Attorney General, where she was responsible for conducting research on the administration of civil and criminal law.

Dr. Cavoukian speaks extensively on the importance of privacy around the world. Her published works include a book on privacy titled *Who Knows: Safeguarding Your Privacy in a Networked World* (McGraw-Hill, 1997).

Dr. Cavoukian received her M.A. and Ph.D. in psychology from the University of Toronto. She specialized in criminology and lectured on psychology and the criminal justice system.

Hon. Thomas M. Cecil

Judge Thomas M. Cecil has served on the Sacramento (California) Superior and Municipal Courts since March 1989. During his tenure on the bench, he has presided over each of the criminal departments in both the municipal and superior courts. For the past 4 years, Judge Cecil has conducted felony trials, the vast majority of which involved murders.

For the 6 years prior to his appointment to the bench, Judge Cecil served as Chief Counsel and Deputy Director of the California Department of Consumer Affairs. His responsibilities included lobbying the California Legislature on issues impacting consumers, press relations, consumer education, and overseeing the legal staff of the Department. As an attorney, Judge Cecil practiced in a variety of areas, including

bankruptcy, corporate law, family law, political law, and general business litigation. He also served as Special Counsel to the Joint Select Committee on Municipal Liability Insurance with the California Legislature.

Judge Cecil previously served as a member and Chair of the Pacific Bell Telecommunications Consumer Advisory Panel (1988-91). He is now a member and current Chair of the California Judicial Council's Advisory Committee on Court Technology.

Col. Timothy J. DaRosa

Col. Timothy J. DaRosa is a 22-year veteran of the Illinois State Police. In March 1991, he was appointed Deputy Director of the Division of Administration. He is responsible for an annual budget in excess of $35 million and over 750 employees who serve in the Bureaus of Communications, Criminal Identification, Personnel, Information Services, and Logistics, and the Crime Studies Section.

In his capacity as Deputy Director, Col. DaRosa is responsible for the administration of the Department's Automated Fingerprint Identification System (AFIS), voice and data communications systems, and the Illinois State Police data center that includes the Law Enforcement Agency Data System (LEADS). Col. DaRosa also oversees the operation of the Firearm Owners Identification (FOID) Program and serves as the Illinois point-of-contact for firearms transactions relative to the National Instant Criminal Background Check System (NICS).

Col. DaRosa currently serves as Chairman of the Illinois LEADS Advisory Policy Board and is a member of the Federal Brady Act Task Force Working Group, and the International Association of Chiefs of Police (IACP) Criminal Justice Information Systems Committee. Col. DaRosa's professional affiliations include the National Criminal Justice Association, the Police Executive Research Forum, the Illinois Association of Chiefs of Police, and the IACP. In November 1998, he was appointed by Illinois' governor to serve on the SEARCH Membership Group.

Col. DaRosa holds a B.S. degree in criminal justice administration from Southern Illinois University at Carbondale, and is a veteran of the U.S. Army.

James X. Dempsey

James X. Dempsey is Senior Staff Counsel at the Center for Democracy and Technology (CDT) in Washington, D.C. He joined CDT in 1997, where he works on fourth amendment and electronic surveillance issues. Prior to joining CDT, Mr. Dempsey was Deputy Director of the Center for National Security Studies. From 1995-96, Mr. Dempsey also served as Special Counsel to the National Security Archive, a nongovernmental organization that uses the *Freedom of Information Act* to gain the declassification of documents on U.S. foreign policy.

From 1985-94, Mr. Dempsey was Assistant Counsel to the House Judiciary Subcommittee on Civil and Constitutional Rights. His primary areas of responsibility for the Subcommittee were oversight of the Federal Bureau of Investigation (FBI), privacy, and civil liberties. He worked on issues at the intersection of national security and constitutional rights, including terrorism, counterintelligence, and electronic surveillance, as well as crime issues, including the Federal death penalty, remedies for racial bias in death sentencing, information privacy, and police brutality. Mr. Dempsey has traveled to Russia, Poland, Hungary, Bulgaria, Guatemala, Chile, and Argentina to speak on civil liberties issues.

From 1980-84, Mr. Dempsey was an Associate with the Washington, D.C., law firm of Arnold & Porter, where he practiced in areas of government and commercial contracts, energy law, and anti-trust. He also maintained an extensive *pro bono* representation of death row inmates in Federal habeas proceedings. He clerked for the Hon. Robert Braucher of the Massachusetts Supreme Court.

Mr. Dempsey graduated from Harvard Law School in 1979 and from Yale College in 1975. He is co-author of *Terrorism & the Constitution: Sacrificing Civil Liberties in the Name of National Security* (with Prof. Davie Cole of Georgetown Law School).

Dr. David H. Flaherty

Dr. David H. Flaherty is Principal Officer of David H. Flaherty, Inc., Privacy and Information Consultants, in Victoria, British Columbia, Canada. He became British Columbia's first Information and Privacy Commissioner in 1993. Appointed by the government of British Columbia, Dr. Flaherty had a 6-year, nonrenewable term of office. In this position, he was an independent Officer of the Legislature of British Columbia, and his role was to independently monitor the administration of British Columbia's *Freedom of Information and Protection of Privacy Act*.

Dr. Flaherty has over 20 years of experience with privacy protection and access to information issues as an academic, a teacher, an advisor, a consultant, and an advocate. He is recognized as one of the world's leading experts on privacy and data protection.

Since 1965, Dr. Flaherty has been a full-time academic in the United States and Canada. He received a B.A. (honors) degree in history from McGill University in 1962, and an M.A. and Ph.D. in history from Columbia University in 1963 and 1967, respectively. He taught at Princeton University from 1965-68 and the University of Virginia from 1968-72. In 1972, Dr. Flaherty joined the faculty at the University of Western Ontario, where he taught history and law until accepting the position of Commissioner. His research and teaching fields include American and Canadian legal history, information law and policy, and privacy and data protection in modern industrial societies.

From 1971-72, Dr. Flaherty was a Fellow in law and history at Harvard Law School; a Visiting Fellow at Magdalen College, Oxford, in 1978-79; a Visiting Scholar at Stanford Law School in 1985-86; a Fellow of the Woodrow Wilson International Centre for Scholars in Washington, D.C., during the 1992-93 academic year; a Canada-U.S. Fulbright Fellow (Law); a Visiting Scholar at the Georgetown National Law Center; and a Fellow of the Kennedy Institute for Ethics, at Georgetown University. From 1985-87, Dr. Flaherty served as a Consultant to the Standing Committee on Justice and Solicitor General of the Canadian House of Commons for its report on the functioning of Federal access to information and privacy acts.

Dr. Flaherty has written and published four books and edited two international bibliographies on privacy and data protection policy. His major book, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (1989), examines how privacy and data protection laws for the public sector work in practice. In addition, he also has been an editor and co-editor of six publications relating to various aspects of Canadian and American studies, including *Challenging Times: The Women's Movement in Canada and the United States* (1992). Several of Dr. Flaherty's current writings emanate from his role as Information and Privacy Commissioner, and discuss the principles and practical application of information and privacy law in British Columbia.

Dr. Charles M. Friel

Dr. Charles M. Friel is a Professor in the College of Criminal Justice, Sam Houston State University (Texas), where he previously served as Dean.

In 1978 and again in 1984, Dr. Friel received fellowships from the Japanese Ministry of Justice to study that nation's correctional system. In 1988, he served as a visiting lecturer in various police colleges in the People's Republic of China.

Dr. Friel has lectured extensively throughout the United States and Canada. He is an At-large Member of SEARCH, as well as a member of its Board of Directors. He was the 1988 recipient of

SEARCH's *O.J. Hawkins Award for Innovative Leadership and Outstanding Contributions in Criminal Justice Information Systems, Policy and Statistics in the United States*. Dr. Friel is also the 1992 recipient of the *Justice Charles W. Barrow Award* for distinguished service to the Texas judiciary.

Dr. Friel's undergraduate studies at Maryknoll College (New York) included philosophy and Latin; he received a Ph.D. in experimental psychology from the Catholic University of America, Washington, D.C.

David Gavin

David Gavin has worked for the Texas Department of Public Safety for 21 years. Since 1991, Mr. Gavin has served as Assistant Chief of the Department's Administration Division. He held prior positions with the Texas Crime Information Center, the Texas Uniform Crime Reporting Program, the Texas Computerized Criminal History File, and the Texas Automated Fingerprint Identification System. Mr. Gavin's current duties include responsibilities for all those programs.

Within the FBI's Criminal Justice Information Services (CJIS) advisory process, he has served as Chair of the Western Regional Working Group and the National Crime Information Center Subcommittee. He currently is Chair of the FBI CJIS Advisory Policy Board. His education includes a master's degree from the University of Texas, Austin.

Roger W. Ham

Roger W. Ham is the first Chief Information Officer (CIO) of the Los Angeles (California) Police Department (LAPD). He serves the Department at the level of Deputy Chief and commands five divisions, including Emergency Command and Control Communications Systems, Communications, Information Resources, Crime Analysis Section, and the Systems Development Task Force. Chief Ham manages a professional and operational staff of over 900, including sworn commanding officers and civilian managers. As Commanding Officer, he is responsible for the conduct of operations and the efficient utilization of the financial and human resources in the Information and Communications Services Bureau. Chief Ham directs and manages an annual technology project budget of over $400 million.

As CIO, Chief Ham is developing information systems divisions, which are centers of competency with speed, maneuverability, responsiveness, flexibility, and accountability. He has a focused synergistic approach so that all units under his command work together toward the shared vision and goals of the LAPD.

Chief Ham has over 28 years of experience in developing leading-edge technologies. He started his career working for Mobil Oil Corporation as a project engineer managing command and control of field operations through automated systems. He was the Bureau Commander, Communications Administrator, and Information Systems Manager for the City of Huntington Beach Police Department in California for over 21 years.

Chief Ham has an M.B.A. from the University of Southern California and a bachelor's degree in electrical engineering from California State University, Long Beach. He has served on many professional and business organizations.

Ronald P. Hawley

Ronald P. Hawley began his career with the North Carolina State Bureau of Investigation (SBI) in August 1973. Since January 2001, he has served as CIO of the North Carolina Office of Information Technology Services. Previous to that, he served as Assistant Director for the SBI's Division of Criminal Information, a position he had held since July 1993. Mr. Hawley's early assignments with the SBI included Special Agent, Assistant District Supervisor, District Supervisor, and a tour of duty with Governor's Security.

Subsequent to his appointment to the Division, Mr. Hawley became involved with several committees and working groups related to criminal justice

information technology. These include Co-chair of the Criminal Justice Information Network Study Committee, member of the Criminal Justice Information Services (CJIS) Southern Regional Working Group, and member of the CJIS Ad Hoc Task Force on Security, Privacy and Policy Matters. Mr. Hawley is an At-Large appointee to the SEARCH Membership Group. He previously was the governor-appointed member of SEARCH representing North Carolina, and served on the SEARCH Board of Directors and as Vice Chair of the SEARCH Law and Policy Program Advisory Committee.

Mr. Hawley is a graduate of Campbell College and received a master's degree in education from the University of Maine.

Hon. Catherine D. "Kitty" Kimball

The Honorable Catherine D. "Kitty" Kimball serves as Associate Justice of the Louisiana Supreme Court. Her previous work experience included Law Clerk, U.S. District Court, Western District of Louisiana; Special Counsel, Louisiana Attorney General's Office; General Counsel, Louisiana Commission on Law Enforcement and Administration of Criminal Justice; private solo practice; and Assistant District Attorney for the 18th Judicial District.

In December 1982, Justice Kimball was elected District Judge, Division A, for the 18th Judicial District. She served in that capacity until being elected as Associate Justice of the Supreme Court of Louisiana in November 1992.

Justice Kimball's current professional responsibilities and associations include: Member, Louisiana State Bar Association; Member, American Judicature Society; Member, National Association of Women Judges; Member, State-Federal Judicial Council; Member, Wex Malone American Inn of Court; Charter Member, Louisiana Association of Elected Women; Chair, Louisiana Supreme Court Case Management Information System Task Force; Member, Governor's Task Force on Violent Crime and Homicide; Member, Automated Fingerprint Identification Selection Committee; and Chair, Judicial Budgetary Control Board.

Justice Kimball has previously served as Past President, Louisiana Legislative Wives Auxiliary; First Vice-President and Member, Executive Committee of the Louisiana District Judges Association; President and Member, Louisiana State University Law Alumni Association; Member, Louisiana Juvenile Judges Association; Member, National Conference of State Trial Judges; Member, 18th Judicial District Bar Association; Member, American Trial Lawyers Association; Chief Judge, 18th Judicial District Court; Member, Governor's Commission on Child Support; Member, Economic Justice for All Task Force; Member, Committee to Evaluate New Judgeships; Member, Orleans Criminal and Civil Court Committee; Member, Supreme Court Committee on the Judicial Electoral Process; Member, Louisiana Task Force on Women in the Courts. She also has been inducted into the Louisiana State University Law School Hall of Fame.

Prof. Jane E. Kirtley

Jane E. Kirtley is the Silha Professor of Media Law and Ethics at the School of Journalism and Mass Communication, University of Minnesota. Prior to assuming her position at the University of Minnesota in August 1999, Prof. Kirtley served as Executive Director of The Reporters Committee for Freedom of the Press, a voluntary unincorporated association of reporters and editors devoted to protecting the first amendment and freedom of information interests of the news media. In that position, she was responsible for overseeing the legal defense and publications efforts of the Reporters Committee, as well as supervising the group's fundraising activities. Prof. Kirtley also edited the Committee's quarterly magazine, *The News Media & The Law*.

Prof. Kirtley has prepared numerous friend-of-the-court briefs on behalf of the Reporters Committee and other news media organizations, including *Reno* v. *ACLU, Hustler Magazine* v. *Falwell, The*

Florida Star v. *B.J.F.*, and *Department of Justice* v. *Tax Analysts.* She frequently writes and speaks on media law and freedom of information issues in the United States and abroad, including Russia, Mongolia, Belarus, Bulgaria, Latvia, Romania, Poland, the Czech Republic, Japan, Chile, the United Kingdom, Ireland, and Canada. Prof. Kirtley also writes "The Press and the Law" column each month for *American Journalism Review*, and has appeared on programs such as "Nightline," "All Things Considered," "The Jim Lehrer News Hour," "Good Morning America," "Today," "Donahue!," "Crossfire," "Burden of Proof," "CNN & Co.," and the British Broadcasting Corp.'s "Law in Action." She also has served as an Adjunct Professor with the American University School of Communications Graduate Program.

Prior to her tenure at the Reporters Committee, Prof. Kirtley was associated with the law firm of Nixon, Hargrave, Devans & Doyle. She is a member of the New York, District of Columbia, and Virginia bars. Prof. Kirtley worked as a reporter of the *Evansville Press*, the *Oak Ridger*, and the *Nashville Banner*.

She serves on many advisory boards and committees, including the Freedom Forum's First Amendment Center, the American Bar Association's (ABA) National Conference of Lawyers and Representatives of the Media, the Libel Defense Resource, the Student Press Law Center, and the editorial board of *Government Information Quarterly.* In 1993, Prof. Kirtley received the Distinguished Service Award from the Newspaper Division of the Association for Education in Journalism and Mass Communication, and in 1994, the John Peter Zenger Award for Freedom of the Press and the People's Right to Know from the University of Arizona. In 1996, she was one of 24 individuals inducted into the *Freedom of Information Act* Hall of Fame, established to commemorate the 30th anniversary of the signing of the Act.

Prof. Kirtley obtained her J.D. degree in 1979 from Vanderbilt University School of Law, where she served as Executive Articles Editor of the Vanderbilt *Journal of Transnational Law.* She received bachelor's and master's degrees from Northwestern University's Medill School of Journalism in 1975 and 1976.

Linda Lightfoot

Linda Lightfoot is Executive Editor of *The Advocate* in Baton Rouge, Louisiana. Ms. Lightfoot has been employed by Capital City Press, the publisher of *The Advocate*, since 1965. She started as a "society" writer, and has been a Reporter in the areas of courts and education; headed the Capitol News Bureau, covering State government and higher education; and was Assistant Executive Editor prior to her present appointment as Executive Editor in 1991.

Ms. Lightfoot has and continues to be involved in many professional and community activities, including the American Society of Newspaper Editors (ASNE), currently serving on its Board of Directors; as a member of the Freedom of Information Committee; and as representative of ASNE on the National Conference of Lawyers and Representatives of the News Media, which is a committee of the ABA. She has also served as a Nominating Juror for the Pulitzer Prize for 1997 and 1998. She currently is on the Visiting Committee for the School of Communications, Loyola University; a member of the Society of Professional Journalists; a member of the Board of Directors of the Press Club of Baton Rouge; a member of the Louisiana Press Association's Legislative Committee; and a member of the Louisiana Leadership Alumni, a program of the Council for a Better Louisiana.

In 1993-94, Ms. Lightfoot served on the Task Force to Study Cameras in the Trial Courts of Louisiana. She was appointed by the Supreme Court of Louisiana to represent newspapers on the Task Force and authored the majority of the report in favor of cameras.

Ms. Lightfoot received a bachelor's degree in political

science and journalism from the University of Mississippi, and has studied at the Institute of Politics, Loyola University, and the Louisiana State University Executive Program.

Anthony S. Lowe

Anthony S. Lowe is Senior Legislative Counsel to the U.S. Senate Judiciary Committee's Subcommittee on Antitrust, Business Rights, and Competition, a position he has held since 1997. He is responsible for the development and introduction of crime-related legislation and handles all crime-related issues before the full committee for the subcommittee chair.

Mr. Lowe's prior experience includes Legislative Assistant to U.S. Sen. Slade Gorton (R-WA) from 1988-90, during which time he was assigned to the these committees: Judiciary; Rules; Commerce, State, Justice Appropriations; Government Affairs; Impeachment Trial; and Indian Affairs. He also served as Legal Counsel to the Washington State Senate, Majority Office of Legal Counsel and Policy Development from 1991-92; as Deputy Prosecutor in the King County, Washington, Prosecutor's Office; as Judicial Extern for the U.S. Court of Appeals for the Ninth Circuit, Judge Robert R. Beezer; as Associate Director, International Center for Economic Growth and International Center for Self-Governance Programs of the Institute for Contemporary Studies, Washington, D.C.; and as Senior Trade Intern, International Trade Administration, Foreign and Commercial Service, U.S. Department of Commerce.

Mr. Lowe received his B.A. (*cum laude*) degree in international political science from the University of Washington and his J.D. from the University of Santa Clara (California). He also studied at the National University of Singapore Law School and the East China Institute of Politics and Law. He is a member of the Bars of Pennsylvania, Washington State, U.S. Court of Appeals for the Ninth Circuit, U.S. Court of International Trade, U.S. District Court for the Western District of Washington, and Washington, D.C.

Dr. Barry Mahoney

Since 1993, Dr. Barry Mahoney has been President of The Justice Management Institute (JMI), a Denver-based, nonprofit organization engaged in education, research, and technical assistance focused on the operations of courts and other organizations involved in the administration of justice. He is responsible for overall management and program development for JMI, and during 1998-99 he directed JMI projects on reduction of litigation cost and delay, drug court planning and implementation, and court-linked community justice innovations.

Dr. Mahoney's prior professional work includes extensive experience in litigation as an Assistant Attorney General for the State of New York in 1962-67, and as a lawyer in private practice in New York City in 1967-71. During 1971-73, he was First Assistant Counsel for the New York State Division of Criminal Justice Services. From 1973-78, he was with the National Center for State Courts (NCSC), where he was the Associate Director responsible for all of the organization's national-scope research and technical assistance programs. In 1978-79 and 1982-83, Dr. Mahoney was the Director of the London Office of the Vera Institute of Justice. During 1979-82 and 1983-92, he was with the NCSC's Institute for Court Management, where he led a number of national-scope research and technical assistance projects focused on court delay reduction, intermediate sanctions, and fine use and collection.

Dr. Mahoney has served as a lead faculty member for educational programs conducted by the National Judicial College, the National Association for Court Management, and many other national-, State-, and local-level organizations. Dr. Mahoney served as a member of the Advisory Panel for the Assessment of Alternatives for a National Computerized Criminal History System conducted by the Office of Technology Assessment of the

U.S. Congress in 1979-82, and since 1997 has been a member of the SEARCH/Bureau of Justice Assistance National Task Force on Court Automation and Integration.

Dr. Mahoney is a graduate of Dartmouth College and the Harvard Law School, and holds a Ph.D. in political science from Columbia University.

Prof. Kent Markus

Kent Markus is a visiting Professor at Capital University Law School in Columbus, Ohio, and Director of Capital's new Dave Thomas Center for Adoption Law, the first law school-based institution focused on adoption law in the United States.

Before heading to Capital in the fall of 1998, Prof. Markus served as the Deputy Chief of Staff at the U.S. Department of Justice (DOJ) and as the highest-ranking advisor — Counselor — to Attorney General Janet Reno. During his approximately 5 years at the DOJ, Prof. Markus, at various points in time, was responsible for the national implementation of the *Brady Handgun Violence Prevention Act* and the *1994 Crime Act*; established and was the first director of the Community Oriented Policing Services (COPS) Office (responsible for putting 100,000 new community policing officers on America's streets); managed the DOJ's dealings with the Congress; and was the DOJ's point person on crime policy in general, with special attention to juvenile crime, gun violence, and criminal record systems.

Prior to his service at the DOJ, Prof. Markus was the Chief of Staff at the Democratic National Committee. He also previously served as Chief of Staff for former Ohio Attorney General Lee Fisher. Earlier in his career, Prof. Markus, a Cleveland native, worked at law firms in Australia, Alaska, and Washington, D.C., before heading back home to clerk for U.S. District Judge Alvin I. "Buddy" Krenzer, practice law, and teach at Cleveland State Law School. On Capitol Hill, Prof. Markus worked for former U.S. House Speakers Carl Albert and Thomas P. "Tip" O'Neill, and former House Rules Committee Chairman Richard Bolling.

Prof. Markus teaches Administrative Law, Remedies, and a seminar on the Role of the Prosecutor at Capital University. He is a 1981 graduate of Northwestern University's School of Speech, a 1984 honors graduate of Harvard Law School, and a graduate of the Kennedy School's Program for Senior Executives in State and Local Government.

Hon. Gordon A. Martin, Jr.

Judge Gordon A. Martin, Jr., was appointed to the Massachusetts Trial Court in 1983. He headed one of the country's frontline urban district courts with the most gun, drug, and domestic violence cases in the State, and now operates a special assignment session for cases from various Eastern Massachusetts courts.
Judge Martin was a Trial Attorney with the Civil Rights Division of the U.S. DOJ during the Kennedy Administration and thereafter First Assistant U.S. Attorney for the District of Massachusetts. He was subsequently a Commissioner of the Massachusetts Commission Against Discrimination before organizing the firm in which he was a partner until becoming a judge.

In 1994, he was honored by New England's largest program for battered women, Casa Myrna Vasquez, for his work on behalf of abused women. That same year, Judge Martin was designated one of the three initial U.S. House of Representatives "practitioner" appointees to the Federal Coordinating Council on Juvenile Justice and Delinquency Prevention, chaired by Attorney General Janet Reno. In that capacity, he participated in the preparation of *Combating Violence and Delinquency: The National Juvenile Justice Action Plan.* He was re-appointed to the Council in 1998. Judge Martin also is completing his second term as a trustee of the National Council of Juvenile and Family Court Judges. He spoke at the SEARCH/Bureau of Justice Statistics National Conference on Juvenile Justice Records in 1996.

Judge Martin co-authored *Civil Rights Litigation: Cases and Perspectives* (Carolina Press 1995), and has written law review articles on a wide range of topics, including juvenile justice articles in the *Connecticut Law Review* and the *New England Journal on Criminal and Civil Confinement.*

Judge Martin is a graduate of Harvard College and the New York University School of Law.

Thomas R. McMahon

Thomas R. McMahon is General Counsel of the Illinois Department of Human Services. The Department is comprised of the former Departments of Mental Health and Developmental Disabilities; Alcohol and Substance Abuse; Rehabilitation Services; and portions of the Departments of Public Aid, Public Health, and Children and Family Services. He administers the Division of Legal Services and provides counsel to the Department on a wide range of administrative, policy, and regulatory matters.

Prior to his employment with the Department, Mr. McMahon was associated with the firm of Cappetta & Shadle, Ltd., and served as an Assistant States Attorney in Lake County, Illinois. Before entering the legal profession, Mr. McMahon was employed by the Ray Graham Association for the Handicapped in various capacities, including the administration of sheltered workshop programming for individuals with developmental disabilities.

Mr. McMahon received his undergraduate degree from the University of Illinois and his J.D. from The John Marshall Law School. Mr. McMahon is an adjunct faculty member at DePaul University School of Law (Illinois).

Iris Morgan

Iris Morgan is a Senior Management Analyst II for the Criminal Justice Information Services (CJIS) Program in the Florida Department of Law Enforcement (FDLE). She is currently serving as the coordinator for delivery of information services statewide, supervisor of the CJIS Help Desk, and project leader for the development and installation of the Florida Crime Information Center (FCIC) II Workstation Software Project. Prior to assuming that role, she was responsible for conducting FCIC/National Crime Information System (NCIC) audits of criminal justice agencies accessing the FCIC/NCIC systems.

Ms. Morgan has over 19 years experience with FDLE and the CJIS Program Area. During this time she has served in a variety of technical, analytical, and supervisory positions. She has also been instrumental in designing several major criminal justice information system enhancements, including: the Offender-Based Transaction System, Uniform Offense and Arrest Reports, National Fingerprint File Program, Uniform Crime Reports Program, and Criminal Justice Data Element Dictionary, as well as redesign of the Computerized Criminal History file.

Deirdre Mulligan

Deirdre Mulligan is Staff Counsel at the Center for Democracy and Technology, a public interest organization based in Washington, D.C., dedicated to preserving and enhancing democratic values and civil liberties on the Internet and other interactive communications media. As Staff Counsel, Ms. Mulligan evaluates the impact of technology on individual privacy. She works with other privacy and civil liberties advocates, the communications and computer industries, and public policy makers to strengthen fair information practices and enhance individual control over personal information through the development of individual empowering policies and technologies. Currently Ms. Mulligan is shepherding the Internet Privacy Working Group — a collaborative public interest/private-sector working group — developing a framework for privacy on the Internet.

Prior to joining the Center, Ms. Mulligan worked on information privacy issues in emerging technologies at the Electronic Frontier Foundation (EFF). While at EFF, Ms. Mulligan staffed the National

Information Infrastructure Advisory Council's Megaproject III on Privacy, Security and Intellectual Property for Co-chair Ester Dyson.

Ms. Mulligan received her undergraduate degree from Smith College. She received her law degree from Georgetown University.

Ron Oldroyd

Ron Oldroyd is the Assistant Juvenile Court Administrator for Utah. He began his career with the Juvenile Court in 1973 as a Deputy Probation Officer. Since then he has held a number of positions within the Juvenile Court. He received his B.S. and M.S. degrees from the University of Utah. After receiving his M.S. degree in School Counseling, he left the court to work as an elementary school counselor for 4 years prior to returning to the court as the Chief of Probation in Salt Lake City.

During his tenure with the courts, Mr. Oldroyd has been very involved with programming for delinquent youth and Utah's Juvenile Justice Management Information System. He is currently chairing the re-engineering of this system, an effort that is expected to take 3 years. Mr. Oldroyd was also a participant in an initiative of the U.S. DOJ's Office of Juvenile Justice and Delinquency Prevention to define juvenile probation and its expectations on a national level.

Lawrence F. Potts

Lawrence F. Potts has served as Treasury Division Director and currently as Director of the Administrative Group of the Boy Scouts of America. In his present position, he directs Information Systems, Properties, and Treasury.

Mr. Potts has served with the National Council of the Boy Scouts since 1982, and in his current position since 1992. Prior to joining the National Council, he had extensive experience in the causality insurance industry, holding positions of controller and treasurer and serving as a member of several boards of directors. He also served with the U.S. Armed Forces with the rank of Captain.

Mr. Potts was an original member of the Boy Scouts of America Youth Protection Task Force. In this capacity, he was instrumental in creating several tools for the prevention of child abuse in society and Scouting.

He also was an original member of the National Collaboration for Youth Sexual Abuse Task Force. This is an association of 16 not-for-profit youth-serving organizations interested in the prevention of child sexual abuse. This group pioneered efforts in information-sharing and education about sexual abuse among youth-serving agencies. Mr. Potts is the author of a paper on a model program's efforts in the child abuse area.

Through the Boy Scouts of America, Mr. Potts is able to communicate with more than 4.4 million youth and 1.1 million adults of mixed ethnic and racial backgrounds, and many others throughout society. Currently, he holds the positions of Chairman, Boy Scouts of America Youth Protection Task Force; Chairman, Child Abuse Expert Advisory Panel; Chairman, National Collaboration for Youth Child Sexual Abuse Task Force; and Member, National Child Abuse Coalition. He was a member of the U.S. Advisory Board on Child Abuse and Neglect from 1992-96.

Mr. Potts is a Certified Public Accountant and, as such, a member of the American and Texas Institutes of CPAs. He also is a member of the Association of Investment Analysts, the Southwest Pension Conference, and the Sentinel Institute.

Mr. Potts is a graduate of the University of Texas, Austin, and is a member of Beta Alpha Psi and Phi Kappa Phi organizations.

Jack H. Reed

Jack H. Reed is Chairman of I.R.S.C., Inc., an information provider company, and Confidential Business Resources, Inc., a corporation recently formed by the merger of nine companies representing all facets of the information industry.

Mr. Reed began his career in the personal finance business, where he spent 9 years, serving in various management positions. He has been a licensed Private Investigator since 1964, at which time he founded J.H.R.I., Inc., a private investigation firm. Mr. Reed founded I.R.S.C., Inc., in 1979 and began selling public record and nonpublic information to private investigators, corporations, insurance companies, and financial institutions in 1983.

Mr. Reed entered Western State University, College of Law in 1966. His graduation was delayed until 1972 due to a serious injury that left him quadriplegic. During his recovery period, J.H.R.I. continued to grow with Mr. Reed at the helm.

As a member of the California Association of Licensed Investigators, Mr. Reed has served as President, and on the Board of Directors as Vice President of Investigations, District Director, and Director at Large. He served on the Legislative Committee for over 20 years and re-engineered this committee into a formidable entity, which, since its inception, has prevented any negative legislation affecting the private investigation and security industry.

Mr. Reed was President of the National Council of Investigation and Security Services (NCISS), as well as its Legislative Committee Chair, which involved overseeing Federal legislation issues in 1997-98. He is an active member of various other State, national, and international professional associations, and serves on various committees within these organizations.

Mr. Reed has been appointed by the Software/Information Industry Association (SIIA) Board of Directors to serve on the Executive Committee of the Public Policy and Government Relations Council. He also serves on the SIIA Committee on Privacy and Information Regulation and chairs the State Issues Working Group and Government Information Policy Committee. Additionally, Mr. Reed served on the privacy task force spearheaded by California State Sen. Steve Peace of California (D-El Cajon).

In June 1997, Mr. Reed was invited to attend the Federal Trade Commission (FTC) hearings, representing NCISS and the Individual Reference Services Group (IRSG). Mr. Reed is also a founding member of the IRSG, which is based in Washington, D.C., and is comprised of representatives from leading companies within the information industry who are addressing privacy concerns. Mr. Reed was recently elected Vice Chair and Secretary-Treasurer of the IRSG. This group has compiled "Privacy Principles," which are intended to serve as the industry model for ethical and privacy standards. These Principles were approved by the FTC, and resulted in a recommendation from the FTC in its "Report to Congress" that no new legislation was needed to regulate the information industry.

Jack Scheidegger

Jack Scheidegger is Chief Executive Officer of the Western Identification Network, Inc., a position he has held since 1996. Prior to his current appointment, Mr. Scheidegger was Chief of the Bureau of Criminal Identification and Information in the California DOJ.

He also has previously held the positions of Chief, Bureau of Forensic Services, California DOJ; Director, Bureau of Medi-Cal Fraud and Patient Abuse, California DOJ; and Legislative Advocate for the California Attorney General's Office.

Mr. Scheidegger previously served as California's governor-appointed Member to the SEARCH Membership Group. As a SEARCH Member, he served on its Board of Directors, as Chair of its Law and Policy Program Advisory Committee, and as Chair of the Bureau of Justice Statistics/SEARCH National Task Force on Increasing the Utility of the Criminal History Record. He also has been a member of the California Peace Officers Association, American Society of Crime Laboratory Directors, and the FBI/NCIC Western Regional Working Group (Control Terminal Officer).

Mr. Scheidegger received his B.A. degree in public administration from California State University at Sacramento, and his master's degree in public administration from the University of Southern California.

James F. Shea

James F. Shea is Assistant Director of Systems at the New York State Division of Criminal Justice Services. In this position, he manages a broad range of projects, including the State Automated Fingerprint Identification System, Store and Forward, and the development and support of systems developed for local agencies, including law enforcement, prosecution, jails, and probation.

Mr. Shea manages the State's federally funded National Criminal History Improvement Program and Criminal Justice Records Improvement Program, as well as automation projects supported by the National Institute of Justice and the Office of Juvenile Justice and Delinquency Prevention, U.S. DOJ. He heads up the State criminal justice data standardization project, serves on the Executive Board that oversees data standardization for all State departments, and directs a statewide initiative to re-examine record sealing and information dissemination. Mr. Shea previously served on the Governor's Task Force to improve information systems in New York State.

Mr. Shea holds a B.S. degree from Holy Cross College, an M.B.A. from Union College, and has participated in Executive Training Programs at Harvard's Kennedy School of Government.

Harold M. "Hal" Sklar

Harold M. "Hal" Sklar is an Attorney-Advisor to the Criminal Justice Information Services Division of the FBI, having been appointed to that position in September 1997. He received his J.D. and L.L.M. from the Temple University School of Law (Pennsylvania) and the Georgetown University Law Center, respectively. Half of his 16 years of practice has been in government service, most notably as a Trial Attorney pursuing *Employee Retirement Income Security Act* (ERISA) fraud for the U.S. Department of Labor, abusive tax shelter promotion for the U.S. DOJ, and savings and loan defalcation (Resolution Trust Corporation).

Prof. George B. Trubow

From 1976 until his retirement in 2001, Prof. George B. Trubow was a Professor of Law at The John Marshall Law School in Chicago, Illinois, where he taught Information Law and Policy, Cyberspace Law, Privacy Law, and Computer Law and directed the Center for Information Technology and Privacy Law.

Prof. Trubow practiced law in Kansas and Missouri from 1958-61, and in 1961 became assistant at The John Marshall Law School. In 1965, he was awarded a Congressional Fellowship with the American Political Science Association in Washington, D.C. From 1966-68, Prof. Trubow was Deputy Counsel to the U.S. Senate Judiciary Subcommittee on Judicial Machinery. In 1968, he became Executive Director of the Maryland Governor's Commission on the Administration of Justice, and he served on the U.S. Attorney General's Advisory Council on Law Enforcement Education from 1968-70.

In 1970, Prof. Trubow joined the Law Enforcement Assistance Administration (LEAA), U.S. DOJ, where he served as Deputy Director of Law Enforcement Programs and Director of Inspection and Review, in charge of grant programs to the States and planning and program development for LEAA.

In 1974, Prof. Trubow became General Counsel to the Committee on the Right to Privacy, Executive Office of the President, during the Ford Administration. The Committee was concerned with the analysis and development of Federal information and privacy law and policy. Prof. Trubow returned to John Marshall in 1976.

Prof. Trubow is active in the ABA Section of Science and Technology; he was advisor to the National Commission on Uniform State Laws in drafting the Uniform State Information Practices Code; and was Reporter for the *Uniform*

Criminal History Records Act. He was Chair of the 1994 International Conference on Computers, Freedom and Privacy and was a longtime member of the Board of Directors of SEARCH. He has been an advisor to the Office of Technology Assessment of the U.S. Congress and to the National Research Council in Fraud Institute, and a member of the Federal Computer Systems Security and Privacy Advisory Board.

Prof. Trubow has written and spoken widely on the law of information technology, "cyberspace," and privacy. He was law editor of IEEE's *Software* magazine, and his Center for Information Technology and Privacy Law publishes a quarterly law review, *The Journal of Computer and Information Law*. He is editor-in-chief of the three-volume treatise, *Privacy Law and Practice* (1987), and co-author of the casebook, *Privacy Law* (1992).

Prof. Trubow is a graduate of the University of Michigan, earning both bachelor's and law degrees.

Donna M. Uzzell

Donna M. Uzzell was appointed Director of Criminal Justice Information Services (CJIS) for the Florida Department of Law Enforcement (FDLE) in November 1996, after serving as Special Agent in Charge of the Investigative Support Bureau. The CJIS program provides instant telecommunications capabilities for law enforcement throughout the State; criminal justice information storage and retrieval capabilities in Florida and over the entire Nation; criminal identification services; the ability to document and analyze criminal activity for the entire State; statistical and crime trend analysis; criminal record inquiry services for governmental, private, and public record requests; improved system integrity through biennial terminal audits; and a statewide training program for law enforcement. Prior to her appointment at FDLE, she was a Sergeant with the Tallahassee Police Department and a member of that agency for 13 years.

In 1988, Ms. Uzzell was elected to the Leon County (Florida) School Board and completed her 8 years in office, serving 2 years as Board Chair. During the past 8 years, she has worked on safe school policy and procedures and has conducted training throughout the State on crisis intervention, safe school planning, interagency collaboration, and Serious Habitual Offender Comprehensive Action Program (SHOCAP). She currently is an adjunct professor at Florida State University, teaching in the School of Criminology, and is a consultant for Fox Valley Technical College in Wisconsin.

Ms. Uzzell is a certified crime prevention practitioner and former Drug Abuse Resistance Education (D.A.R.E.) officer. She has received recognition for her work in the area of child safety, including a Law Enforcement Officer of the Year award. She has served on several statewide task forces on school and child safety and juvenile justice issues. In 1993, she completed a 4-month special assignment to the Commissioner of Education on law enforcement and education collaborative relationships. In 1993, she spent 5 months on special assignment to the Florida Attorney General's Office developing and implementing the Florida Community Juvenile Justice Partnership Grant Program.

William C. Vickrey

William C. Vickrey is Administrative Director of the Courts of the Administrative Office of the California Courts, managing its legal, court services, fiscal, and other operations that support the California judicial system. As Administrative Director of the Courts, Mr. Vickrey also serves as Secretary of the Judicial Council of California and the Commission on Judicial Appointment, both of which are chaired by the Chief Justice of the California Supreme Court.

Appointed to the position in 1992, Mr. Vickrey has been responsible for many improvements in the State judicial system, including the development of a long-range planning process for State courts, implementation of a statewide budgeting system, and coordination of trial court resources.

Prior to coming to the Administrative Office of the California Courts, Mr. Vickrey was the State Court Administrator for the Utah Administrative Office of the Courts. He also previously served as Executive Director for the Utah Department of Corrections, and Director for the Utah State Division of Youth Corrections.

Mr. Vickrey received the Warren E. Burger Award from the National Center for State Courts in 1995. He previously served as President of the Conference of State Court Administrators.

Mr. Vickrey also co-authored *Managing Transition in a Youth Corrections System* (University of Chicago Press); drafted legislation to establish the Commission on Criminal and Juvenile Justice; and received the 1984 James Larson Award for Outstanding Contributions to Corrections. During 1985, he served as staff to the Governor's Judicial Article Task Force in Utah. This resulted in the passage of HB 100, which established the Court of Appeals, among other reforms of the judiciary. He also co-authored "Utah Court of Appeals: Blueprint for Judicial Reform" for the *Utah Bar Journal.*

Mr. Vickrey received his bachelor's degree from the University of Utah.

Dr. Alan F. Westin

Dr. Alan F. Westin is Professor Emeritus of Public Law and Government at Columbia University; publisher of *Privacy & American Business*; and President of the Center for Social & Legal Research. He is the author or editor of 26 books on constitutional law, civil liberties and civil rights, and American politics.

Dr. Westin's major books on privacy — *Privacy and Freedom* (1967) and *Databanks in a Free Society* (1972) — were pioneering works in the field of privacy and data protection, as were his field studies for the U.S. National Bureau of Standards, *Computers, Health Records, and Citizen Rights* (1976), and *Computers, Personnel Administration, and Citizen Rights* (1979).

Over the past 40 years, Dr. Westin has been a member of Federal and State government privacy commissions and an expert witness before many State and Federal legislative committees and regulatory agencies. These activities have covered privacy issues in such fields as financial services, credit- and consumer-reporting, direct marketing, medical and health, telecommunications, employment, law enforcement, online and interactive services, and social services.

Dr. Westin has been a privacy consultant to many Federal, State, and local government agencies and private foundations. He also has consulted on privacy for over 100 major and start-up companies, including IBM, Security Pacific National Bank, Equifax, American Express, Citicorp, Bell, Prudential, Bank of America, Chrysler, AT&T, SmithKline Beecham, News Corporation, Visa, and Glaxo Wellcome.

He also has spoken at more than 500 national and international business and government meetings on privacy issues since the early 1960s, as well as appearing on all the national U.S. television networks to discuss current privacy developments in business or government.

Between 1978-98, he has been the academic advisor to Louis Harris & Associates for 20 national surveys of public and leadership attitudes toward consumer, employee, and citizen privacy issues in the United States and Canada. He also has worked with Opinion Research Corporation on a dozen proprietary privacy surveys for companies and industry associations.

In 1993, with Robert Belair, he founded a national newsletter and information service, *Privacy & American Business,* to provide expert analysis and a balanced voice on business-privacy issues. *P&AB* also conducts an annual national conference in Washington on "Managing the Privacy Revolution," attended by 250 business, government,

academic, and public interest group representatives. *P&AB* also conducts the Corporate Privacy Leadership Program, and a Global Business Privacy Policies Project.
Dr. Westin earned his bachelor's degree from the University of Florida, an L.L.B. from Harvard Law School, and his Ph.D. in political science from Harvard University. He is a member of the District of Columbia Bar and has been listed in *Who's Who in America* for three decades.

Dr. John Woulds

Dr. John Woulds is Director of Operations at the Office of the Data Protection Registrar, the supervisory authority established in the United Kingdom under the 1984 *Data Protection Act*. Dr. Woulds has been in the Office of the Data Protection Registrar since March 1985. As Director of Operations, he is a member of the Registrar's Management Board and has responsibility for all operational aspects of the work of the office. This includes registration, complaints, casework, investigations, compliance casework, and policy advisory work in all sectors.

Prior to his appointment with the Data Protection Registrar, he worked for several years in computer management in scientific computing centers. Before that, he was an active research scientist in the field of high-energy particle physics.

Staff biographies

— Bureau of Justice Statistics, U.S. Department of Justice

Dr. Jan M. Chaiken

Dr. Jan M. Chaiken was Director of the Bureau of Justice Statistics (BJS), U.S. DOJ, until January 2001. His appointment to this position by President Clinton was confirmed in September 1994.

Dr. Chaiken earned his Ph.D. in mathematics at the Massachusetts Institute of Technology (MIT). He was an Assistant Professor in the mathematics department of Cornell University; a Research Associate at MIT; a Senior Mathematician at the Rand Corporation in Santa Monica, California, from 1972-84; an Adjunct Associate Professor in the system sciences department of the University of California, Los Angeles; and a Principal Scientist in the law and justice area at Abt Associates, Inc., in Cambridge, Massachusetts, from 1984 until his nomination as BJS Director.

Dr. Chaiken's research has focused on developing and applying methods for improving operations of criminal justice agencies, including studies of the criminal investigation process, police patrol allocation, predicting prison populations, models of the criminal justice system, and statistical analyses of the Federal criminal justice system.

Dr. Chaiken and his wife, Dr. Marcia Chaiken, who is now Director of Research at LINC in Alexandria, Virginia, collaborated on numerous research topics, such as varieties of criminal behavior, identifying career criminals for priority prosecution, drugs and crime, multijurisdictional drug task forces, improving sample designs for learning about drug use of arrestees, and private policing.

During his tenure as BJS Director, Dr. Chaiken has focused on the use of modern technologies, such as the World Wide Web, to provide the public with accurate, up-to-date statistics, to allow the rapid interstate exchange of criminal histories and information about registries of sex offenders, to facilitate the implementation of the FBI's National Incident-Based Reporting System, and to develop improved computerized tracking of Federal arrestees and defendants through the criminal justice process.

Carol G. Kaplan

Carol G. Kaplan is currently Chief, Criminal History Improvement Programs, BJS, U.S. DOJ. In this capacity, she is responsible for managing all BJS programs that focus on improving the quality and accessibility of criminal history records and the establishment of the national criminal record system. Ms. Kaplan is also responsible for all BJS activities to ensure the privacy of criminal record data and to support implementation of the *Brady*

Handgun Violence Prevention Act and the *National Child Protection Act of 1993*.

Previously, Ms. Kaplan served as the Assistant Deputy Director, BJS, overseeing programs relating to criminal justice information policy, privacy policy development, and Federal justice statistics. In this position, she was responsible for all BJS publications, conferences, and technical assistance dealing with criminal history record issues, privacy policy, and Federal justice statistics.

Ms. Kaplan has been involved in Federal activities relating to the development of privacy policy throughout her career, and participated in drafting the initial landmark Federal regulations ensuring the privacy, accuracy, and completeness of criminal records and the confidentiality of federally supported research data. She has served on numerous interagency task forces to develop policies and standards applicable to record usage and was a charter member of the Office of Justice Programs' Intelligence Systems Policy Review Board.

Ms. Kaplan was formerly an Attorney with the Department of Health, Education and Welfare and the Federal Communications Commission.

Ms. Kaplan is a graduate of Columbia University Law School and Radcliffe College.

— Office of Justice Programs, U.S. Department of Justice

Anne Gardner

Anne Gardner is an Attorney-Advisor for the Office of Justice Programs (OJP), U.S. DOJ, under the Attorney General's Honors Program. Ms. Gardner is a member of OJP's Intergovernmental Information Sharing Working Group, Intelligence Systems Policy Review Board, and Privacy Task Force.

Ms. Gardner received her B.S. degree from the University of Wisconsin – Madison, and her J.D. from The Catholic University of America, Columbus School of Law, *cum laude.* Her publications include "Legislation: A New Design for Justice Integration," 30 *McGeorge Law Review* 9 (1998).

Paul F. Kendall

Paul F. Kendall, General Counsel for OJP, is the Executive Chairman of OJP's Information Technology Executive Council, as well as Chairman of the Executive Council's Inter-governmental Information Sharing Working Group, the Intelligence Systems Policy Review Board, and the Privacy Task Force. Mr. Kendall is leading a variety of efforts in developing State and local coordinated information technology programs, and is leading the Review Board's examination of legal and public policy issues associated with information sharing. Prior to his appointment as General Counsel, Mr. Kendall held positions of Senior Counsel at the Federal Mine Safety Board, and Assistant General Counsel of the Legal Services Corporation, as well as other positions in public and private practice.

Mr. Kendall received his B.A. degree from Columbia College of Columbia University, his M.B.A. from the University of Maryland, and his J.D. from The Catholic University of America, Columbus School of Law. His publications include "Legislation: A New Design for Justice Integration," 30 *McGeorge Law Review* 9 (1998).

— SEARCH, The National Consortium for Justice Information and Statistics

Sheila J. Barton

As a Deputy Executive Director of SEARCH, Sheila J. Barton is responsible for the development and implementation of a multifaceted program of public policy analysis, documentation of State and Federal information policy development, education, and assistance to State and local policymakers; the conduct of national conferences and workshops on justice information policy issues; and the publication of timely studies on justice information policy. She is also In-house Counsel and staff to the SEARCH Law and Policy Program Advisory

Committee and Board of Directors.

Prior to joining SEARCH, Ms. Barton was a Municipal Judge in Cheyenne, Wyoming, and also was engaged in the private practice of law. She also has held the positions of Public Defender for Cheyenne, and Staff Attorney to the Wyoming Supreme Court. She previously served in the New York State Department of Correctional Services, Office of the Special Legal Assistant to the Commissioner, and Legal Specialist for the Department's Division of Health Services. Prior to her service in New York, she was Associate County Judge for Lincoln County, Nebraska.

Ms. Barton holds a B.A. degree from Augustana College (South Dakota) and a J.D. from the University of Nebraska College of Law. She is a member of the Bars of California, Nebraska, and Wyoming.

Gary R. Cooper

Since 1983, Gary R. Cooper has served as the Executive Director of SEARCH. In his role as Executive Director, Mr. Cooper is called upon to represent SEARCH before the various branches and levels of government, including the U.S. Congress and the U. S. DOJ; criminal justice associations; and the private sector. He has twice chaired the Evaluation Committee for tests of the Interstate Identification Index, a committee of the Advisory Policy Board to the FBI's National Crime Information Center, and currently chairs the FBI's Evaluation Group for the National Fingerprint File Pilot Project.

In 1981, Mr. Cooper was appointed by California's Governor to the California Commission on Personal Privacy. He currently serves on the Board of Directors for the National Foundation for Law and Technology. With SEARCH for 26 years, Mr. Cooper also has served as the Deputy Director and the Director of the Law and Policy Program.

Mr. Cooper's law enforcement career began as a Patrolman for the City of Sacramento, and he has held various research and planning positions with the California Council on Criminal Justice and the California Crime Technological Research Foundation. He has written extensively in all areas of information law and policy, with an emphasis on the privacy and security of criminal history records.

Mr. Cooper received his B.A. degree in political science from the University of California, Davis.

Eric C. Johnson

Eric C. Johnson is a Policy Research Analyst in SEARCH's Law and Policy Division, where he researches and writes on issues relating to criminal justice information management and policy. Mr. Johnson joined SEARCH's Corporate Communications staff in July 1997 as a Writer/Researcher. He contributed to SEARCH publications, including *Interface*, *SEARCH Update*, and *SEARCHLite*, and also worked on other communications and program-related projects involving writing, editing, and design.

Mr. Johnson authored two of SEARCH's *Technical Bulletins*: "Court Automation and Integration: Issues and Technologies," and "From the Inkpad to the Mousepad: IAFIS and Fingerprint Technology at the Dawn of the 21st Century." The latter, which focused on the FBI's Integrated Automated Fingerprint Identification System, was reprinted in the April 1999 issue of *Government Technology* magazine.

Before joining SEARCH, Mr. Johnson served for 7 years as Editor of the Northern California *Teamster* newspaper, with a circulation of 65,000 in the greater San Francisco Bay area. He has worked in the mainstream press as a Reporter and Assignment Editor, and also in government and in public relations, where his writing was honored with a Bay Area Publicity Club Award. He holds a Bachelor of Arts degree in Journalism from San Francisco State University.

Mr. Johnson joined SEARCH's Law and Policy staff on May 1, 1999.

Appendix 2:

Glossary of criminal justice information terms

Confidentiality refers to information itself, and means that only certain persons under specified circumstances are authorized to have access to particular information.[1]

Criminal History Record Information (CHRI) means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations or other formal criminal charges (and any disposition arising therefrom), sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. State and Federal Inspector General Offices are included.[2]

Criminal Intelligence Information means information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity.[3]

Criminal Investigative Information means information on identifiable individuals compiled in the course of an investigation of specific criminal acts.[4]

Criminal Justice Agency means (1) Courts; (2) A government agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.[5]

Criminal Justice Information includes CHRI, criminal intelligence information, criminal investigative information, disposition information, identification record information, nonconviction information, and wanted person information.[6]

Disposition means information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings, and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Examples of dispositions include (but are not limited to), acquittal, dismissal, case continued without finding, charge dismissed, charge still pending, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed defendant discharged (civil action, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial), executive clemency, placed on probation, paroled, or released from correctional supervision.[7]

Nonconviction information means arrest information without disposition if an interval of 1 year has elapsed from the date of arrest and no active prosecution of the charge is pending; or information disclosing that the police have elected not to refer a matter to a prosecutor; or information disclosing that a prosecutor has elected not to commence criminal proceedings; or information disclosing that proceedings have been indefinitely postponed, as well as all acquittals and all dismissals.[8]

Privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[9]

---

[1] George B. Trubow, "Information Law Overview," 18 *J. Marshall L. Rev.* 815, 817 (1985).

[2] 28 C.F.R. § 20.23(b).

[3] *Technical Report No. 13: Standards for the Security and Privacy of Criminal History Record Information*, 3rd ed. (Sacramento: SEARCH Group, Inc., 1988) Standard 2.1(d). Hereafter, Technical Report No. 13.

[4] Technical Report No. 13, Standard 2.1(e).

[5] 28 C.F.R. § 20.23(c).

[6] Technical Report No. 13, Standard 2.1.

[7] 28 C.F.R. § 20.23(e).

[8] 28 C.F.R. § 20.23(k).

[9] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) p. 7.

Appendix 3:

Comparison of criminal history and other privacy measures

- Notice
- Choice
- Onward transfer
- Security
- Data integrity
- Access
- Enforcement

Comparison of criminal history and other privacy measures[1]	
	Notice
Federal justice information system regulations[2]	None.
Safe Harbor Privacy Principles[3]	An organization must inform individuals about: · The purposes for which it collects and uses PII. · How to contact the organization with any inquiries or complaints. · The types of third parties to which it discloses the information. · The choices and means offered to individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language that is readily understood; and the notice must be made available when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable. In any event, notice must be provided before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization, or before the organization discloses it for the first time to a third party.
Online Privacy Alliance Principles	The policy must state clearly: · What PII is collected. · The use of that information. · Possible third-party distribution. · The choices available to an individual. · The company's commitment to data security. · What steps the organization takes to ensure data quality and access. The policy should: · Disclose any consequences of a refusal to provide PII. · Include a statement of enforcement mechanisms and how to contact the organization. A privacy policy must be easy to find, read, and understand. The policy must be available prior to or at the time that the PII is collected or requested.

[1]The measures reviewed here use various terms to identify and, in some cases, to define the personal information covered by the measure. Examples include personal information and data, protected health information, individually identifiable information, and so on. For ease of comparison, this chart uses the abbreviation "PII" (personally identifiable information), or simply "information" or "data."

[2]28 C.F.R. Part 20. (Also known as the "DOJ regulations.")

[3]65 *Federal Register* 45666 (July 24, 2000).

	Notice (cont.)
Fair Credit Reporting Act	Upon request, notice, substantially similar to the model promulgated by the Federal Trade Commission (FTC), must be provided to consumers; those who regularly supply the credit-reporting agency with information; and those who receive reports.[4] A consumer-reporting agency that furnishes a consumer report for employment purposes containing public record information, including criminal history records, which is "likely to have an adverse effect upon a consumer's ability to obtain employment," must either provide the consumer with notice at the same time that the information is reported to the potential employer or "must maintain strict procedures" to ensure that the information is complete and up-to-date.[5] Consumers also must be notified if a credit report provided the basis for an adverse determination.[6]
Individual Reference Services Group Principles	Each individual reference service (Service) shall have an information practices policy statement that is available upon request that describes: · What types of PII it has. · From what types of sources. · How it is collected. · The type of entities to whom it may be disclosed. · The type of uses to which it is put.[7]
European Union Directive	Requires disclosure of information, such as: · The identity of the controller. · The purposes of the processing for which the data are intended. Notice should also include any further information necessary to guarantee fair processing, such as: · The recipients or categories of recipients of the data. · Whether replies to questions are obligatory or voluntary, and possible consequences for failing to reply. · The existence of the right of access and the right to rectify data.[8]
Comments	Notice of potential uses of criminal justice information traditionally has not been viewed as necessary, in part because the notice will not influence subject behavior and it is unlikely that the individual will be interested in the contents of a privacy notice at the time of arrest, conviction, or imprisonment.

[4] 15 U.S.C. § 1681e(d).
[5] 15 U.S.C. § 1681k.
[6] 15 U.S.C. § 1681b(b)(3).
[7] Individual Reference Services Group, "Individual Reference Service Industry Principles" (December 15, 1997) Article VII. Available at **http://www.dbtonline.com/irsg-principles.asp**. Hereafter, IRSG Principles.
[8] Directive 95/46/EC, Articles 10, 11. Hereafter, Directive.

Comparison of criminal history and other privacy measures	
	Choice
Federal justice information system regulations	None.
Safe Harbor Privacy Principles	Organization must: · Offer the opportunity to choose whether PII they provide is disclosed to third parties or used (where such use is incompatible with the purpose for which it was originally collected or subsequently authorized). · Provide clear, conspicuous, readily available, and affordable mechanisms. · Require opt-in choice for sensitive types of information.
Online Privacy Alliance Principles	Individuals must be given the opportunity to exercise choice regarding how PII collected from them online may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use.
Fair Credit Reporting Act	With certain exceptions, consumer consent is required before a consumer report may be furnished.[9] Consumers may elect to be excluded from certain lists relating to offers of insurance or credit not initiated by the consumer.[10] Consumer-reporting agencies may not provide reports containing medical information for certain purposes without the consent of the consumer.[11]
Individual Reference Services Group Principles	Each Service shall, upon request, inform individuals of the choices, if any, available to limit access or use of information about them in its database, provided, however, that in the case of nonpublic information distributed to the general public, a Service shall provide an opportunity for an individual to limit the general public's access or use of such information.[12]
European Union Directive	Individual consent for processing is frequently required; however, certain nonconsensual processing is also permitted.[13] Provides individual with the right to object, in certain circumstances, to certain processing of data about the individual.[14]
Comments	Record subjects have never been able to choose to consent or opt-out of the criminal history record regime. Participants in the criminal justice process are not voluntary participants; given the potential for adverse consequences resulting from disclosure, it is assumed that all record subjects would opt-out.

[9] 15 U.S.C. § 1681b(b)(2), (c)(1).
[10] 15 U.S.C. § 1681b(e).
[11] 15 U.S.C. § 1681b(g).
[12] IRSG Principles, Article VIII.
[13] See, for example, Directive, Articles 7, 9, and 13.
[14] Directive, Article 14.

Comparison of criminal history and other privacy measures	
	Onward transfer
Federal justice information system regulations	Dissemination of nonconviction data must be limited to: · Criminal justice agencies for administration of the justice system and justice agency employment. · Individuals or agencies as authorized by statute, executive order, ordinance, or court action. · Agents and contractors of criminal justice agencies. · Individuals and agencies for the express purpose of research, evaluative, or statistical activities, provided safeguards are in place.[15]
Safe Harbor Privacy Principles	· An organization may only disclose PII to a third party for the third party's own use consistent with the principles of notice and choice. · PII may be transferred to a third party acting as the organization's agent, provided that the third party has adopted the Safe Harbor Principles, is subject to another "adequate" privacy regime, or has provided suitable contractual assurances regarding the third party's privacy practices.
Online Privacy Alliance Principles	· In most circumstances, where there is third-party distribution of PII, collected online from the individual, unrelated to the purpose for which it was collected, the individual should be given the opportunity to opt-out. · Consent for such use or third-party distribution may also be obtained through technological tools or opt-in. Organizations should ensure that third parties to which they transfer PII are aware of these security practices, and take reasonable precautions to protect any transferred PII.
Fair Credit Reporting Act	Consumer reports may be only used for permissible purposes. Information may be provided to consumer-reporting agencies without individual consent. Consent is required for most disclosures of consumer report information.
Individual Reference Services Group Principles	See Choice section.
European Union Directive	Individual consent for processing is frequently required; however, certain nonconsensual processing is also permitted.[16] Restricts onward transfers to countries without "adequate" privacy protections.[17] Contractors "must provide sufficient guarantees," by contract, which obligate the contractor to the required security measures.[18]
Comments	Under the DOJ regulations, conviction information may be disseminated without restriction while nonconviction information is unavailable unless specifically authorized by State law, regulation, or policy. The DOJ regulations are detailed and relatively privacy-protective of the criminal history information covered.

[15]28 C.F.R. § 20.21(b).
[16]See, for example, Directive, Articles 7, 9, and 13.
[17]Directive, Articles 25, 26.
[18]Directive, Article 17(2) and (3).

Comparison of criminal history and other privacy measures	
	Security
Federal justice information system regulations	Wherever criminal history record information is collected, stored, or disseminated, each State shall ensure that technical, physical, or administrative actions are taken to ensure the security of the information.[19]
Safe Harbor Privacy Principles	Organizations creating, maintaining, using, or disseminating records of PII must take reasonable precautions to protect it from loss, misuse, unauthorized access, or disclosure, alteration, and destruction.
Online Privacy Alliance Principles	Organizations creating, maintaining, using, or disseminating PII should take: · Appropriate measures to ensure its reliability. · Reasonable precautions to protect it from loss, misuse, or alteration.
Fair Credit Reporting Act	Consumer-reporting agencies are required to "maintain reasonable procedures" to avoid violations of key provisions of the Act.[20]
Individual Reference Services Group Principles	Services shall maintain facilities and systems to protect information from unauthorized access and persons who may exceed their authorization. In addition to physical and electronic security, Services shall reasonably implement employee and contractor supervision and system reviews at appropriate intervals.[21]
European Union Directive	Requires "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves transmission of data over a network, and against all other unlawful forms of processing."[22]
Comments	The DOJ regulations compare favorably with those found in other privacy measures. The DOJ regulations require a wide range of security measures to guard against unauthorized access or disclosure, as well as natural disasters.

[19]28 C.F.R. § 20.21(f).
[20]15 U.S.C. § 1681e(a).
[21]IRSG Principles, Article VI.
[22]Directive, Article 17(1).

Comparison of criminal history and other privacy measures	
	Data integrity
Federal justice information system regulations	Complete records should be maintained at a central State repository. To be "complete" means that the State repository must record a disposition within 90 days of the date of disposition. To be "accurate" means that no record containing criminal history record information shall contain erroneous information. Criminal justice agencies shall institute processes that will minimize the possibility of recording and storing information of an inaccurate nature.[23]
Safe Harbor Privacy Principles	Consistent with the other principles, PII must be relevant to the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data are accurate, complete, and current.
Online Privacy Alliance Principles	Organizations creating, maintaining, using, or disseminating PII should take reasonable steps to ensure that the data are accurate, complete, and timely for the purposes for which they are to be used.
Fair Credit Reporting Act	Consumer-reporting agencies may disclose a consumer report only for specified permissible purposes.[24] The Act prohibits certain information from inclusion in most consumer reports.[25]
Individual Reference Services Group Principles	Reasonable steps shall be taken to help ensure the accuracy of the information in Services. When contacted about alleged inaccuracies, Services shall either correct any inaccuracy or direct the individual to the source of the information.[26]
European Union Directive	PII must be "collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical, or scientific purposes shall not be considered as incompatible, provided that Member States provide appropriate safeguards."[27]
Comments	The DOJ regulations are at least comparable to the other measures examined here. In some cases, such as the OPA and IRSG Principles, the DOJ standards may actually be more stringent because they appear to require more than "reasonable" efforts.

[23]28 C.F.R. § 20.21(a).
[24]15 U.S.C. § 1681(b).
[25]15 U.S.C. § 1681(c).
[26]IRSG Principles, Article III.
[27]Directive, Article 6(1)(b).

Comparison of criminal history and other privacy measures	
	Access
Federal justice information system regulations	Requires that States grant access to record subjects upon satisfactory verification of identity. Record subjects are permitted to obtain copies of records (excluding intelligence, investigative, and related files) when necessary for challenge or correction. States are required to establish administrative review and appeal procedures for record subjects who challenge the accuracy of information.[28]
Safe Harbor Privacy Principles	Individuals must have access to PII about them that an organization holds and be able to correct, amend**,** or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
Online Privacy Alliance Principles	Organizations should establish appropriate processes or mechanisms so that inaccuracies in material PII, such as account or contact information, may be corrected. These procedures and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to ensure data quality may include use of reliable sources and collection methods; reasonable and appropriate consumer access and correction; and protections against accidental or unauthorized alteration.
Fair Credit Reporting Act	Consumer-reporting agencies are required to disclose, upon the consumer's request, specified information that the credit-reporting agency possesses about the consumer, as well as a summary of the individual's rights under FCRA and contact information. (Summary of rights must be substantially similar to FTC model.)[29] Consumer has the ability to dispute information believed to be inaccurate and to request reinvestigation of such information.[30]
Individual Reference Services Group Principles	Upon request and reasonable terms, Services shall: · Inform individuals about the nature of public record and publicly available information it makes available in its products. · Provide individuals with nonpublic information contained in products or services that specifically identify the individual. · Direct individuals to a consumer-reporting agency when such agency is the source of the PII.[31]

[28] 28 C.F.R. § 20.21(g).
[29] 15 U.S.C. § 1681g.
[30] 15 U.S.C. § 1681I.
[31] IRSG Principles, Article IX.

	Access (cont.)
European Union Directive	Requires, with certain exceptions, that inquiries be acted upon "without constraint at reasonable intervals and without excessive delay or expense."[32] Requires Member States to guarantee a data subject's right to determine if personal data are being processed and what data are being processed.[33] "Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information."[34] Requires that data subjects be given the rights of "rectification, erasure, or blocking," as appropriate.[35]
Comments	The DOJ standards are largely comparable concerning individual rights of access and correction. The DOJ regulations are more favorable than some of the other measures in that they guarantee administrative procedures and appeals in the event of disagreements between the record subject and agency over record correction requests. The DOJ regulations are less protective insofar as they only guarantee record subjects the right to obtain copies of their records if necessary for purposes of challenge or correction.

[32]Directive, Article 12(a).
[33]Ibid.
[34]Recital 42.
[35]Directive, Article 12(b).

Comparison of criminal history and other privacy measures	
	Enforcement
Federal justice information system regulations	Any agency or individual in violation may be fined up to $10,000. In addition, agencies may be subject to loss of Federal funding.[36] States must establish administrative and appeals processes for record subject challenges to record accuracy.[37]
Safe Harbor Privacy Principles	At a minimum, mechanisms must include: · Readily available and affordable independent recourse by which an individual's complaints and disputes can be investigated and resolved and damages awarded where provided by applicable law or private initiative. · Procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that practices are implemented as presented. · Obligations to remedy problems arising out of noncompliance by companies adopting the principles. · Sufficiently rigorous sanctions to ensure compliance.
Online Privacy Alliance Principles	Whether administered by a third-party seal program, licensing program, or membership association, the effective enforcement of self-regulation requires: · Verification and monitoring. · Complaint resolution. · Education and outreach. OPA believes the best way to create public trust is for organizations to alert consumers and other individuals to the organization's practices and procedures through participation in a program that has an easy-to-recognize symbol or seal.
Fair Credit Reporting Act	Authorizes private right of action by consumers.[38] Administrative enforcement by the FTC is authorized and the FTC may initiate civil court actions. States and other Federal agencies may bring actions in specified circumstances.[39]
Individual Reference Services Group Principles	Periodic compliance audits by outside auditors are required. A summary of results must be made publicly available.[40]
European Union Directive	Member States are required to provide judicial remedies for a data subject whose rights are provided under national law.[41] Data subjects are to be entitled to "compensation from the controller for the damage suffered."[42]
Comments	The DOJ regulations authorize fines against both agencies and individuals for violations of the regulations. In addition, agencies run the risk of losing Federal funding if they fail to comply with the regulations.

[36]28 C.F.R. § 20.25.
[37]28 C.F.R. § 20.21(g).
[38]15 U.S.C. § 1681n.
[39]15 U.S.C. §1681s.
[40]IRSG Principles, Article XI.
[41]Directive, Article 22.
[42]Directive, Article 21(1).