# National Conference on Privacy, Technology and Criminal Justice Information

## *Proceedings of a Bureau of Justice Statistics/SEARCH conference*

**Papers presented by**


**Gary R. Cooper**
**Peter P. Swire**
**Dr. Jan M. Chaiken**
**Timothy D. Ellard**
**Dr. Alan F. Westin**
**Robert R. Belair**
**John T. Bentivoglio**
**Hon. Thomas M. Cecil**
**Hon. Gordon A. Martin Jr.**
**David Gavin**
**Iris Morgan**
**Roger W. Ham**
**Dr. John N. Woulds**
**James X. Dempsey**
**Beth Givens**
**Prof. Jane E. Kirtley**
**Dr. Donald F. Harris**
**Lawrence F. Potts**
**Emilio W. Cividanes**
**Peter L. O'Neill**
**Stuart K. Pratt**

# National Conference on Privacy, Technology and Criminal Justice Information

## *Proceedings of a Bureau of Justice Statistics/SEARCH conference*

**November 2001**

**Papers presented by**

**Gary R. Cooper**
**Peter P. Swire**
**Dr. Jan M. Chaiken**
**Timothy D. Ellard**
**Dr. Alan F. Westin**
**Robert R. Belair**
**John T. Bentivoglio**
**Hon. Thomas M. Cecil**
**Hon. Gordon A. Martin Jr.**
**David Gavin**
**Iris Morgan**
**Roger W. Ham**
**Dr. John N. Woulds**
**James X. Dempsey**
**Beth Givens**
**Prof. Jane E. Kirtley**
**Dr. Donald F. Harris**
**Lawrence F. Potts**
**Emilio W. Cividanes**
**Peter L. O'Neill**
**Stuart K. Pratt**

**SEARCH**
The National Consortium for Justice Information and Statistics
7311 Greenhaven Drive, Suite 145 • Sacramento, CA 95831
(916) 392-2550 • Fax (916) 392-8440 • www.search.org

**Acknowledgments**

This report was prepared by SEARCH, The National Consortium for Justice Information and Statistics, Kenneth E. Bischoff, Chairman, and Gary R. Cooper, Executive Director. The Project director was Sheila J. Barton, Deputy Director. Linda B. Townsdin, Writer/Editor, Corporate Communications, and Eric Johnson, Policy Research Analyst, edited the proceedings. Jane L. Bassett, Publishing Specialist, provided layout and design assistance. The Federal project monitor was Carol G. Kaplan, Chief, National Criminal History Improvement Programs, Bureau of Justice Statistics.

Report of work performed under BJS Grant No. 2000-MU-MU-K006, awarded to SEARCH Group, Inc., 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831. Contents of this document do not necessarily reflect the views or policies of the Bureau of Justice Statistics or the U.S. Department of Justice.

# Contents

## Introduction

The two-year "Millennium Privacy Project" undertaken in 1998 by the Bureau of Justice Statistics (BJS), Office of Justice Programs, U.S. Department of Justice (DOJ), and SEARCH, The National Consortium for Justice Information and Statistics, culminated in the *National Conference on Privacy, Technology and Criminal Justice Information*, which was held in Washington D.C., May 31-June 1, 2000.

The project scope involved a comprehensive review of the law and policy addressing the collection, use, and dissemination of criminal justice record information and, particularly, criminal history record information (CHRI).[1]

To aid in this project, BJS and SEARCH assembled a task force that included experts from criminal history record repositories and courts, commercial compilers of CHRI, criminal justice and noncriminal justice users, the media (open records advocates), academics, and government agency representatives to tackle the complex issues surrounding law and policy for handling CHRI. The National Task Force on Privacy, Technology and Criminal Justice Information met for a total of 6 days over a period of 2 years. Serving as the foundation for this conference were (1) the Task Force report,[2] which identified and recommended strategies for dealing with the privacy implications for criminal justice information management; and (2) the results of the first professionally commissioned public opinion survey on a comprehensive range of criminal justice privacy issues.[3]

The conference provided resources and guidance to policymakers and practitioners charged with managing criminal justice information. It provided a forum for exchanging ideas and sharing experiences about the changing landscape of the criminal justice environment. Some of the changes identified by the Task Force included: (1) the growing demand for

[1] The project was funded by and operated under the auspices of BJS, a bureau within the U.S. DOJ that is the United States' primary source for criminal justice statistics. *See* www.ojp.usdoj.gov/bjs/. SEARCH is a State criminal justice support organization that promotes the effective and appropriate use of information, identification, and communications technology for State and local criminal justice agencies. *See* www.search.org.

[2] Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology, and Criminal Justice Information*, Privacy, Technology, and Criminal Justice Information series, NCJ 187669 (Washington, D.C.: U.S. Department of Justice, August 2001). The report is available at www.ojp.usdoj.gov/bjs/abstract/rntfptcj.htm.

[3] A report that summarizes the survey findings is available at www.ojp.usdoj.gov/bjs/abstract/pauchi.htm. *See* Bureau of Justice Statistics, *Public Attitudes Toward Uses of Criminal History Information, A Privacy, Technology, and Criminal Justice Information Report*, NCJ 187663 (Washington, D.C.: U.S. Department of Justice, July 2001).

criminal justice information; (2) the impact of recent advances in information, identification, and communication technologies; (3) the trend toward integrated systems and open criminal history records across jurisdictional, agency, and criminal and noncriminal justice lines; (4) the trend toward increased public access and demand for criminal justice information; and (5) the impact of Federal legislation, such as the *National Child Protection* and the *Sex Offender Registration Acts*, and State legislation such as statutorily mandated employment background checks. In addition, the growing commercialization of records — criminal histories being compiled from public records for sale to the private sector — and other complex issues were presented and debated during the course of the conference.

Presenters included officials from the U.S. DOJ and Federal Bureau of Investigation (FBI); representatives from State, national, and international criminal justice agencies and organizations; and commercial providers of background information. Representatives of agencies in 44 States and England and Canada attended. This document presents the proceedings of the conference.

## Overview

Day one focused primarily on the challenges of privacy in the 21st century. Two keynote speakers addressed privacy and the future of justice statistics, and an overview of the Federal role in collecting statistical information. The keynotes were followed by a panel discussion on privacy and public attitudes toward uses of criminal history information, and then a detailed report from the Chair of the National Task Force on Privacy, Technology and Criminal Justice Information regarding the findings and recommendations the Task Force reached based on its research and deliberations.

Day two focused on the stakeholders of privacy interests and began with a keynote address that provided an overview of the U.S. DOJ's role in the privacy area. Two subsequent panels representing government holders of criminal justice information discussed CHRI from the viewpoint of the courts role, and then from the role of law enforcement and State criminal history repositories. The courts panel, comprised of two trial court judges, discussed whether courts should continue to be an open public records source for CHRI, and the implications for juvenile record subjects. The law enforcement panel, comprised of representatives of Federal, State, and local justice agencies, discussed whether States should continue to impose restrictions on access to information held in repositories.

A third "stakeholder" panel, which included privacy experts from the United States and United Kingdom, discussed the role of privacy in the Information Age from a privacy advocacy perspective. Then, a media expert offered the media's perspective on regulating the dissemination of CHRI.

A fourth "stakeholder" panel focused on criminal

history record consumers and the determining factors concerning who has or should be allowed to access this information. The final "stakeholder" panel focused on commercial providers of background information and whether they should be regulated and in what manner. The conference concluded with remarks from the Chair of the National Conference on Privacy, Technology and Criminal Justice Information.

The following is a more detailed description of these presentations and discussions.

## Challenges of privacy in the 21st century

Mr. Gary R. Cooper, Executive Director of SEARCH, opened day one of the conference with welcoming remarks, and an anecdote that set the tone for conference attendees to consider the difficult balance that must be achieved between the need of government and society to have information, and the individual's right to privacy.

Mr. Peter P. Swire, who was Privacy Counselor to the President at the time of the conference, delivered the first keynote address, in which he talked about the free flow of information in society, the Administration's recent activities in the privacy area, the Federal government's role, and the area of public records in the context of current privacy discussions. His address ended with a question-and-answer session with conference attendees.

The next keynote speaker, Dr. Jan M. Chaiken, who was BJS Director at the time of the conference, discussed "The role of confidentiality in collecting statistical information." Dr. Chaiken presented examples of the laws and regulations BJS must adhere to in gathering and disseminating statistical information, and concluded that within the Federal statistical system, "review and oversight of the practices are so strong that it is nearly impossible for someone's confidential information to be misused."

## Privacy and public opinion

Next, a panel discussed the issue of privacy and public opinion, and was moderated by Dr. David H. Flaherty, of David H. Flaherty Inc., Privacy and Information Policy Consultants. The panel was comprised of Mr. Timothy D. Ellard, Senior Vice President, Opinion Research Corporation, and Dr. Alan F. Westin, Professor Emeritus, Columbia University. Panelist presentations were followed by a question-and-answer session, which provided an opportunity for individuals to discuss specific experiences related to the presentations.

Mr. Ellard spoke about "Public attitudes toward uses of criminal history information," summarizing the survey his company conducted on behalf of SEARCH and BJS. More than 1,000 respondents were interviewed by telephone for this survey. He reported that key findings from the survey indicated that "U.S. adults' concern about misuse of personal information extends to criminal history (and related) records, but that most are willing to

give up some privacy protection if the trade-off results in a benefit to the public, such as increased safety, crime prevention, or the protection of children."

In a related presentation, Dr. Westin spoke about "Balancing privacy and public uses of criminal history information." From his perspective as a long-time privacy expert and survey advisor, Dr. Westin commented on what the data from Mr. Ellard's survey said about public attitudes toward the use of criminal history information both inside and outside the criminal justice system. His general conclusion was that the "public will support the development of new rules for societal uses of criminal history information in an information-rich age when people are seeking better access to criminal history information on the one hand, while also being very worried about inappropriate or dangerous uses of information."

The final speaker on day one, Mr. Robert R. Belair, reported on the activities of the National Task Force on Privacy, Technology and Criminal Justice Information. Mr. Belair, who is SEARCH General Counsel, chaired the Task Force. He discussed the four deliverables generated by the Task Force: (1) the Task Force report, which analyzes existing law and policy for handling CHRI, and identifies the technological and societal developments that may be changing the criminal justice privacy environment; (2) the public opinion survey discussed in the previous panel; (3) the Task Force recommendations; and (4) the final conference proceedings. In Mr. Belair's concluding remarks, he stressed, "policy and law for criminal history is going to change dramatically over the next 5 years, and the Task Force effort is the first step in shaping what that new generation should look like."

Mr. Belair's presentation included a question-and-answer session with conference attendees.

### Stakeholders of privacy interests

Day two of the conference focused on the theme "The stakeholders of privacy interests." Mr. John T. Bentivoglio, Counsel to the Deputy Attorney General, U.S. DOJ, delivered the keynote address. Mr. Bentivoglio presented an overview of what the DOJ is doing in the privacy area. He stressed the importance of addressing the challenges of the Information Age "through collaborative efforts — the law enforcement and public safety community will have to work with industry as well." His address also concluded with a question-and-answer session with the audience.

Two panel discussions followed that addressed privacy issues from the perspective of government holders of criminal justice information. The first panel addressed the role of courts, specifically whether courts should continue to be an open public records source for CHRI and the implications for juvenile record subjects. The panel, which was moderated by SEARCH Courts Program Director Francis L. Bremson, was comprised of two nationally known experts in this area, the Honorable Thomas M.

Cecil, former presiding judge of the Sacramento (California) Superior Court, and the Honorable Gordon A. Martin Jr., Massachusetts Trial Court.

Judge Cecil discussed his concern about the "constant call for increased public access to the courts." He stressed, "Not everybody understands what that means, or if everybody has the same definitions. An automated court system would be more effective and efficient, but issues relative to expungement, rehabilitation, and others must be taken under consideration as well to ensure an accurate, realistic, and well-thought-out balance between privacy and public safety."

Judge Martin, from the perspective of having completed 6 years as a Trustee of the National Council of Juvenile and Family Court Judges, presented an overview of juvenile courts today. Juvenile courts have existed in our country for more than 100 years. Today, 42 States allow the court records of juveniles charged with delinquency to be released to the public. Judge Martin emphasized that the juveniles who have committed a violent act are already in adult court due to changes in laws over the last decade, and are no longer under the protection of juvenile courts.

Judges Cecil and Martin then responded to questions from the audience.

The second "government stakeholder" panel discussed "The role of law enforcement and the State criminal history repositories" with respect to privacy, specifically whether States should continue to impose restrictions on access to CHRI held in repositories. Mr. Ronald P. Hawley, Chief Operating Officer of the North Carolina Office of Information Technology Services, moderated the panel.

The first panelist was Mr. David Gavin, Chair of the FBI Criminal Justice Information Services Advisory Policy Board (CJIS APB), and Assistant Chief of Administration, Crime Records Service, Texas Department of Public Safety. In responding to the question as to whether access to CHRI should be restricted, Mr. Gavin concluded that, from the point of view of the FBI's national advisory process, "even under the global set of controls, law enforcement systems, courts records systems, and commercial provider records systems serve different purposes, so rather than simply lifting the restrictions, (we should) also figure out how to maintain the purposes of those separate entities."

The next panelist to speak was Ms. Iris Morgan, Senior Management Analyst, Criminal Justice Information Services, Florida Department of Law Enforcement. Ms. Morgan presented an overview of Florida as an open records State. In 1999, Florida processed over 400,000 record checks approved under State statutes. Florida has also posted sexual predator data on the Internet since 1996, and the site has received well over 1 million hits.

A third panelist was Mr. Roger W. Ham, Chief Information Officer, Los Angeles (California) Police Department, who presented an overview and talked about the technology in use and future goals of his agency.

He concluded that the LAPD believes criminal justice information should be for law enforcement purposes only.

This panel ended with a question-and-answer session, during which participants discussed global rules for collecting, using, and disseminating CHRI; how the National Crime Prevention and Privacy Compact Council regulates dissemination of CHRI for noncriminal justice purposes in light of State statutes; and more in-depth details of Florida's open records system.

## Privacy advocates

A "privacy advocates" panel discussion was next, moderated by Prof. Kent Markus, Visiting Professor, Capital University Law School. The three panelists discussed privacy and CHRI, and the role for privacy in the Internet Age.

Dr. John N. Woulds, Director of Operations, Office of the Data Protection Commissioner, United Kingdom, presented the international perspective on privacy protection. Dr. Woulds, who considers himself a "privacy regulator" rather than a privacy advocate, spoke about the European Union, and the technical barriers to the free transfer of information from one country to another.

The next panelist, Mr. James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology, discussed the impact of the new technology on the criminal justice system, policy conclusions that can be drawn, and what the implications are for privacy. Mr. Dempsey recommended, "As new systems are designed, it is possible to build in privacy and reinsert some of the fair information practices and principles."

In a frank presentation, Ms. Beth Givens, Director, Privacy Rights Clearinghouse, talked about the upsurge in identity fraud and criminal identity theft over the past several years. Ms. Givens' presentation focused on criminal identity theft, including a description of the crime and specific case histories; information about an ad hoc task force in California that has been studying how victims can clear their records; information on two legislative bills in California; unresolved issues of the information brokers; and some recommendations to help the victims.

The panel presentations concluded with a question-and-answer session that presented some follow-up debate concerning the Data Privacy Directive and the Safe Harbor, as well as other issues.

## Media perspective

Prof. Jane E. Kirtley, Silha Professor of Media Ethics and Law, School of Journalism and Mass Communication, University of Minnesota, covered the media's perspective on whether the its dissemination of CHRI should be regulated, and responded to questions from the audience. Prof. Kirtley stressed, "In this desire to protect the public from itself and to protect the public from the press, we are going to eviscerate the important rights of the public and press to engage in government oversight."

## Consumers and commercial providers of criminal history records

The question posed to the next panel — Should certain categories of consumers be allowed access to criminal history record information? — was addressed first by Dr. Donald F. Harris, President, HR Privacy Solutions, in his presentation, "The use of criminal history records by employers." He discussed the significant privacy concerns around relevancy, the quality and extent of notice that is provided, fairness in collection, secondary uses, and storage and retention of criminal history information by employers. Mr. Harris concluded that the current system is time-consuming, confusing, and costly for employers, and he strongly recommended guidelines for employers in this area.

The second panelist, Mr. Lawrence F. Potts, Director, Administrative Group, Boy Scouts of America (BSA), offered the perspective of a noncriminal justice user of criminal information. Mr. Potts stated his belief that organizations such as the BSA should have access to background information systems in order to ensure acquiring the highest quality in leadership and volunteers. He recommended passage of the National Crime Prevention and Privacy Compact at the State level; low-cost, high-speed, responsible access to criminal background check information; awareness that the cost of access for nonprofit organizations is an important concern; and uniform guidelines to access criminal background check information.

Mr. Jack Scheidegger, Chief Executive Officer, Western Identification Network Inc., moderated the Criminal History Record Consumers panel.

The final panel of the conference dealt with whether (and, if so, how) commercial providers of background information should be regulated. Mr. Emilio Cividanes, Partner, Piper, Marbury, Rudnick and Wolfe, LLP, panel moderator, presented an overview of the Individual Reference Services Group, and the self-regulatory efforts of that organization.

The first panelist, Mr. Peter L. O'Neill, Chief Executive Officer, CARCO Group Inc., presented an overview of the *Fair Credit Reporting Act*[4] (FCRA) as it relates to criminal history records and commercial providers of background information. He concluded his speech with recommendations for achieving the maximum benefit from the FCRA.

The second panelist, Mr. Stuart K. Pratt, Vice President of Government Relations, Associated Credit Bureaus, stated that the "specialized companies that obtain information and then aggregate it with investigative data through other traditional data sources, and provide that to the employer *are* regulated under the *Fair Credit Reporting Act*." In his presentation, he said the key is a "responsible system of managing criminal history information to make sure that even through the commercial marketplace, societal needs can be met."

[4] 15 U.S.C. §1681 *et seq*., as amended.

The conference ended with concluding remarks from the Task Force Chair, Mr. Robert R. Belair, thanking Task Force and conference participants. Special thanks were extended to BJS, Dr. Jan M. Chaiken, and Ms. Carol Kaplan, Chief, National Criminal History Improvement Programs for BJS, for financial support, leadership, and guidance. Mention and thanks were also offered to Prof. Kent Markus, who ably served as conference moderator.

# Day one: The challenges of privacy in the 21st century

## Welcome and keynote addresses

Welcome
*Gary R. Cooper*

Privacy and the future of justice statistics
*Peter P. Swire*

The role of confidentiality in collecting statistical information
*Dr. Jan M. Chaiken*

# Welcome

**GARY R. COOPER**
*Executive Director*
*SEARCH, The National Consortium for Justice Information and Statistics*

Let me read you an article that appeared in a Boca Raton, Florida, newspaper last month. If you are not already thinking about the issue of privacy, I think this will get you started.

This involves an incident that occurred in Boca Raton. The article reads, "Spanish River High School students attending Friday night's prom in the upper-class suburb had more to worry about than finding the perfect dress or tuxedo. They had to hope that their guests cleared a police check. To ensure a safer prom, administrators at Spanish River screened dates who are not students at the school, banning those they felt posed a threat. Seniors with nonstudent dates were required in advance to fill out a form listing their date's name, driver's license number, date of birth, grade in school or employer, employer's address and phone number, and the last school they attended. About 15 percent of the 500 people holding $100 tickets to the school-sponsored prom did not attend the Palm Beach County school."

The article goes on to say, "School officials told Spanish River senior Karen Miller Wednesday that her date did not pass the school police check. The news came after Miller spent $1,000 for a dress and shoes, plus the cost of a limousine, flowers, hairstyle, makeup, and other expenses. Karen's mother was furious. 'I can understand them not wanting troublemakers at the prom,' Barbara Miller said. 'But they shouldn't tell them 48 hours before the prom begins.' Karen was told later that her date, a Spanish River graduate with a discipline record, could attend since the school dean had agreed to keep an eye on him."

Is this an invasion of privacy, or is this a responsible action by school administrators who are attempting to maintain a secure environment for the children, and prevent some of the bloody activities that have taken place in schools around the country over the last several years? It is difficult to find the balance between the need of government and society to have information and the individual's right to privacy.

On that note, I want to welcome you to the *National Conference on Privacy, Technology and Criminal Justice Information*. This conference is brought to you through the joint efforts and partnership of the Bureau of Justice Statistics (BJS), U.S. Department of Justice, and SEARCH, The National Consortium for Justice Information and Statistics. My name is Gary Cooper,

and I am the Executive Director at SEARCH. For those of you who are unfamiliar with SEARCH, we are a criminal justice membership organization. We have one member from each State and the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. Each member is appointed by the State's Governor or executive officer. Our members have responsibility for the management of large justice databases, including the criminal history databases, at the State level. And they are also often responsible for the technology that moves this information around within the individual States, and between States and between the States and the Federal government. In addition to the State members, we also have eight members who we call At-Large members. They are appointed by our Chair. These members add a different perspective from those of our State-appointed members in that they are from the judiciary, academia, or local government. They are brought in to add a fresh view to our debates.

Since SEARCH's inception in 1969, we have advocated the application of advanced information and identification technology to improve the administration of justice through better management of justice information. The proper management of criminal justice information requires the development of laws and policies that strike a balance between government's need for information about people, and the individual's right to privacy and his or her ability to restrict access to personal information, and, for purposes of this conference, criminal justice information. As you heard from the article that I read, that balance is often hard to strike. The balance seems to shift from decade to decade. In the 1970s, policies were made to restrict access to information, motivated often by the fact that the data quality was bad. Moving to the 1990s, there are national efforts to improve the completeness and accuracy of justice records, and growing pressures to open up databases. We have sex offender registries in all States and the public is urged to access them and criminal history databases on the Internet.

For over 25 years, in partnership with BJS, and before that, with the Law Enforcement Assistance Administration (LEAA), we have examined and discussed trends in the development of laws, policies, and information practices as they change to accommodate the public and governmental demand for information and the privacy rights of individuals who are the subjects of criminal justice information. We have done this in several ways, including countless studies such as the one that is being presented at this conference. We have looked at the right of access, the media right of access, public employer/private employer rights of access, and access to juvenile justice information, and we have published extensively on these issues.

Since 1970, SEARCH has published more than 40 detailed publications specifically focused on privacy. In addition to issue analysis, we have proposed model legislative

standards upon which most of the State laws are based that regulate the collection, use, and dissemination of criminal history records. Most of those laws can be tracked directly to the legislative standards, in SEARCH's *Technical Report 13, Standards for the Security and Privacy of Criminal History Record Information*.[1] They were also influential in the development of the LEAA regulations,[2] which came out in the mid-1970s. This was the first time there was national discussion about standard access and dissemination of criminal history records. We also monitor the introduction of practices and policies resulting from these regulations and State issues. Those of you in State criminal history programs — I want to thank you for your constant response to our countless surveys. I know it is a lot of work, but I think it helps build a body of knowledge regarding this important issue. In the last decade, we have also convened 10 conferences that focused in whole or in part on privacy.

Now, with advances in technology — particularly browser technology — society's demand for information is increasing exponentially. With sophisticated delivery mechanisms like the Internet and the World Wide Web, and with the movement in the justice field to sharing information in an automated fashion among the different disciplines within the justice system and between the justice system and other agencies of State, local, and Federal government, and with justice information now residing in private and unregulated databases, the debate around criminal justice information privacy becomes much more compelling and much more complicated as you will hear throughout today and tomorrow.

We have 44 States represented here today. We also have representatives from Canada and England. Thirty percent of you are from the law enforcement field; 16 percent of you are from the courts; and 4 percent are from corrections. Prosecutors, defense, and juvenile justice representatives make up 2 percent. That means 48 percent falls into that category called "Other." When we started these conferences in the 1970s, usually 2, 3, or 4 percent were classified as "Other." The scope of the group that has interest or that is affected by privacy policy has broadened, and we certainly welcome all of you to the conference.

I would like to recognize several people whose assistance and leadership on this project proved invaluable. First, Dr. Jan Chaiken, the Director of BJS, for his commitment to dealing with the issue of privacy. I would also like to thank Carol Kaplan, who is the Chief of the National Criminal History Improvement Programs for BJS. Carol and I have dealt with this issue since the mid-1970s. She has been a tireless analyst and leader on these issues. I'd also like to recognize SEARCH staff — Sheila Barton, who is our Deputy Executive Director responsible for the Law and Policy Program; Eric Johnson,

[1] *Technical Report No. 13: Standards for the Security and Privacy of Criminal History Record Information*, 3rd ed. (Sacramento: SEARCH Group, Inc., 1988).

[2] 28 C.F.R. § 20.01.

who works for her and worked hard in helping bring this conference together; and Terri Nyberg, my assistant, who helped with registration and bringing all of the materials to you for the conference. I want to also recognize Dr. Alan Westin, Professor Emeritus from Columbia University. Alan is an internationally recognized expert on criminal justice and other types of informational privacy issues. I want to thank him for his effort and hard work on this project. I want to thank Robert Belair, Task Force Chair, and Dr. John Woulds, Director of Operations for the Office of the Data Protection Commissioner in the United Kingdom. I want to thank the Advisory Committee. Many of them will be speaking today, although they are not listed in your registration materials; however, they will be listed in the report when it is published. And lastly, I want to thank the speakers who have taken the time from their busy schedules to be with you today and tomorrow.

I now want to introduce to you Kent Markus, who is the conference moderator. I have known Kent for 6 or 7 years now. I met him when he came to the U.S. Department of Justice *after* the passage of the *Brady Act* and the Department was faced with implementing that Act. They put it in Kent's hands and he did a marvelous job. While getting to know Kent, my responsibility was to represent SEARCH and represent different States' points of view on issues regarding the creation of a national instant check system. Kent was easily accessible, and was very open to ideas from the States and the local agencies on these and other issues. He was very responsive to the States in his time with the Justice Department.

So if you would, please join me in welcoming and meeting your moderator, Kent Markus.[3]

[3] ***Editor's note***: Mr. Markus' brief remarks, and those of most of the individual panel moderators, are not included in these proceedings.

# Privacy and the future of justice statistics

**PETER P. SWIRE**

*Privacy Counselor to the President*

It is a pleasure to be here and to have worked with Alan Westin and Bob Belair, both of whom will be speaking this morning. It is also a pleasure to be here with all of you who are considering justice statistics. I have done a lot of work with the U.S. Department of Justice (DOJ) in the last year and a half since joining the Administration, and the degree of expertise and energy that many of you have brought to this effort is impressive. I think it bodes well for the final report and for its implementation.

Today I am going to talk about the free flow of information in society, which is a noble goal.[1] I am going to talk about what the Administration has been doing in the privacy area, how the Federal government is seeking to be a model on this issue, and the area of public records in general as I try to provide a context for how privacy discussions are proceeding today. I will then have some concluding thoughts that apply more specifically to justice statistics.

## Free flow of information

We are living in an Internet world where we have a noble goal of ensuring the free flow of information throughout society, but what does it really mean? Is it really free in that sense? For security purposes, do we want a free flow of data to hackers in society? For intellectual property, such as copyrights and trade secrets, do we want a free flow of information of those trade secrets to copyright pirates? In the privacy area, do we want a free flow of information to intruders, people who look into the parts of our lives that they are not supposed to be looking into? In all of these areas, we see that there are many wonderful flows of data from the Information Superhighway, but some of the new flows of technology present conflict, particularly in the area of privacy.

Let me give you an example. It is a common practice in many communities for police to have unlisted telephone numbers and addresses to make it more difficult for people — particularly offenders who have been locked up by these police officers — to locate them. Officers often want to make it more difficult for people to come to their homes to threaten them or their families. This issue came to a head in Durham, North Carolina, not too long ago, when law enforcement officers were concerned about having their home addresses and

[1] Mr. Swire's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/justicestats053100b.ppt.

phone numbers posted on the Internet. I use this example because for many of you working in the areas that you do, you may understand the concerns police officers may have regarding their personal safety when a dangerous felon has been released from jail. After debate between the City Council and the Police Chief in Durham, North Carolina, the City Council decided to make the name a hidden field on the city property records. That way, if police officer Joe Smith had a property record on file, it generally would not show who owned the property. These were tax records that showed whether the taxes were paid, but did not show Joe Smith's name. However, Durham County officials disagreed with this policy; the Durham County Registrar of Deeds, over the police officers' objections, decided to keep the property owners' names listed on their tax records and posted that information on the Internet. The County Tax Assessor then planned to post the blueprints of houses located in the county on the Internet. This would include the blueprints of the houses, for instance, of the police officers or other public officials and for officials who have some basis for concern that there may be people who could cause problems for their families. Having these sorts of policies, particularly policies that could conceivably present security problems for public servants, raised concern.

The question that we should ask is: Which flows of information make sense? Out of all the new technologies that enable us to post an increasing amount of information on the Internet, should they all automatically be posted to the Web? Should they automatically be available to people just because they are available in a paper-based world? When should there be some sort of thoughtful consideration, discussion, or debate of whether personal information should become increasingly available on the Internet? The blueprints to the property records in the county were apparently available in a paper file somewhere down at the courthouse, but it was not an easy or standard thing for a member of the public to obtain. Someone planning an attack on a house probably would not have gone to the courthouse and risk being seen looking at the blueprints of a police officer's house. This is the sort of framing of context required when asking which flows of information we want.

## Administration privacy policy

Let me describe what the Administration has been doing on the privacy issue in general. There is a lot going on in this field, not just in criminal justice statistics, but in many different areas of public concern. The Administration's privacy policy in the private sector has been to support self-regulation as a general principle to try to push industry to create good structures for how they handle the information. We have said that there are certain sensitive categories of data that deserve legal protection. And again, we are talking primarily about the private sector — your medical and genetic data, financial records, and bank records. We have also supported legislation to

protect children who go online. We have said that government should lead by example in this area.

In the Internet area, there has been a great deal of conversation about what the rules should be for the Web sites when you go browsing on the Web. We have seen a remarkable change in the number of commercial Web sites that have privacy policies in place — from 15 percent 2 years ago to 88 percent today, according to a recent survey. The quality of the policies has continued to improve — and a better choice for individuals to say whether they want their information transferred to others. We want to have incentives for companies that employ good information collection and dissemination practices. If there is going to be legislation in the future — and there are many proposals circulating — we would want to make sure that the companies that have stepped forward and have put good policies in place are recognized. There is an increasing concern about the people who are in the Internet space who have no privacy policies, who may be giving a bad name to other companies, and what is it that we are to do about them?

A major initiative and some proposals are coming to surface in the medical arena. The initiative would affect police departments, among others. In 1996, Congress passed a law that said that Congress should pass another law by August 1999 that would include comprehensive privacy legislation for medical records. When Congress was not able to act, President Clinton in October 1999 announced proposed privacy regulations with the Secretary of Health and Human Services. And then there was a comment period in which 53,000 comments were submitted on the proposed rules. You all can help. We are reading these and there is a process within the Department of Health and Human Services and within the government to thoroughly examine these public comments. In the State of the Union address in January 2000, the President promised to make the regulations final this year. Therefore, we are hard at work on finalizing these medical records regulations. The core of the medical records privacy initiative reflects familiar ideas of fair information practices, which also exist in the criminal records area:

- There should be notice of how your data is being used by your doctor and your hospital.
- There should be patient choice before your data is used for unrelated purposes, such as marketing.
- A patient should have access to his or her medical record to make sure that there is no information that could lead to an inaccurate diagnosis or other problem.
- There should be security around medical records so that people are not breaking into them.
- There should be some sort of enforcement and accountability if people are breaking the privacy rules.

These are principles widely accepted as fair information practices in many settings, and we are building them into the medical records. The regulations have many other provisions, and there is one that may be of interest to you all: What are the rules going to be for law enforcement access to medical records? The police officer shows up at the emergency room and says, "I want to see all the records to see who has a knife wound." Maybe you do not get all the records. Maybe you get the knife wound records in an emergency. How do we work out those sorts of different concerns in that area?

When it comes to genetic discrimination, the possibility exists that a tremendous amount of information about individuals will be opened up. In February 2000, President Clinton issued an Executive Order that prohibits Federal agencies from using genetic information in hiring decisions or promotion decisions. If you are a Federal employee, your boss cannot scan your genetic code to see if you are more likely to develop disease or illness. We have also called for legislation that would similarly affect the private sector. The Vice President renewed that call just over the weekend, saying the same protections should exist regarding hiring in the private sector, and that these rules should also apply for the purchase of health insurance. In the law enforcement context, I would like to raise the question: What will the public concerns about DNA databases be over time? If individuals' DNA samples are being kept, what sort of safeguards will have to be in place to let that DNA data be made available for law enforcement purposes, but clearly wrapped up very carefully and not made available for other purposes? That is a challenge that we have as genetic information becomes more powerful and more available in ways that it previously was not.

Last year, as part of the big legislative overhaul of the financial system, there was a whole section on privacy in the *Gramm-Leach-Bliley Act.*[2] You will get notice of your uses in the banking records; you will have the chance to decide whether your account information goes to outside companies. And there are enforcement provisions just like for other banking rules.

The President recently announced a plan to fill in the gaps in last year's law. So we say there should be choice before it goes to the affiliated companies because there are so many affiliates in a modern holding company. We say that some data is especially sensitive and deserves an optimum level of choice. Medical information that is circulated in these holding companies is one example.

In 1998, the President supported and signed the *Children's Online Privacy Protection Act.*[3] The rules were issued and took effect in April 2000. The key component of the legislation is that parents should give consent for children under age 13 to provide personal information.

[2] Pub. L. 106-102, codified at 15 U.S.C. § 6801-6810.
[3] 15 U.S.C. § 6501, *et seq*.

An identity theft law was passed in 1998 making it a crime to steal someone's identity for use on the Internet. There were "pretext calling" provisions in the *Financial Services Modernization Act of 1999* so that people cannot pretend to be someone else in order to access financial records.[4] There is also — and the Administration did not take a position on this — a provision for motor vehicle records used for marketing purposes. There was a new opt-in provision that Congress included in a transportation bill last year.

Looking at all of this, we see that there is a significant level of legislative activity on privacy. There is a significant level of public concern for the issue. You will hear this in various ways. One example is a *Wall Street Journal* poll conducted in September 1999. The *Wall Street Journal* asked, "What do you fear most in the coming century?" They included some pretty scary things — global warming, terrorism, nuclear holocaust — some things that I would consider to be pretty big worries in the scheme of things. When Americans were asked this, out of 12 possible answers, the one that came out first or second from 29 percent of the answers was erosion of personal privacy. None of the other answers reached above 23 percent. Erosion of personal privacy was at the top of the list for the largest number. This is a sign of significant concern by a wide number of Americans. So given this activity, given the concerns, our Administration, and I think all of you, are seeking this balance that has already been mentioned today. That is, among multiple goals, there should be privacy but also the goal of public safety, in which law enforcement officials have such an important responsibility.

## Government as a model

We have the Internet. We have electronic commerce. We are trying to promote these and keep the economy growing. We also do not want certain information flows. So again and again the question is: Which uses of data are not beneficial? Which kinds of data really do help? And after we consider it, which are the ones that should not flow so freely for some of the reasons already stated?

Let me give you a sense of what we in the Federal government have been trying to do in this area because we should be a model, and we also have a certain responsibility as the government to take care of people's personal data. In doing this, I will touch on what we have done for Federal Web sites, for computer security in the government, development of privacy impact assessments, and the importance of oversight mechanisms to make sure these initiatives actually work.

One of the things citizens want to know when they are on a government Web site is how the government is using their data. In June 1999, the Director of the Office of Management and Budget (OMB) issued guidance for all Federal agencies, saying that they should have clearly posted privacy policies that

[4] Pub. L. 106-102, 113 Stat. 1338 (1999).

explain what they do with data at the government sites.[5] By December 1999, when the time allotted for implementation was up, all Federal agencies at all of the required Web sites had indeed clearly posted privacy policies. This is something for you all to consider for your Web sites when you are collecting or using personal information. The first step is to give notice of what is being collected and how it is used.

People think privacy and security are somehow related. Let me try to make my opinion clear on this. First, good security is absolutely required in order to have privacy. If we have weak security, if anybody can just tap into the databases, that will allow access to the tax records, to criminal investigative files, and to whatever the government has. Weak security provisions are like not putting a lock on the door. It might even be like not having a door, just letting anyone right in. Good security stops the hackers and the unauthorized users. It stops those third parties who are not supposed to be able to come into the building. However, good security is not enough. It is not sufficient to answer the privacy question. The privacy issue also involves what an authorized user can *do* with the data. Suppose you have received some data over a super-encrypted line using the strongest keys available. And now you have received the data. And now you post it on the Internet for everybody to read. We had great security. We sent that data to you in an absolutely secure form. The question is what do you do with it once you are allowed to have the data in your hand? Privacy policies govern the authorized users. It governs the people who are supposed to be able to have it, and the question is, for what uses and for what purposes?

That leads into this idea of privacy impact assessments (PIA), not as a horrible bureaucratic thing that crowds out the world, but as an idea that we want to try to build good security into our new information technology (IT) system. There should similarly be an idea of building good privacy mechanisms, especially into the new or revised systems. The Internal Revenue Service developed one of these over the last few years, and it has been improved by the Federal Chief Information Officers' Council as a best practice. We are now working with other agencies to do this. The Federal Bureau of Investigation is working on a PIA. BJS, I understand, is in the process of considering this. What I have in mind with these kinds of assessments is a structured set of questions. What laws apply to this data? Does the Federal *Privacy Act of 1974*[6] apply? Are there other laws that apply? Wouldn't you like to know if you are complying with the law before you build a new system? What agency or other policies apply?

Another aspect of privacy impact assessments is what I call the "Friends and Family Test." If you go home at night for dinner and sit down with your spouse or with your friends on Saturday night, and you

[5] *See* www.whitehouse.gov/omb/memoranda/m99-18.html.

[6] 5 U.S.C. § 552A, as amended.

describe what you are doing with your data, are they comfortable with that? Do they say, "Good, that is a good thing? We are glad that you are doing that. That is the right way to handle that." Or, instead, do they look at you with that sort of odd look on their faces? Do they say, "You do that? You tell people that?" And if you get that reaction from sensible people that you know in your life, then there is reason to be a little careful. It is a reason to think twice about whether what you thought was a good idea, might deserve a little extra thought. So in the privacy assessments we are describing, it is (1) comply with laws, (2) comply with policies, and (3) comply with common sense, and do a "stop, look, and listen" as you build these new systems because the data is going to get out there.

The other thing we are discussing as we build government systems is oversight mechanisms. What sort of second looks will there be because there are public concerns about how the data is being used? We know that these new databases, these new flows of information, particularly the Internet technology, often achieve important public safety and other goals. These information flows get data to people who need it, and the data is going to save lives and stop criminals. But what are the built-in mechanisms? In our enthusiasm to meet one goal, what are the ways we have to build in other goals? When will privacy considerations come up in the process? At what point will you make sure that someone is following the privacy rules you previously established? In the absence of oversight mechanisms, there may be public questions. There may be questions from your legislature or from citizens: "Are you really doing this?" In response, we have been setting up boards, review committees, consulting committees — people who have some interest in asking the questions. That is something that we have been doing in a number of settings.

## Public records

What we have done is talk about the free flow of information. We have talked about what the Administration is doing generally. We talked a little bit about the government as a model. Let me now talk about something a little closer to the issues that many of you are struggling with — the area of public records. The idea is that records have traditionally been open to the public. Many court records and certain kinds of criminal records are in this public records category. Two years ago the Vice President said that we should have a dialogue with the States on the issue of public records, and my office has been coordinating with the Washington offices of the Governors' Association, the State Legislatures, and all the rest, to try to make sure that there is a dissemination of information about these topics. I am going to talk about the recent Supreme Court cases briefly, and then I am going to focus on a type of Federal public record where we are doing some work — bankruptcy records.

This last year, the U.S. Supreme Court had two privacy- and public records-related cases. The

first one is *Los Angeles Police Department v. United Reporting Publishing Corp.*[7] It involved a State law that had stricter limits on marketing of arrest record information than it did for other uses, such as media use. This was challenged on the basis that public records are public records and that you cannot choose the purpose for which those records are used. The Supreme Court upheld the State law. It said that under the Constitution, the State could pick and choose in this way. In another case, *Reno v. Condon*,[8] there was a Federal statute that limited how States could release motor vehicle records and drivers' records. In this case, once again, the law was upheld against the Federalism challenge. In both of these cases, many observers thought that the privacy interest would not win, that the laws would be struck down. In both cases, and in other cases over recent years, the Supreme Court has shown itself to be quite sensitive to privacy concerns. So as we are developing laws and jurisprudence in this area, these cases form a backdrop that suggests that the Court is at least willing to listen carefully to the privacy arguments as various laws come up in the area.

Let me talk about bankruptcy records. Bankruptcy records are in the process of moving from the paper files to the Internet, and as that is happening, we have started to ask some questions. You can go to the courthouse today and get someone's actual bank account numbers from their bankruptcy file, which is a public file. You can get the numbers they have at their local bank or brokerage house. You can get their social security numbers. You can get a lot of other information that has been in those files traditionally. Should we place these numbers online for millions of Americans? If you are putting the actual bank account numbers of millions of people on the Internet, doesn't that pose a high risk for identity theft, for fraud, for people using those bank account numbers as targets for crime? We have concerns about that and the President last month asked the OMB, the Treasury Department, the Justice Department, and the Executive Office of U.S. Trustees, to issue a report on bankruptcy and public records. We are going to have the report done this calendar year. It is one area where the Federal role is substantial; therefore, we have taken it as an opportunity to study this public records area. As you have records that are public, it suggests again maybe not everything works just the same way as it does online.

Many flows of information in the Information Age are good. It brings many benefits to society, but not all flows are positive. You are not against progress because you think 1 out of 100 or 1 out of 1,000 new flows of information perhaps should be limited. We should take advantage of new technologies to promote public safety, economic growth, public education, and other values that come from this fantastic flow of information. But there should also be thoughtful

---

[7] 528 U.S. 32 (1999). *See* www.freedomforum.org/fac/99-2000/lapd_ind.htm.

[8] 528 U.S. 141 (2000). *See* www.aclu.org/court/reno1.html.

consideration of that small subset of flows that are technically possible, but perhaps not advisable. Should the home addresses of vulnerable people — such as rape victims or people who are under protective order — be made available to the public necessarily? Should the bank account numbers of individuals be posted on the Internet for criminals to see? In the justice system, improving technologies makes many of these new flows less expensive than before, and more practical. You can share with officers across the country and agencies in other States in ways that you couldn't before. But as you do this, I think it makes sense for your practices to meet the requirements of the applicable law, and the policies and the confidence of the public in how you are using the data that has been entrusted into your hands. And so the way that we have talked about that is privacy impact assessments. Whether you call it by that formal name, complying with law and policy is something on which we can agree. In the Information Age, there will be a constant stream of new issues as technology changes. Which of these information flows are good? You cannot just have a conference this year. You are going to need one again with the new technology changes next year and the year after. President Clinton has asked, "How do we keep our traditional value of privacy in this area of new technology?" The Fourth Amendment says that people should be secure in their homes, their papers, and their effects. What does the Fourth Amendment mean as far as being subject to reasonable search? What does it mean in the Internet Age when the data is available in new ways? The answer to these issues will be in the goodwill of all of us who build:

- New information systems.
- New medical systems for your psychiatric records and arrests.
- Genetic systems that have your DNA in it.
- Financial systems that list every purchase you have ever made in your life.

Should that be made available to your neighbor or your boss? The government in general needs to think about how to build these systems effectively. The justice systems in particular, and this is your charge, need to think about what is wise to do in these areas. From our side, and I think from your side, we look forward to this challenge of how to make the values of America, of individuality and autonomy and privacy and freedom, real in an age when information flows are so new. Thank you very much.

## Question-and-answer session

**Q:** You mentioned at one point the issue of building privacy protection into intersystem design and system development. I think that is a very important point. Too often we have found, certainly in the United Kingdom in the past, that people have developed systems with security in mind. But as you rightly pointed out, security is only part of privacy protection. Security is not sufficient to ensure good privacy protection. It is interesting that we have a couple of examples in our country of

commercial software and system developers who are now developing methodologies to build privacy protection into system design at the beginning. I think this is a very interesting and important development. It is something that we as a regulatory agency are encouraging, but have not been able to achieve until now. It is interesting, too, that these companies are doing this principally for commercial reasons. They see that they can steal a commercial advantage on the competitors by being able to develop systems that take proper account of privacy protection in the first place.

My question is to what extent, if any, the Administration policy on privacy protection has been influenced by developments in Europe, and particularly, the European directive on data protection?

**A**: (Swire) In terms of the European Union, I actually have some news that I got in the car ride in this morning. The European Union, Article 31 Committee, unanimously approved the "Safe Harbor" approach for the United States and Europe. It is a culmination of more than 2 years of intense discussion with Europe on the privacy issue. The details of that will be announced at the Summit that the President is at today in Europe with leaders there. The upshot of that would be that it clarifies the rules under which data can flow about individuals from the European Union to the United States. I think we are all very gratified to have a successful vote on that to allow that to go forward. In terms of the United States being influenced by the European Union, certainly I was influenced by study of that. I wrote a book for the Brookings Institution on that issue before coming to work in the government sector. I think it is clear that there was an educational role for many people who have worked in the privacy area that was developed in the course of discussing these issues with Europe. I think that if you look at where these privacy issues of legislation are coming from, the timing of it and where the instincts of privacy come from, it has been an authentic, domestic American view. So the American area has focused very much on sensitive areas of data — children who go online, medical records, and financial records. It has been the tradition of the United States to look at the sectors, including criminal justice record sectors, where there are special sensitivities for data. So I think we have spent a lot of time in this country saying some data is really especially sensitive. We have to be very careful about it. Other data is much closer to the free flow of information. I think that was true in the *Fair Credit Reporting Act* that was passed in 1970. I would say that it has educated us by engaging with Europe on the issues, but these issues of privacy have really come from the American experience.

**Q:** My question is related to privacy within our inmate database. I want to share with you a request, and I would like your feedback on the appropriateness of releasing that data. The request was from an Ohio university for the addresses from our almost 47,000-

inmate database. The request was from a professor who is doing research for the United Way, which wanted the information to identify locations for targeting funding for programs for parolees. I suggested that I could supply the aggregate data by census track, giving them numbers of inmates in particular census tracks, rather than to individual addresses. However, I was advised that that is a public record and that I should release the information. I did not tell that to the professor. I simply advised that I would release the aggregate data. But I do need your feedback on that.

**A:** That is a question that illustrates several points that we will be facing. One is that when people make a request for individualized data for research purposes, it can often be released in aggregate form and the research will work just as effectively. I do not know the facts of the case, so I am not commenting in particular on the United Way request. But if the idea is which neighborhoods need help from the United Way, census-tracked information sounds like a very sensible response. So that is one point. A second point is that you need to know what your local laws and policies are. I happen to know a little bit about the Ohio public records laws and you can probably get my research notes under the Ohio public records laws as a professor. Ohio has an extremely wide-open statute compared to many other States. So it may well be as a matter of statute in Ohio that they have the legal right to get the individualized data. That would just be a matter of researching the local statute. Even if they have the right to get that data in an individualized way, you as a public official may have discretion, depending on the statute, to suggest the census- tracked approach, the aggregated approach. You might say, "This seems responsive to your request, and here is why we have these concerns about individualized data and the complaints that we would get. Given your research and your stated goals that you have announced, will this do?" The researcher might say yes. And that is a way to handle it; even where they have a legal right to it, they may decide in their discretion that the census-tracked data is just fine. For public records, more generally, each State has very different rules, and sometimes it is different for subsets of records. In the bankruptcy example, the Administration at this point is seriously studying whether we should change some things that used to be in the public category and place then in the private category. That sort of discussion is likely to happen in a lot of other places. And it is OK. Even if it was in a public file 200 years ago, that does not mean as a matter of Constitutional law that it has to be in a public file today. Those are decisions that society can make that we reshuffle. We may make some things public that we did not make public before. So in the *Megan's Law* kinds of cases, there have been decisions to make things — in this case, sex offender files — more public than they were before. In other cases, you might decide to make certain fields less public. That is subject to your debate and your wisdom.

You are not necessarily handed something from 50 years ago that you have to follow slavishly.

**Q:** I am interested in the Individual Reference Services Group (IRSG) voluntary agreement that was established in 1997 and that the Federal Trade Commission entered into with 14 information brokers. From a privacy advocate standpoint, I was quite disappointed that it did not strongly adhere to the Fair Information principles. I notice that you did not mention that particular development in your remarks as things that have been accomplished by the Administration. I am wondering if there has been any thought of revisiting the IRSG agreement and looking at it in terms of the Fair Information principles and also in terms of the advances in technology.

**A:** The IRSG is comprised of companies that have, for a variety of reasons, information about many individuals. There has been a recent issue about the extent to which some of those records are covered by the financial privacy regulations that were issued recently. In November 1999, the U.S. Congress passed a law updating the financial services. There are provisions about Social Security numbers and other account number information. The seven independent agencies issued regulations under that, which came out in final form recently. There has been discussion in the media over whether the ISRG members and some of their activities are covered by those new regulations. There has been discussion about whether there is going to be litigation about the rules because of that coverage. So the extent to which the new financial privacy rules will turn out to affect those companies is a live issue.

**Q:** I have a question about Federal Web sites. You mentioned that they are supposed to indicate what their privacy policies are, but could you comment about Federal Web sites capturing information about visitors to their Web sites or requiring visitors to their Web sites to provide any information about themselves?

**A:** The rules for capturing information are covered by the *Privacy Act of 1974*. The key thing is if it is called a "system of records" that is being created by the agency, then the *Privacy Act* kicks in and the usual rules of the *Privacy Act* apply. On the other hand, if you are collecting logs that have dynamic Internet Provider (IP) addresses, and it is just a log of visitors in that way are even static IP addresses, but if you are just running your logs like a normal Web site, our position has been that that does not create a system of records and you do not have to kick into the *Privacy Act*, even though in theory with enough forensic work you might be able to backtrack and find out who some of the visitors were. So the issues really come down to when it is a "system of records," and once it is, the *Privacy Act* applies.

**Q:** Could you explain a little more what it means you can do or not do when the *Privacy Act* kicks in?

**A:** The *Privacy Act*, which applies to Federal agencies or to contractors who are working for Federal

agencies, has rules of notice. It has rules of access to the records so that the individual can see what information the government has about them. It has rules about the information being limited to that agency, except if it is under statutory exception or routine use. And the routine uses are the uses that are put out in the *Federal Register* notice when you create the system. When you say, "As a routine matter, we share we these sorts of folks, but not these other sorts of folks." So there is a certain notice to the public at the time that you create the system, which is in the *Federal Register*. There is a notice to the individual at the time that you actually interact with the individual, a shorter notice. If you look at the back of a W-2 or W-4, you will see the *Privacy Act* statement and it will describe how the information is being used. So we have notice, we have limits where it goes to, we have access to the records, the ability to correct the records if there is a problem, and civil and criminal penalties if the agency officers do not follow that. Those are some of the principle requirements under the *Privacy Act*.

**Q:** Earlier you were talking about enforcement mechanisms as far as Federal agencies go. I am thinking about Federal employees, especially law enforcement agencies. They have a lot of access to private records, just like IRS employees do. A couple of years ago, as you know, there was a huge issue of IRS employees surfing the databases. I can see how this would also be a temptation for law enforcement agencies at the Federal level. The IRS ended up setting up a really elaborate training program to prevent this. Are we going to have to look at this from a law enforcement point of view as they get more data?

**A:** What occurred with the IRS were some actions in response to the browsing concerns of the IRS, looking at a celebrity's tax records. That was a real example. There were training programs instituted as you said. There were new criminal provisions that clarified that it was a crime to be looking at these records without authorization. So those were a couple of steps that were taken at that time. I am not aware of us having taken any position on whether those criminal sanctions should be extended further. I am also not aware of any recent reports of improper use of the data by Federal law enforcement officials. There had been substantial reports, a substantial number of IRS employees improperly using the data. We are most tempted to try to do something about it when the problem has a factual basis.

**Q:** So the law specifically applies to IRS employees. As far as you know it does not apply to Department of Justice or FBI employees?

**A:** I believe the statute is tied to looking at tax records. That is what I think triggers it.

In terms of looking at criminal justice information and law enforcement access to it, there are procedures in place in the systems used by the FBI and the State and local agencies to audit and control access.

**Q:** I am a policy advisor to the Office of Justice

Programs (OJP). I wanted to highlight the fact that OJP has been working on privacy impact assessment guidelines. We have been working with the FBI and the governments of Canada and the United Kingdom to develop these guidelines. In working with the States, we run into a little bit of resistance from some of the chief information officers (CIOs) who are concerned that the DOJ may be going off in a parochial direction and it is not being properly coordinated with what the Department of Health and Human Services (HHS) and some of the other agencies are doing. My question for you is what are the Office of Information and Regulatory Affairs and the White House doing to coordinate the different approaches by the Federal government to privacy impact assessment guidelines, and coordinating the Federal positions with the States, particularly the CIOs?

**A:** The Federal CIO Council has taken it on as a project to try to work on privacy impact assessments and their CIOs from all of the departments that are included in that process. The Federal government is a pretty big place. Sometimes people have to speak up and let us know about certain issues before we are aware of them. When we found out about lack of coordination, we got the people in the room together and talked about it. For instance, in the process of the HHS privacy regulations, we worked extensively with Justice and HHS officials to try to make sure that all the different concerns are built in there. If there is a problem of that sort, contact my office and we will see what we can do. Also, John Bentivoglio has a coordinating role within the Justice Department. He is a spectacular person to work with. He is also very effective in that coordinating role. In terms of the States, I think it is fair to say that we might need to find more ways to ensure that there are effective discussions. But sometimes if the State's CIOs talk to counterparts on the Federal side and see how things are being solved, that might be one path toward seeing ways to go forward.

# The role of confidentiality in collecting statistical information

**DR. JAN M. CHAIKEN**
*Director, Bureau of Justice Statistics*
*U.S. Department of Justice*

I am the Director of the Bureau of Justice Statistics (BJS), U.S. Department of Justice.[1] I know all of you here today are charged with responsibility related to confidentiality of information. For employees of Federal statistical agencies, it is a constant preoccupation. In the Federal government, there are about 70 organizational units that collect and publish statistics. In each department, one of those units is the principal statistics agency that is coordinated through an interagency council on statistical policy, headed by a person with the title of chief statistician of the United States. She is in the Executive Office of the President in the Office of Management and Budget (OMB). Some of the major Federal statistics agencies are the Bureau of Labor Statistics, the Census Bureau, the National Center for Health Statistics, the National Center for Educational Statistics, the Internal Revenue Service, and the Bureau of Transportation Statistics. BJS is the statistical agency of the Justice Department, but the Federal Bureau of Investigation (FBI) also collects statistical information, as does the Immigration and Naturalization Service (INS); BJS is the representative of those on the interagency council.

One of the functions of Federal statistics agencies is to sponsor research and conferences, like the one today, on issues related to privacy and confidentiality.[2] The type of research we sponsor includes public opinion research, which you heard this morning. We are very proud to be a sponsor of that, as well as technical work on threats to confidentiality of data and on methods that can used to protect against those threats. Recently, the Federal statistics agencies joined with other Federal agencies and commissioned a panel of the National Academy of Sciences that looked specifically at how to maintain the confidentiality of statistical information.

Privacy or confidentiality issues are probably sitting in the center of your desk. As a member of the general public, this topic would probably not be on your desk — it might be in the bottom rear of one of the file cabinets. If you are not the head of your agency, I want you to think about the person who heads your agency and the

[1] At the time of the conference, Dr. Chaiken was Director of BJS.

[2] Dr. Chaiken's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/privacy2.ppt.

extent to which privacy or confidentiality issues enter into that person's deliberations. I can tell you that the heads of Federal statistics agencies are concerned and directly involved with issues of confidentiality at all times. We constantly review our activities. The Director of the Census Bureau, Ken Prewitt, and I have exchanged about three letters back and forth this year concerning confidentiality issues, and I am sure that you are aware that the year 2000 is not a quiet year for the Census Bureau. When I say letters back and forth, they were not one-sentence correspondences — they ran from 3 to 15 pages each. This is a random snapshot of how much attention we pay to privacy issues. We also sponsor and expend resources on our interviewer manual. It is one thing to have policies; it is another thing to enforce them in the field and make them actually happen. I personally attend some of the training for our field representatives, and their supervisors meet regularly. I also personally attend some of the supervisors' meetings. I think that would be normal for a statistical agency head.

## Strict confidentiality statutes

Statistical agencies are subject to various laws and regulations established by the chief statistician that I mentioned. Some of these laws and regulations apply to all statistics agencies and their employees. Others apply to a variety of research and statistics agencies and their staff, contractors, and grantees. These confidentiality statutes are very strict, and they provide for penalties like 5 years in Federal prison for violating their conditions. Sometimes when I am trying to deal with some of these confidentiality issues I ponder what it would be like for me to appear in our own data files of people prosecuted by the Federal government. Confidentiality under the Federal statutes applies to identifiable data. Of course, it is the business of statistics agencies to circulate, disseminate, and share unidentifiable data, so some of the trickier issues arise with knowing what falls in the identifiable category. In any event, data records that have clear identifiers, such as name, Social Security number, address, and so forth, are clearly deserving of confidentiality protection. There are also regulations about keeping statistical information secret until it is released to the public. That is a different issue and is not related to the confidentiality of the records. The existing legal structure is a patchwork of different requirements. The statute applying to BJS has particular provisions that are pertinent for collecting information from prisoners and arrestees. I am going to read you this statute because I know a lot of you receive funding from BJS or the National Institute of Justice or the Bureau of Justice Assistance. As I read this, you will see that it applies to you also.

"Except as provided by Federal law, no officer or employee of the Federal government, and no recipient of assistance under the provisions of this Chapter shall use or reveal any research or statistical information furnished under this Chapter by any person and identifiable to a

specific private person for any purpose other than the purpose for which it was obtained. Such information and copies thereof shall be immune from legal process and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for the purpose of any action, suit or other judicial, legislative or administrative proceedings."[3]

For us, this means that we can't provide any of the identifiable information that we collect to our friends in the FBI or elsewhere in the Department of Justice. Now this is quite an old statute and it specifically addresses criminal history information. So I am going to read this next passage to emphasize the various shifts in uses of criminal history information that have occurred. Here is what the law says:

"All criminal history information collected, stored, or disseminated through support under this Chapter shall contain, to the maximum extent feasible, disposition as well as arrest data where arrest data is included in it. The collection, storage, and dissemination of such information shall take place under procedures reasonably designed to ensure that all such information is kept current. The Office of Justice Programs shall assure that the security and privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes. In addition, an individual who believes that criminal history information concerning him contained in an automated system is inaccurate, incomplete, or maintained in violation of this Chapter shall, upon satisfactory verification of his identity, be entitled to review such information and to obtain a copy of it for the purpose of challenge or correction."[4]

I think that wording has applied all the way back to the beginning BJS. So it is remarkable to me that a number of the issues that were addressed in the public survey done in conjunction with this conference were already considered by those who put together this legislation. It also seems that the assurances that are offered remain matters that members of the public care about — for example, that people can see and correct their own criminal history information.

I know that all statistics agencies are aware of these requirements, but at BJS we are particularly aware of these requirements because we are surrounded by attorneys, and if there were any criminal violations of this statute by any employee of a statistics agency, it would be DOJ that would prosecute. Moreover, the people with whom we interact, victims of crimes and offenders, had a recent experience with the criminal justice system and are particularly attuned to what the law is, what their rights are, and what the data is about.

Now as I read to you, the statutes in general apply to our own employees and also grantees, contractors, and anybody who receives financial assistance from us. At BJS, our basic

[3] 42 U.S.C. § 10604d.

[4] 42 U.S.C. § 3789g.

approach to dealing with these confidentiality statutes is to not have any kind of data with identifiers available to us. There are only a few exceptions to that. The one major exception that is operated by BJS is our capital punishment series. Here the names are a matter of public record. You can read newspaper articles about practically everybody who is in our data files. But we still keep them confidential in accordance with that statute because of the other information that we have in the files about those people. In general, if anybody from BJS or representing BJS collects data from your system's files, it may be public in your files, or it may be confidential in your files. Once it is in our files, if it is identifiable, it becomes confidential without influencing the confidentiality status of the records from which we took the information. In some instances, we do need to have identifiable records in our offices. For example, we may want to audit or review the work of our grantees — not only how they did the data collection but some of them apply algorithms for matching records, and we can't really assess how they are doing unless we have some of the files and we try them ourselves. In those cases, we temporarily have identifiable data in hand and we try to follow the same procedures that we would expect everyone else who has identifiable data to have. We also collect a lot of information from organizations about organizations and we keep it confidential. But none of the regulations that I described really touches on data that are collected from organizations and about organizations.

We enforce the requirements on our grantees by asking them to submit a confidentiality certificate when they apply for Federal funding (or in any event before they receive any Federal funding) that specifies what kind of identifiable data they are going to have in hand and the purposes for which they are going to be used. These privacy certificates are required under the regulations. The grantee or the recipient of funding has to tell us who will have access to the data, what it will be used for, and confirm that the only people who have access to it will have a need to know the contents of the data. Also, it must be agreed that the information will be destroyed when it is no longer needed, or that the identifiers will be removed from it when it is no longer needed. Or, in case there is some reason — for example, for follow-up studies — to maintain the identifiers for a lengthy period of time, they will be put it in a separate linked file. The project plans and details about all of those things have to be reported to BJS before the organization gets our funding.

The reason we care about maintaining confidentiality is because for a lot of the data collections we undertake, we would not be able to get any valid information, or in some cases any information at all, if we couldn't promise confidentiality and stick to our promises. Furthermore, there are all the other Federal statistics agencies. In a way, we are arranged in a chain, and the weakest link can bring down the whole operation. Any

failing on our part with respect to confidentiality could impact the efforts of the Census Bureau, or the Bureau of Transportation Statistics, just through the general perception of the reputation of the Federal agencies.

### Differences among confidentiality statutes

Currently, there are differences among the confidentiality statutes, which pose quite a bit of a problem for Federal statistics agencies and are being addressed in proposed new legislation. First of all, there are some uses of data that are collected that are statistical in nature but are prohibited because of the particular statute that was cited when the data were collected or what was told to the respondents. So there are certain kinds of analyses we can't do because of the statute that applied when the data were collected. The second problem is that sometimes one statistics agency has to collect the same information that another statistics agency has because they are not allowed to share the identified records and transfer the information from one agency to another. A third problem that arises is that there are so many Federal surveys going on you could have three different Federal statistics agencies arriving at the same household. One might be trying to collect data about crime, and another trying to collect data about their income. When we can share identifiers, we avoid placing unnecessary burdens on the same people. So all these issues are addressed by the legislation that I mentioned.

I want you to think a little bit about what it is like to be a respondent to our surveys. The National Crime Victimization Survey is a national survey of a representative sample of households. Our interviewers talk to about 90,000 people twice a year. Once we select a household for the survey, the field representative visits the household, describes the whole operation, and collects the information that is needed on a one-time basis, like the birth dates, sexes, and races of the members of the household. After that first visit, most of the subsequent interviews are by telephone. At that first visit, the interviewer, a field representative, administers our National Criminal Victimization Survey, but we actually throw away that set of data because we are interested in being able to bound the time period of our interviews to a six-month period. So at the next time we return, we can filter out any events that they already told us about. Now, there are several things that those field representatives have to do if the data are going to remain confidential. First, they have to not let other people know why they are visiting or calling the selected household. Recently, there were two Census Bureau employees whose assignment was to get the census data from the Governor of Virginia, who had failed to return his census form. Naturally media representatives camp outside of every governor's office. So when the Census employees were asked why they were there, they said that Governor Gilmore hadn't filled out his census form. That was enough to get them fired, illustrating the importance of this area of

confidentiality to statistics agencies. Now think about this: we have different people in the same household and the interviewer is talking to all of them. But in order to get the truth out of each of them, it is very important for the interviewers to isolate information from different people in the household. So often the interviewer will ask somebody about whether such-and-so had ever happened to them? And the respondent might say, "Are you going to tell anybody else?" And they say, "No, we are not going to tell anybody else." And the respondents might ask for four or five levels of assurances because they go on to say, "Well, I couldn't even explain to my family why I was in this location where this crime happened if they found out about it." So you have to realize the interviewers come back 6 months later and they may need to refer to that previous incident. So they have to make sure that they don't refer to a previous incident that was mentioned by somebody else other than the person that they are talking to. All of these confidentiality conditions have to be adhered to even though it could be different field representatives calling on different occasions.

As I mentioned, we usually don't have identified data being analyzed at BJS for several reasons. In our data files of people being prosecuted or arrested or victimized, maybe famous people, there may have been cases that everybody would recognize from the newspaper, and BJS has additional data about those cases or about the people involved in the cases. We have data about cases that are before the grand jury, so you see that grand jury secrecy applies to the proceedings before the grand jury, but not to the collection of statistical data files. We have the possibility that there is an investigation of somebody that one of our statisticians knows, or there could be an investigation of somebody who is applying for a job at the Office of Justice Programs. All those purposes, like using the data for evaluating job applicants, are prohibited. We may have data about the details of the victimization of a person that you know. I recently faced a situation where there was a Federal case against myself. I think it is fairly common for Federal officials to have various lawsuits against them, and I represent BJS in one of those cases. So the data involving those cases are in our data files, and I have to be pretty careful not to try to figure out which of the records apply to my own case.

The Census Bureau operates our surveys like the National Crime Victimization Survey, and they have a different confidentiality statute than BJS has. So as far as the Census Bureau is concerned, the people at BJS are like the general public. We are no more privileged to see the data that we paid them to collect than anybody else is. The U.S. Census Bureau operates a microdata review. They have something called the Disclosure Review Board. Before we can get our hands on the data that we paid to collect, we have to go through that process. So we have to document a whole bunch of information about what we want to have, whether we want to have the raw data, or collapsed variables, or

other approaches to keeping the data confidential.

I will give you an example. BJS fielded a police public contact survey having to do with what kinds of contacts people have with the police. Were they positive or negative? Did any kind of violence ensue and so forth. So, it is very much designed to study issues related to racial profiling or to brutality by the police. After we requested the data so we could analyze it, the Census Bureau told us that we would have to drop the age and race variables in order to maintain the confidentiality of the people in this sample. There are about 70,000 people in this sample. We wouldn't be able to learn whether there were differences in these patterns by race if the Census Bureau wouldn't turn over the race information to us. The Census Bureau operates data centers where anybody can go and submit a tabulation or analysis that they want to run, and then have the output reviewed and released to them if it is acceptable. BJS staff could, if they wanted to, go to one of the Census data centers and submit its analyses of our own data and get the tabulations and look at the tabulations that way. But we have never done that because it is quite a burden on our staff. So you can see that these different statutes present daily obstacles for us. In addition to our analysis issues, we can't do planning with our own records. For example, we would like to track people over time, whether somebody who reported a victimization in one visit is less likely to report a victimization in a later visit. We can't do that because we don't have access to the identifiers to know who is the same person in the next visit. So, even for our own internal, budgetary, and planning purposes, we have to pay the Census Bureau staff to do this kind of work.

## Release of data records

BJS makes data available on its Web site and operates the National Archive for Criminal Justice Data at the University of Michigan. So statistics agencies have a traditional role of making raw data files with unidentified data available to researchers and the general public for various purposes. But there are a number of issues related to archiving and releasing archived data. In the past, before the data files were accessible on the Internet, people had to apply in writing for the data or they had to communicate in some way with the Archive to get a copy of the data. Now that we have them available for free on the Internet, some of the same issues of access with regard to criminal justice information or criminal history information also arise in regard to these kinds of statistical records. Making them available over the Internet is a different ball of wax. The main difference is that previously we knew who received the data, and we could make sure that they were aware of the limitations on the use of the data and they could sign that they subscribe to those allowed uses. Once the information is made available on the Internet, we can put as many screens as we like saying this cannot be used for this purpose or that purpose, but it doesn't make any

difference. We can't ensure that the user has seen those warnings or subscribes to them. So some of the data files that we have traditionally made available are statistical data files with no identifiers. We have had to withdraw some of these data files from release over the Internet. So with statistical data, we face some of the same issues with regard to criminal history records.

Since we don't release the identifiers, we have to expend resources on providing alternatives to identifiers that let people link records, if that is desirable. For example, on a prison file there could be a different record for each entry into prison, but if you look at the identified records, you can see that some of these people who enter into prison two, three, or four times are the same person. Whereas if we strip all of the identifiers, that would look like three, four, or five different people. So, for studies of recidivism, it is really important that the user of the data file be able to know which of the records refer to the same person even though they do not know who the person is. So we have to expend resources in order to capture that aspect of our statistical records and add that, rather than an identifier, back into the records. That causes an additional level of review because providing a capability to link different files can increase the risk of breaching the confidentiality. In addition, we have to review what was told to the respondent of the data that was collected, and whether or not we told them that we might link it to other information.

So I have talked to you about data collection. I have talked to you about release of individual records. Now I am going to talk about plain old statistical tables that just have rows and columns of numbers. They are not individual records for anybody. Some kinds of tabulations or combinations of tabulations provide too much information and would allow the talented statistician to identify particular people who are in the data by asking for answers to several different questions and examining the combinations of the different tabulations. For example, there might be a physician who worked on an Indian reservation and was the only white male of his age for 100 miles around. In statistical tabulations that show age, race, and gender, he could always find his answer to census questions or anything else. So the traditional solutions for preventing this kind of statistical discovery have been to obscure statistics that are drawn from too few observations. In some of our reports, we don't show any data that came from less than 10 people. In other reports we don't show any data that came from less than 5 people, depending on the sensitivity of the information. One way is to leave a blank in tables when the number of observations is too small. Another approach is to do various kinds of rounding, which drives the user absolutely crazy because there are bizarre combinations where the columns don't add up to the total and so forth.

Another function the Census Bureau provides is

the Census Data Center. You can go to a data center, tabulate some data records, and take away the tabulation, but you never get to see the records that you just tabulated. Now, as part of the research that I had mentioned, recently developed techniques for maintaining confidentiality in this particular area include injecting statistical noise into the records. From the point of view of the statistician, if you have a sample, it will have a certain variance of the estimate based on the fact that it is a sample and you can tolerate a somewhat larger variance of the estimate, which is caused by adding statistical noise, which means that some variables are changed or a small quantity is added or subtracted from them at random. So that is one approach to keeping records confidential and still allowing them to be used by the public. Another is when we make data files available on the Internet for different people to tabulate, we have the problem that if they are persistent enough and go through numerous tabulations, they can identify a particular person. So another recent innovation is to build in audit trails of the cumulative uses that have been made of the data and stop anybody from doing additional analyses if they have passed that limit.

## Strong review and oversight

We face a growing distrust that the protections, statutes, regulations, and everything I have just described to you, which in my mind we adhere to so rigorously as to be a burden, are not actually followed, that there are common breaches, and that data provided to statistical agencies are not really safe. Even in cases where data files, which are not statistical files, have been misused by the Federal government — even if the misuse was inadvertent or a mistake — it adds to the distrust of our Federal files. Maybe nobody intends to do this, but it can just happen that your data winds up on the front stoop of a Federal office building.

The other interesting development to me is all these legislative changes over the last few years, which have allowed criminal history records to be more widely available and have allowed sex offender registry information searchable on the Internet. All of those kinds of legislative loosening of prior restrictions represent a danger in the mind of the person who is providing information today. You can tell them about all the confidentiality limitations in the world, but they may be concerned that tomorrow the legislature could change that, if that is the trend of things. Then what they give you today in total confidence will not be confidential anymore tomorrow. I do think that the collective activity of loosening prior restrictions has that kind of impact on Federal statistics agencies. The issue has been raised as to whether legislatures that do this are getting ahead of what the public really finds acceptable.

So this is our view as a statistics agency. Review and oversight of the practices are so strong, that it is really a very remote possibility for someone's confidential information to be in danger of misuse or compromise by a Federal statistics agency. Within

the Federal statistical system, it really seems to me that there is not any justification for concern about confidentiality of individually identifiable data.

## Privacy and public opinion

Public attitudes toward uses of criminal history information
*Timothy D. Ellard*

Balancing privacy and public uses of criminal history information
*Dr. Alan F. Westin*

# Public attitudes toward uses of criminal history information

**TIMOTHY D. ELLARD**
*Senior Vice President*
*Opinion Research Corporation*

My task this morning is to walk you through an ocean of data.[1] I am not an expert on privacy matters as they apply here; but certainly, privacy is one of the principal concerns in my business. If you read our company's Code of Ethics, you will see that privacy is the principal subject. Otherwise, I am talking today as a representative of the general public. I am going to take you through an interview about public attitudes. Public attitudes, you must remember, are really rather thin, rather unformed. Let's take an analogy of a busy office, maybe your office. There is a large volume in the center of your desk that deals with privacy issues. It is something that you think about all the time. It is something of great importance to you. In contrast, if you are dealing with the general public, and you go to the same office and bring up privacy, the public goes to a file cabinet in the corner. It has to go to the lowest drawer and reach back to find something on privacy. It is not the same for you as it is for members of the general public. They do not think about privacy issues every day, and yet they have attitudes and opinions about them. I will walk you through some of the attitudes and opinions they reported to us.

## The survey

Today, I am reporting on a survey that was conducted on behalf of SEARCH and the Bureau of Justice Statistics.[2] Its purpose was to gauge public attitudes about the use of criminal history records outside the criminal justice system. Now, we really went through a lot of subjects when conducting this survey. It involved more than 1,000 respondents who were contacted by telephone. The interviews took approximately 25 minutes. This was a probability sample of U.S. continental households. We used a design that gave us an equal number of men and women respondents. The interviews were conducted rather recently, in late February and early March 2000. The results, in total, have a confidence level at about plus or minus 3 percent. Now, when we go into some detail here, we won't be talking about the full survey. We won't be talking about 1,000 people.

[1] Mr. Ellard's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/search_orc.ppt.

[2] Bureau of Justice Statistics, *Public Attitudes Toward Uses of Criminal History Information: A Privacy, Technology, and Criminal Justice Information Report*, NCJ 187663 (Washington, D.C.: U.S. Department of Justice, July 2001). *See* www.ojp.usdoj.gov/bjs/abstract/pauchi.htm.

We will be talking about, in some cases, 100 or 200 people. If I talk about statistical significance today, I will be using the correct bases and the calculation that sometimes takes a lot more of a difference between small groups. But the differences are there.

These are our key findings. They are really a summary of a summary. As adults, you are concerned about misuse of personal information as it extends to criminal history and related records, but most adults are willing to give up some privacy protection if the trade-off results in a benefit to the public, such as increased safety, crime prevention, or the protection of children. This is an interesting dichotomy. We will introduce each subject as we go along.

## Misuse of public information

Our first subject is concern about misuse of public information. I should point out that we treated this as a classification question. As a classification question, it was asked very near the end of the interview. Therefore, all of the rest of the information that we sought may have affected some of the things that brought this answer up. We asked how concerned are you about the possible misuse of your personal information in America today? Are you very, somewhat, or not very concerned? We found that 64 percent of the respondents — a strong majority of the public — were very concerned, and an additional 25 percent were very or somewhat concerned, for a total of 89 percent. When you are in survey research, you are not accustomed to seeing 89 percent of anything very often. It happens sometimes in attitudes toward simple subjects, but even motherhood doesn't get 100 percent in the United States.

We also asked about respondents' experiences. We asked whether they had ever personally been the victim of what they felt was an improper invasion of privacy by any of the following: a business collecting and using information about you; a law enforcement agency; a government tax, social service, welfare, or license agency; or a charitable, political, or nonprofit organization? Sixty-two percent of the people said they had not been victimized in this way. The other 38 percent mentioned business most frequently, followed by nonprofits, law enforcement, and finally, government. If you add up the answers on the right-hand side (on slide 7 of my PowerPoint presentation, which follows this presentation), you find that 38 percent of the people gave us 60 percent of the answers, meaning that the average person mentioned two of these. So, when they think about being victimized, the last thing they think about is government. The next to last is law enforcement, but businesses collecting and using information and charitable organizations are seen as the primary offenders. It is very hard to separate these two into business and nonbusiness. They seem to operate much in the same way.

Now, when we look at this question by gender and by race we see some interesting differences (slide 8). When it comes down to law enforcement agencies, men are far more

likely to say that they have been victimized. If it comes down to law enforcement agencies, African Americans say they are much more likely to have been victimized. The tiny arrows besides some of these numbers indicate statistical significance.

Then we asked people their views of the criminal justice system (slide 10). Seven out of 10 adults felt that they at least knew the basics when it came to the American system of criminal justice. Only 13 percent said they knew it a great deal, but 57 percent said they knew the basics. This adds up to 70 percent. Note that this is a self-appraisal. We may have interviewed a district attorney who felt that he or she really didn't know the system at all, and we may have interviewed someone who had had no familiarity whatsoever, other than perhaps viewing a couple episodes of *Law and Order* on television, and they felt very well-informed. We didn't test them. We just asked how they felt about it.

Next we asked them what they thought about some aspects of criminal justice (slide 11). We asked that, based on what they had heard or read or on personal experiences, how effective did they think the overall American criminal justice system was in each of the following areas: investigating and arresting persons suspected of committing crimes; prosecuting accused persons and in reaching just outcomes at criminal trials? Now, we see that "very effective" gets rather low numbers from everybody on everything. But "somewhat effective" brings the ratings up to a pretty high number, particularly for arresting the right people. In "prosecuting people" the numbers drop, and in "just outcomes," the numbers drop even further. Later on, when we see things like releasing "arrest records without convictions," we can go back and look at the fact that the respondents thought the arresting process was pretty good.

We also asked respondents about how they thought the system was doing in protecting the rights and the liberties of suspects (slide 12). Again, at 24 percent, the "very well" answers were not so high, but higher than some of the other things we saw. Added to the "somewhat well" response of 46 percent, the two categories accumulated a total of 70 percent. The preponderance of "somewhat well" over "very well" might be a lack of enthusiasm; but often, in doing public attitude studies, you find that "somewhat well" reflects a lack of real knowledge and a little uncertainty.

## Access to records

Regarding access to "conviction" records and "arrest without conviction" records outside the criminal justice system, we found that most of the public supports access being provided to "conviction" records where there is some public benefit, such as safety, crime prevention, or protection of children. However, access should be limited to only those with a legitimate need. The definition of a "legitimate need" will be fairly open as we go along. There is more here than you can read (slide 15), but again, I

am acting as a respondent listening to questions. The next question began with the statement, "Under American law and practice, government criminal history records are made available to some government and private users outside the criminal justice system." Respondents were then asked to express their preference for one of the following three policies for making such government records available:

- A completely open system where anyone can obtain either the "conviction" or the "arrest without conviction" record of any individual because such broad access helps protect society.

- A partially open system where anyone can obtain "conviction" records but not records for "arrest without convictions" because persons who are not convicted are presumed innocent in our constitutional system.

- A system that is open only to selected users for either "conviction" or "nonconviction" records such as employers or government licensing authorities because society feels certain uses have a valid need but others do not have a valid need.

Most adults supported providing employers and occupational licensing agencies with access to "conviction" records in extremely sensitive jobs — those involved in handling money, working with children, or security guards, for example. Attitudes toward employers and licensing agencies turn out to be almost identical. On slide 16 we see that the survey shows all employers should have access — 40 percent. While that is a minority and it is in second place, it is a big number. Fifty-five percent believed that access should depend on the job. Notice that only 4 percent say there should be no access to "conviction" records.

We then asked respondents to please think about the government records of persons arrested for, but not convicted of, crimes. Would you take the same position on groups having access to those records as you just did for "conviction" records, or would you take different positions as to records of "arrest without conviction?" Sixty-seven percent of the people said they would take different positions. We didn't ask what positions; we just asked whether they would be different. We see some of those different positions on the next slide. We have two bars on slide 18. The dark bar is "arrests without convictions." Forty-nine percent of the respondents say it "depends on the job" whether that type of information should be made available to employers. Compare that to the figure represented by the light bar, which depicts "conviction" information. The numbers are almost similar, but there are some interesting changes that really start with the people who say "all" records should be available. Forty percent of the people say that all conviction records should be available. Fifteen percent say everyone should have access. We went from 4 percent saying no access to 31 percent saying no access. If you do this as a waterfall, starting with the

notion that “everybody should have the availability,” we lost 35 percent of the people down to one of the next two items — “depends on the job” or “none.” Then we lost people down to “none.” Releasing records for “arrests without convictions” is not a popular concept at this point.

We asked respondents who they thought might want access to “conviction” and “arrest without conviction” records (slide 19). We received the following answers. In each case, there is probably more of a willingness to release “arrest without conviction” records than we thought there might be. The top groups we have are the Boy Scouts, others working with children, and the military. The next group consists of insurance companies investigating fraud. Down at the bottom, we have some interesting sorts of cats and dogs such as reporters, banks looking at loans, or individuals who want to learn if a neighbor has a criminal record. That one is exciting. We also have companies that issue credit cards listed there. As you can see, people were initially reluctant to release record information on almost anything, but that changes when they are given some reason for the release.

## Rehabilitation concerns

The next subjects we have are rehabilitation concerns, access to juvenile records, and, potentially, sealing records of ex-offenders (beginning with slide 20). The majority viewpoint here is that most respondents want to give juveniles a second chance, but adults should have to live with the consequences of their actions. A small majority of adults — 54 percent to 40 percent — actually prefer to keep juvenile records sealed. This is not a huge difference and things can happen here. The question was framed as follows:

“Today, many States limit the availability of records about juveniles charged and processed in juvenile courts; for example, not allowing access to employers, government licensing agencies, or military enlistment officers. This practice is based on the judgment that juveniles should be given an opportunity to overcome youthful criminal behavior. Out of concern over current juvenile crimes, some people would open juvenile records to greater access. Please listen to the following two policies and indicate which one you think would be best: Keeping restrictions on disclosure of juvenile court records because giving juvenile offenders a chance to overcome a bad record is a sound approach, or opening juvenile records to the same government and private organizations that can get adult criminal records, since protecting society and the public should be the primary concern.”

As I noted before, there are some differences in attitudes. For example, 50 percent of those who spent no time in college favored restrictions, while 56 percent who have at least some college education favored such restrictions. Fifty-one percent of Whites and 69 percent of African Americans favored the restrictions (slide 23).

In some instances, respondents' points of view influenced their responses to the juvenile record question (slide 24). Fifty-one percent of those who believed that the justice system respects the rights of subjects felt that the dissemination restrictions should be kept. The percentage of respondents who believed that the system did not respect the rights of subjects and who felt that the dissemination restrictions should be kept was higher: 59 percent. Of those who have not worked in criminal justice, 52 percent favored keeping the restrictions. Of those who have ever worked in criminal justice of any kind, 64 percent would keep the restrictions. The bottom line is, we favor keeping restrictions on the disclosure of juvenile justice records.

Only a minority supported sealing the records of adult ex-offenders after a defined period of time (slide 25). Some people believed that if a person convicted of a crime served his or her sentence and then did not violate the law for a period such as 5 years, government record agencies should not make that criminal record available to employers or licensing agencies. Notice again, we have this sort of mild split. The split reveals, in this case, that respondents favored restricting access to juvenile offenders records, but they did not favor restricting access to records sealed after a specific period of no criminal activity.

Also, we again have our demographic differences. Forty percent of Whites compared to 60 percent of African Americans believed that records should not be available after a specific period. Only 37 percent of households with incomes $50,000 or higher were in favor of sealed records, compared to 48 percent of those with incomes under $50,000.

## Fair information practices

Going on to our next subject, we talked about fair information practices, which included the following:

**1. Right of review and error correction**: Each person would have the right to see his or her record, and to have items believed to be incorrect rechecked by the recordkeeping agency and corrected if they were in error.

**2. Impartial complaint resolution**: An impartial procedure would be available for receiving, investigating, and resolving complaints by individuals about misuse of their records or failure to follow agency policies.

**3. Prior notice of creation and use**: Each person would be informed when a record is created, what that record is, how it will be used inside the criminal justice system, and what policies will be followed in making the record available outside the criminal justice system.

We told respondents of certain policies established to protect the individual rights of persons having criminal history records (beginning with slide 29). For each of the policies described above, respondents were asked to rate whether the policy was very important or somewhat important. Notice the degree of "very

important" and notice the degree of agreement. It slacks off to a minor level from "right of review and error correction" down to "prior notice of creation and use," but when presented with these concepts, the general public rates them as extremely important and is very much in favor of it.

Next, we move to the part of the survey gauging public attitudes on "Government Versus Privacy Sector Criminal Records" (beginning with slide 30). Again, I think it is important that I read you the questions. Imagine that you are a respondent. This is what you would hear: "Turning from government record systems to the private sector, there are private companies that collect reports of arrest and trial outcomes from newspaper stories and from various public records, such as criminal court files. These companies sell this information to private parties, such as private employers, insurance companies investigating fraud, or lawyers checking out parties or witnesses in civil litigation. The companies also provide criminal history reports to government licensing agencies, government employers, and other government agencies. Which one of the following judgments about this system of private information suppliers of criminal history records would you agree with most?

1. This commercial system provides relevant information from public record sources, for many important business, social, and government purposes and is okay.

2. It worries me that this is being done by commercial organizations and I favor this being done by the government."

As we can see by the responses (slide 31), there was overwhelming support for leaving this information in government hands. Private agencies doing this sort of thing obviously create a sense of unease in the public.

To carry this one step further, respondents were asked whether they felt that commercial companies should follow the same rules and procedures that public agencies do for giving individuals they report on fair information and fair procedure practices.

Again, we see overwhelming support for the concept that commercial agencies should have to follow the same rules as government agencies do when disclosing this kind of information (slide 32).

Fingerprinting is another area with privacy implications. Our survey found that the public perceives fingerprinting as an acceptable means of identification when the underlying purpose is to protect public safety and prevent fraud. Our survey found that 61 percent of the public had been fingerprinted. We asked that 61 percent, as a separate population, what they thought of it and whether they thought it was appropriate. Eighty-seven percent of those who had been fingerprinted felt that it was appropriate. Twelve percent said it was not. We did not ask why they felt it was not appropriate.

We went back and asked about the various reasons

for fingerprinting. Many of the reasons, as you can see (slide 36), are generally accepted. Public support is high for fingerprinting those arrested for crimes, those applying for government licenses, and those applying for welfare programs. Then it slacks off when the issue is putting a thumbprint on your driver's license, using it to cash a check, to buy an airline ticket, or to apply for a job. Generally, however, there is not a huge undercurrent of resentment towards fingerprinting in these situations.

## The Internet

If you do a survey these days, you always have to mention the Internet. It just seems to come up. The Internet is seen as a potential threat to privacy. Internet use is growing. At the time we did this study with the respondents that we talked to, we found 60 percent said they used the Internet either at home or at work, or both. Forty percent don't use the Internet. If this survey had been conducted a couple of months later, that 60-percent number would probably be a couple of points higher. Internet usage is endemic. It is here. We will be living with it for a long time. We asked people what private information they thought was available on the Internet, such as anyone's credit bureau report, criminal conviction record, Social Security number, credit card numbers, arrest record even if not convicted, or bank checking account balances. We started with around half of the people believing anyone's credit bureau report could be obtained online and dropped down to 36 percent of the respondents who believed that anyone's bank check account balance was available. In almost every case, people who use the Internet are more likely to believe that this information is available compared to the people who are not using the Internet. This is not just a boogey man sitting out there coming out of nowhere. These are people who are on the Internet, and they believe private information is available for sale at this level of the Internet.

Finally, we found that some people believe that State government agencies which maintain criminal history records that are open to the general public under their State laws should post these on the Internet so anyone who wanted to could check whether someone has such a record. Other people feel that even though such records could be obtained by applying to the government record agency for a copy, it isn't a good idea to put all those records on the Internet for anyone to obtain. Which would you prefer? Ninety percent say that they don't like the idea of those records being on the Internet — a rather overwhelming number. No telling when we will see it next.

This brings us to the end of the numbers and the questions. Again, we have now touched on the general public. The general public is lightly informed. They are not concerned with these matters on a moment-to-moment basis. Yet, they have opinions and some of these opinions are quite strong. Because the general public has formed its opinions lightly, that does not mean that they wouldn't change. The

right stimulus or the right incentive introduced tomorrow could switch many of these numbers around. Knowing where they are now presents a number of very interesting insights into how the public thinks about privacy. Let's take a look at our conclusions. There is concern about the misuse of personal information, and the people who feel victimized in such situations tend to be much more likely to mention businesses and not-for-profits, all of which I lump as businesses. It is not the government. It is not the legal system, or not as much. Even with this concern, however, there is a belief that the protection of privacy should not be at the expense of the public good. Perhaps people are almost too willing to find a reasonable excuse to say, "Well, we can make an exception for that." Most U.S. adults believe in the principle that people are innocent until proven guilty. They believe access to "arrest without conviction" records should be limited, and that an individual's rights should be protected. The public believes the government should control these records. It doesn't really care for private companies having access to private data that can be sold on the open market. Finally, even if the government is maintaining criminal records, nine out of 10 adults believe they should not be posted on the Internet.

# Balancing privacy and public uses of criminal history information

**DR. ALAN F. WESTIN**
*Professor Emeritus of Public Law and Government*
*Columbia University*

My assignment is to discuss what the data from the Task Force's commissioned survey tells us about public attitudes toward the use of criminal history information, both inside and outside the criminal justice system.[1] Since the question-by-question results of the survey have already been presented, my role is to offer an interpretive commentary, as a long-time privacy expert and survey advisor.

In beginning, let me express my appreciation to the Bureau of Justice Statistics for commissioning a national public opinion survey, making it part of this National Task Force on Privacy, Technology and Criminal Justice Information project, and adding its findings to the public discussions of criminal justice information uses that are clearly coming in this decade. A similar debt is owed to SEARCH for organizing the Task Force, and to the Task Force Chair, Robert Belair, for managing the project with great skill from beginning to end.

## The privacy surveys environment I: Levels of public concern

Since 1978, I have been the academic advisor to 45 national surveys exploring public attitudes toward privacy issues. This has involved 30 surveys with Louis Harris and Associates (now Harris Interactive), and 15 with Opinion Research Corporation (ORC). One great advantage of such a body of work over 3 decades is that, if you ask thoughtful questions early on and you ask them year after year, you can get solid evidence about changing public perceptions and trends.

Let me illustrate this. In 1970, Harris asked respondents how concerned they were about their personal privacy. Thirty-four percent of the public said it was concerned. When I first started doing surveys with Harris in 1978, Watergate had intervened, along with the anti-war, social protest, racial justice, and gender-equality movements. By that time, 66 percent of the American public said it was concerned about threats to privacy — almost twice the percentage than 1970. By 1990, the same question produced a further rise to 78 percent of concern. With growing concern about information technology applications by business and government in the 1990s, and the rise of an Internet world, a

[1] Dr. Westin's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/!afwsear.chp.

Harris-Westin survey in 1999 found that over 9 in 10 Americans — 94 percent — now answer the trend question that they are concerned about privacy threats in the U.S. today.

Privacy trend questions also allow us to probe the intensity of feeling. In good survey analysis, you want to look at the "very concerned" response when you are putting together the answers of people who say they are either "very concerned" or "somewhat concerned" about a particular topic. In a 1999 survey, 77 percent — three-fourths of American adults — chose *very* concerned when they were asked their level of concern about the misuse of their personal information and threats to their privacy.

So, we see from privacy-survey work between 1970 and today that the initial one-third minority concerned about privacy in 1970 rose to what is now (1999) a 94 percent majority of the American public. And it is intense concern that is now registered by three-fourths of the public — 77 percent.

This is the background against which our survey took place.

## The privacy surveys environment II: Who poses the potential threat?

A second important trend finding involves the shift from the 1970s to today in terms of which institutions the public perceives as the principal potential threat to individual privacy. In the post-Watergate era, the government was overwhelmingly perceived as posing the potential threat. Seventy to 75 percent of survey respondents in 1978 identified the government as being the source for potential threats to privacy. When we last asked this question in the mid-1990s, sentiment had already shifted to the point where respondents identified business and government as equal threats to privacy. About half said the government was the greatest threat, and half that business poses the greatest threat.

## A very timely survey

Our survey was fielded at a moment when, as the Task Force report explains, the information-processing functions of the criminal justice system are expanding in major ways, as a result of new applications of advanced information technology. The governmental system is deepening the records that it collects. It is combining them more extensively inside the criminal justice system, and moving, for example, much deeper into retrieval capacities in court record systems, both civil and criminal.

In addition to the direct criminal-justice system uses, there are often public-policy demands to supply criminal history information to other governmental and private uses. As the Task Force report documents, legislation has required criminal record checks for people who deal with senior citizens, children, and other special populations. Another example is the *Brady Handgun Violence Prevention Act*, with its requirement of a criminal record check for firearm purchases.[2]

[2] Pub. L. 103-159 (November 30, 1993).

The Task Force report also documents the rise of commercial distribution systems, including the media. We now have an industry of substantial size collecting and organizing database information, including criminal history records, and making these available to a variety of users. These users range from employers, government agencies, lawyers, insurance companies, and private investigators to general users of the Internet.

It is this intersection of greatly expanding government and private criminal justice information systems, alongside high public concerns about privacy, that the Task Force set out to consider, and which the survey has explored.

## Putting the survey findings into perspective

Recognizing these background settings, let me turn to analyzing the survey findings and putting them into context. First, how valid is a survey that asks respondents about a topic — government and private uses of criminal history information — that is not an everyday feature of most people's daily lives? Second, how representative is this survey of the other major privacy surveys conducted over the last 20 or 30 years? And third, what do those surveys teach us about how the public makes up its mind about the balance between privacy and public interest?

**1. An anticipative survey.** When a survey of the general public is fielded into a topic as specialized as uses of criminal history information, an initial issue to consider involves the bases that respondents would draw on in answering these questions. Put another way, we need to ask: "Is this survey reactive — presenting issues where most of the public can be expected to understand the issue, the players, and the options — or is it an anticipative survey, asking people to think about rather special unfolding issues and to draw on their deeper attitudes to express some broad preferences?"

Our survey is clearly anticipative rather than reactive. In terms of personal experiences, we know from our survey results that only 10 percent of the sample says it has ever been arrested for a nontraffic offense; that represents about 20 million adults. Within this segment, 57 percent say their arrest resulted in a conviction. This gives us a database of 12.4 million persons who would have personal experiences with conviction records in the criminal justice system. Although that is a big number, it is still a very small percentage — less than 10% — of the total adult population of the United States.

On the other hand, when you deal with issues of employment screening, occupational licensing, and so forth, it is clear that a majority of our respondents can identify with those situations and probably have had direct experiences in having record checks made for these noncriminal justice purposes.

However, we should note that, for the majority of the population, there is not at

present the same salience in use of criminal history records outside the criminal justice system as there was in the late 1960s and 1970s. That was the period when quite a few children of the elites were being arrested — for racial demonstrations, anti-war protests, and other "direct action" activities. These were the children of government officials, business executives, and academics. Because an arrest and especially a conviction record would stigmatize those persons, affecting their entry into employment and issuance of licensing, how arrest and conviction records were going to be used was a visible issue in the late 1960s and 1970s.

That is not where we're at today. For one thing, employers and licensing authorities have learned to examine what an arrest was for. If it was for a protest, it has a different impact on employability and licensing today than under the automatic-stigmatizing assumptions back in the 1960s and 1970s.

It is also important to note that different segments of the national population feel specially impacted by the social uses of criminal history information. As survey findings show, race is the predominant factor here. Minority populations register greater concern over the stigmatizing effects on their opportunities for employment and credit, for licensing, and other kinds of functions in this society.

Finally, our survey is anticipative because most members of the public are not, as the phrase goes, "policy wonks." They don't think in terms of whether a legislative solution should take an opt-in or an opt-out approach, or whether a privacy notice should be cast in a certain way. Those issues are for the experts. They are very important, of course, in terms of policy, but we deliberately stayed away from presenting those kinds of questions in our survey, framing our questions in terms of broad policy and social choices.

**2. Our survey is in line with other privacy polls.** Comparison of our results on several key questions provided confidence that we had a representative sample of the American public when it came to the balancing process that the public uses in weighing public and social interests and privacy rights. Our figures on overall privacy concern parallel those of major privacy surveys during 1997-2000. More specifically, our respondents matched those of other survey populations in viewing information technology uses as generally positive but also as posing some threat. Our respondents recorded the same heavy support for key fair information practices as registered in privacy surveys focusing on other consumer or citizen privacy issues. Specifically, the list of rules that our respondents heavily favor for the handling of criminal history information match the high support for those principles in many of the surveys.

**3. What the survey teaches us**. Finally, the basic privacy orientations of the American public that we obtained matches those found in over 25 years of research from privacy surveys that I have done. We have found, in looking

at the pattern of the public's privacy attitudes, that the public broadly divides into three continuing and consistent segments.

First, you have what I call the "privacy fundamentalist." These people view privacy as a passionate and deep concern. They generally will reject a consumer benefit or social value as being not as important as protecting their privacy. When it comes to consumer privacy issues, they want the government to pass legislation or have regulatory oversight because they think that is the only way that their consumer privacy will be adequately protected.

At the opposite end, you have what I call the "privacy unconcerned." These are the folks who don't know what the issue is all about, and couldn't care less. As consumers, if you give them 5 cents off, they will give you their family histories and anything else you want to know. They also generally feel that public order and public safety is far more important because they don't think they have anything to hide. Those are the characteristics of the privacy unconcerned.

In between those two, you have what I call the "privacy pragmatists." The process by which privacy pragmatists make up their minds about the use of their personal information by government or business follows a well-documented path. First, privacy pragmatists ask, "What is the benefit to me or to my society? What do I get if you extract or require me to give my personal information?" The second question they ask is, "What are the privacy risks and how serious are they? How is my information going to be used, and is it going to be used in ways that I am really very unhappy about and that seem to be excessive?" Third, they ask, "What safeguards or protections are being offered for my privacy against those privacy risks, and how will they be delivered?" Finally, and most important, they ask, "Do I trust the industry or the sector to follow those safeguards?" If they do trust, the privacy pragmatists will supply their personal information, or be comfortable with its uses. If they don't trust the data collectors, the question becomes, "Should legislation be enacted to forbid or to permit-but-regulate these information activities?"

Past surveys show that the percentages in each one of these three categories will vary according to the privacy issue involved. Most people don't have one coherent and consistent view across all the different dimensions of privacy — the citizen, consumer, and employee domains. And, the consumer issues themselves subdivide into different sectors, like financial affairs, health and medical affairs, telecommunications, direct marketing, Internet, etc.

In general, we found on consumer issues that 25 percent of the public are privacy fundamentalists, 20 percent are privacy unconcerned, and 55 percent fall into the privacy pragmatists category. Not surprisingly, when you shift to health and medical issues the privacy fundamentalists category expands to roughly 35 percent. That is a survey finding from

1994. My guess is that if we ran it again, it might be up to 45 percent in terms of the increased sense of sensitivity and risk involved in health and medical records.

On citizen issues, we found about 32 percent were in the privacy fundamentalist category, 12 percent in privacy unconcerned, and 50 percent were privacy pragmatists. Our data suggests that the criminal justice issues approximate the citizen-issues division. About a third were privacy fundamentalists, 15 percent were privacy unconcerned, and 50 percent were privacy pragmatists.

## Attitudes toward the criminal justice system

These patterns are reflected in the findings about general attitudes toward the criminal justice system. By a range of 68 percent to 79 percent in the different dimensions we offered, the public rates the criminal justice system as effective, and 70 percent also say the system "respects civil liberties." Again, as the ORC summary noted, the "very effective" and the "very greatly respects civil liberties" categories were not high. But when we put the "very" and "somewhat" answers together, as is traditional in this kind of survey work, we get the high positive numbers noted. And, only 12 percent say that their own privacy has been invaded as a result of a law enforcement agency action.

It is useful also to compare these ratings with confidence ratings obtained about other institutions. Over the years, the Harris organization has maintained a "confidence in institutions" index. A list of institutions is provided and respondents are asked how much confidence they have in the people running those organizations. Three answers are provided: a great deal of confidence, only some confidence, or hardly any confidence.

The skepticism the American public feels toward most of the government institutions in the Harris surveys makes the generally positive results as to law enforcement shine by comparison. Eighty-two percent in the latest Harris survey say they have *only some* or *hardly any confidence* in the Congress. Negative ratings of 79 percent were registered for the Federal Executive Branch; 76 percent for the White House; 64 percent for the U.S. Supreme Court, and — the big winner — only a 48 percent negative rating for the military.

## Use of criminal history information

With the overall positive ratings of law enforcement in mind, we examine some responses to specific policy issues. Only 12 percent of our sample favors the completely open criminal-history records system in some States. This seems to reflect a sense that there are too many privacy perils in the total access approach for more than 12 percent of the public to feel this is a good solution. Eighty-four percent of our respondents want some kind of limits on either the type of criminal history record that is disseminated or the type of user. When it comes to

*conviction* records, 47 percent favor a system that is completely open, and 37 percent favor a system that could provide access to both conviction and arrest-only records for specific types of users.

Another important finding involves the kinds of access to criminal history records that the public thinks is appropriate. There were no majorities for open access to all criminal history information to all the kinds of private organizations that we listed. Basing their views on the type of user and use, 55 percent would let an employer, and 57 percent would let government-licensing agencies have access to conviction records if there is a sensitive job that makes access important criteria in protecting the public. For arrest-only records, the sensitivity of the job drew under a majority for employers and 50 percent for licensing agencies. Respondents who would deny access to arrest-only records rose to 31 percent and 29 percent in those categories.

Another example is the way access was dealt with in terms of need and relevance. As far as *conviction* records were concerned, there was very high support for groups that work with children, the military, and insurers fighting fraud. On the other hand, there was not a majority for giving access to the media, banks for loan decisions, neighbors checking on criminal history conviction records, and credit card issuers. When we shifted to *arrest-only* records, the center of gravity moved dramatically, with only groups working with children drawing majority support and no others getting a majority for access being provided.

In terms of demographic analysis, we see that the groups that favor more limited or less access are younger respondents who feel that they are still coming up in the system, and that there can be more harm done to them from some of these criminal history information uses. African Americans as compared to Whites are more critical of the criminal justice system, as are respondents who were most worried about privacy threats, and respondents who have been arrested or convicted.

The groups who would most restrict access may not be so much separate categories as combinations of statuses or attitudes. In many privacy surveys, the same individual may be located in demographic categories of lowest education, lowest income, and minority status. My sense is that 20 percent to 35 percent of the total public shares these demographic characteristics and, therefore, have those attitudes.

## Broad support for fingerprinting

When we turned to fingerprinting, heavy majorities said that fingerprinting was acceptable for all of the seven uses that we tested. Not surprisingly, we see very high support — 80 to 94 percent — for using fingerprints to process arrests in the criminal justice system, issuing occupational licenses for sensitive jobs, and policing welfare fraud. Those uses always draw heavy support from the general public. And, because identity

fraud has become — and is perceived by the public — as a major problem affecting millions of victims, there is strong support for using a finger image on driver's licenses to prevent fraudulent use. The survey even received 68 percent to 71 percent support for using fingerprinting for the check cashing.

One result that was somewhat surprising was majority support for the use of fingerprints for buying airline tickets. We may have prompted that response by connecting, in our wording, the use of fingerprint to fight airport terrorism, to explain why such a use might be made. But it is striking to think that a majority of Americans in 2000 believe it's acceptable to fingerprint and verify all people who buy airline tickets.

A few other findings are worth underscoring. Ninety percent of the public expressed opposition to putting what our question called "open public records" on the Internet. Experts know that putting open records online raises some quite sensitive issues, such as access to the home addresses of law enforcement people, mayors, and other public officials. Publicizing bankruptcy records would disclose to anyone sensitive information such as Social Security numbers and personal finances. Whatever specific issues members of the public had in mind, nine-tenths clearly feel there is a tremendous difference between putting open records on the Internet and having them open only at their source or by applying for tapes or printouts.

On handling juvenile records, the survey produced no majority for opening such records for full public uses. Rather, small majorities would keep restrictions on the disclosure of juvenile records, and would allow such records to be available for employers and license agencies.

Two out of three respondents believe it would be better for the government to provide criminal history information for socially valuable uses than it would be to have this done by commercial services.

There is no doubt that the public is worried about the commercial sector providing this information.

## The public wants privacy safeguards

When we turned to explore the privacy policies to surround criminal justice information systems and uses, the public gave high support to installing and administering basic fair information practices. We saw high support for installing the right of subjects to see their records and have corrections made, to have an impartial dispute resolution procedure, to have information procedures explained and policies followed. These were all seen as important. In addition, the public wants commercial agencies to follow the same kinds of fair information practices as government agencies.

## Summary comments

As I have already mentioned, the findings here are well supported by other privacy surveys. In terms of basic divisions of the public, the survey shows that the majority of the public starts out as privacy pragmatists. They

want to pick and choose what uses seem to be legitimate or where the privacy risks seem to be too great. In no sense is there a kind of carte blanche attitude that criminal history information is just okay, so let's use it any place people want it. The process of looking at the value, assessing the risk, checking for safeguards, and deciding whether they trust the people running the system is the process by which people make up their minds.

This leads me to draw a general conclusion from the survey. The public will support the development of new rules for societal uses of criminal history information in an information-rich age when people are seeking better access to criminal history information on the one hand while also being very worried about inappropriate or dangerous uses of information.

Where that debate will go will not be decided in this kind of public opinion survey sense. It will depend on the process by which these issues are tested in legislative arenas, in executive agencies, in the media, and in public debate. What you have in the survey are some underlying attitude sets. How they will be focused depends on the play of debate, and on whether horror stories grip the public and drive decisionmaking, or whether the feeling is that there are workable solutions. We will have major debates in the 2000-decade over reshaping the rules for criminal history information both inside the criminal justice system and in social uses outside. The survey will be useful in providing at least a baseline of understanding about how the public is likely to approach these issues.

## National Task Force report

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

*Robert R. Belair*

# Report of the National Task Force on Privacy, Technology and Criminal Justice Information: An overview

**ROBERT R. BELAIR**
*Chair, National Task Force on Privacy, Technology and Criminal Justice Information*

It is a pleasure to be here to talk about the National Task Force on Privacy, Technology and Criminal Justice Information.[1] Throughout my presentation, I am going to do things a little differently and pose some questions to our moderator, Kent Markus, one of our stellar members of the outstanding group that comprised the Task Force.

You have already heard a good deal about the Task Force today. We have four deliverables. We have a report that currently runs to about 200 pages.[2] It analyzes existing law and policy for handling criminal history record information. It identifies the technological and societal developments that may be changing the criminal justice privacy environment. We have the public opinion survey that Dr. Westin was the academic advisor on, conducted by the Opinion Research Corporation (ORC). You heard the report and you were given materials from that report.[3] We have 14 recommendations, and I am going to discuss the highlights of those recommendations. We also have this national conference, so all of you can think of yourselves as deliverables. It is in this sense that we have not finalized the report. We hope to incorporate all the information gathered at this conference into the final report. That is why the final report is not available here. Today you were given an 18-page Executive Summary that captures the highlights of the report.

This is a quick overview of what I am going to talk about:

- Why did the Bureau of Justice Statistics (BJS) and SEARCH undertake this project?
- Why are BJS and SEARCH qualified to undertake this project? At least to SEARCH, that was certainly a question that members of the Task Force posed from time to time during our deliberations.
- How did we conduct the project?
- What did we conclude? Just as importantly, what didn't we conclude? What still

[1] Mr. Belair's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_200053100srch.ppt.

[2] Bureau of Justice Statistics, *Report of the National Task Force on Privacy, Technology and Criminal Justice Information*, Privacy, Technology, and Criminal Justice Information Series, NCJ 187669 (Washington, D.C.: U.S. Department of Justice, August 2001). Hereafter, Task Force Report.

[3] Bureau of Justice Statistics, *Public Attitudes Toward Uses of Criminal History Information, A Privacy, Technology, and Criminal Justice Information Report*, NCJ 187663 (Washington, D.C.: U.S. Department of Justice, July 2001).

remains to be worked on?

### Why did BJS and SEARCH undertake this project?

I think the key is that the law and policy for criminal history record information (CHRI) has not changed since the 1980s. Yogi Berra spoke that famous line, "When you come to a fork in the road, take it." We are at that fork in the road. We really have to decide, and will surely decide as a society over the next few years, whether we intend to enhance privacy protections for CHRI, or whether we intend to continue down a path that relaxes those protections. There are certainly good policy reasons on both sides of that issue. I don't think it is hyperbolic to suggest that whether we can effectively preserve any degree of confidentiality — in particular, restrictions on public access and disclosure to the public — is a very real question at this juncture. Law today is not so much an interlocking set of standards as it is stand-alone smokestacks. Information held by law enforcement — the rap sheet, the comprehensive criminal history record — is subject to a bevy of restrictions and controls and standards. The report analyzes that issue in detail, and we will discuss that this afternoon. Information held by the courts remains as it always has in this country, public record information. Because of First Amendment rights and other important considerations, when someone is arrested and processed through the court system, it is a public event. There are compelling reasons why society needs access to that information. That was fine 20 years ago when, theoretically, access was available. And if you really cared enough, if you were family, the lawyer, or a newspaper, you could get that information. But as a practical matter, as a de facto matter, that information was unavailable. Today the information is widely available, and because there is a legitimate demand for access to it, a private-sector industry has emerged to collect, maintain, automate, value-add, and disseminate it.

So it can be the very same information, but if the source is the central State repository or a law enforcement agency, it may not be available. If the source is the courts, it is fully available. If it comes from commercial compilers, it may be available in an enhanced mode with other information tied to it, for a fee. So, as BJS and SEARCH looked at this in the summer of 1998, we felt strongly that it was time, for the first time in about 12 years, for us to take a comprehensive look at this body of law, at the policy, and at the social policy implications. That was the birth of this project.

I do not think I can emphasize technology enough. Technology has changed the whole face of this environment and out-flanked the de facto protections that I talked about earlier. Today court records are automated. They are available with a name index so you no longer have to know what day someone was in court to check on a chronological record. They are cumulative and comprehensive. Not as much so, granted, as the central repository rap sheet law enforcement record, but still pretty good. And, of course, the Internet has galvanized the concern even

more so. We have lots of examples, and more all the time, of CHRI made available on the Internet. The sex offender records are prime. It was interesting to see the Task Force survey showing that 90 percent of the American public makes a distinction between records that are in the public domain — criminal history records — being technically available but not available on the Internet. The American public is more worried about privacy than ever before. I think everyone in this room is aware that there is an unprecedented degree of interest today in privacy that has caused a lot of pressure and dislocations. It is not all bad. There is always a silver lining for your friendly neighborhood privacy lawyer. That has been good. But it has been an absolutely unprecedented phenomenon today.

What is interesting is that side by side with the demand for privacy is an unprecedented demand for access to criminal history records for due diligence purposes, background checks, ID fraud, and all kinds of important purposes. Integration, the very real and important effort all across the country to share, integrate, and make our databases more effective, nonetheless raises real privacy issues. Commercial compilers are another issue. Does anyone here have an idea of the number one user by category, by industry, of the criminal justice and criminal history product put together by commercial compilers?

The answer is law enforcement. The Nation's law enforcement agencies by category are the number one user of the criminal history records and the value-added products that are put together by commercial compilers. Apart from privacy and information policy issues, there is a legitimate demand that is not being met in a way that the investigative side of the law enforcement community feels is adequate.

The Task Force was also fascinated by the distinction between CHRI and other types of criminal history information, which increasingly are being amalgamated into the criminal history record.

We also felt that it was important to take a look at intelligence and investigative information — they have their own sophisticated information systems, often with not just intelligence and investigative information, but criminal history information and other types of personal information — and the relationship of those databases to criminal history record databases.

Obviously, juvenile information is also a big part of our report. It is covered in the survey. We spent a lot of time considering whether juvenile information today, given recidivism rates, the severity of juvenile crime and even allowing for the fact that juvenile crime, like other types of crime, has reached a plateau or even decreased. But allowing for that and taking into account the public fear of juvenile crime and gangs, we considered whether we should look at that as well. We did and it is covered in our recommendations. We will talk about that in just a minute.

We also spent a lot of time talking about the differing kinds of noncriminal justice users. Is there a difference

between governmental, noncriminal justice users who want the information for a security clearance, and an employer who wants the information to do background checks because they are providing services to children? Is there a difference between occupational licensing and insurance fraud inquiries? We tried to sort that out. We also spent a lot of time talking about the claims that the general public makes concerning access to CHRI. After all, it is not a private event. It is not your financial information. It is not your medical information. It recounts an individual's encounter with our criminal justice system. You can make a good argument that society has a legitimate interest in that. Not only to protect the individual and to make sure there are not abusive practices, but also for purposes of oversight regarding our criminal justice system and accountability. And also to keep track from a fairness and credentialing standpoint of who has run afoul of the law and who hasn't. These were lively discussions.

To sum up why we spent a couple of years, and over 6 days of meetings on this project, producing a 200-page report, including 14 recommendations: we really didn't have a choice. We had all the stakeholders and experts together and we had to take a look at what is rapidly becoming a dysfunctional system. We looked at the laws that do not relate to the content and use of the information, or the privacy risk posed by the information. We looked at the public policies, public safety, and risk management benefits that arise from the information, but instead found that the focus is based on source. If the information comes from law enforcement, it is not available or available only to certain users. But if it comes from the courts, it is available to everybody. Or it can come from commercial compilers, such as the Individual Reference Services Group (IRSG), which has self-regulatory privacy standards. In addition, for some of the commercial compilers operating in that space, the *Fair Credit Reporting Act*[4] (FCRA) spells out fairly detailed privacy restrictions. And whether you think that law is adequate or inadequate, there is no question that law and self-regulatory set of standards is very different than the law that applies to the same information held by law enforcement. Those were the kinds of issues we felt we needed to address.

We will talk more about what we concluded and how we went about doing it. But first I would like Kent Markus' thoughts about the background of the project. Do you agree that we went ahead with this because we really felt we were on the verge of having a dysfunctional system and somebody needed to look at it?

**Markus** – I think it is not necessarily that it was a dysfunctional system, but that the privacy of criminal history records was changing. I think you are going to talk about a series of things that were causing the privacy status of those records to change. We realized that change could happen and we could sit by and watch it change without any input as to whether the change was good or bad, and whether it would result in good or bad public policy. Or we could look at

[4] 15 U.S.C. § 1681 *et seq.*, as amended.

why the changes were occurring right now, what was causing the change, and what changes were coming about as a result of *change drivers*. We asked questions about where public policy intercessions are happening because of something that is occurring in society, such as changes in public policy views, technology, or other things that are bringing about a difference with respect to the privacy of these records. We either do or do not like the difference that is coming about. And if we want to have any meaningful input about whether the change in privacy that is occurring is good or bad, we better stop and think about why it is occurring and what possible avenues we might take to cause a different course of action, if appropriate. I think that is a big part of why we thought this was the time to jump in. In other words, I absolutely agree with you.

**Belair** – Thank you, Kent. So that is why we began this project. Now the question is, Why BJS and SEARCH?

## Why were BJS and SEARCH qualified for this project?

BJS has been the lead agency in addressing CHRI and privacy issues and numerous other CHRI information policy issues. BJS/SEARCH CHRI recommendations in "Tech 13"[5] were the template for most State CHRI law. Both BJS and SEARCH were well positioned to undertake this project. The two organizations have been together often, sometimes working separately, but always on parallel paths. They have probably been the major organizations that have researched, proposed, and encouraged the development of policy here.

## How did BJS and SEARCH conduct this project?

**Research**. So how did we do it? We conducted extensive research for a 200-page report that will be enriched by the proceedings here in the next couple of days. We analyzed the structure of the criminal justice information system, and the history of information privacy. It was a great honor to have Alan Westin as a part of our group. For me personally, I have worked for Alan and I have been his lifelong friend. When you look at the history and development of information policy in this country, you start with *Privacy and Freedom*, Alan's book in 1967.[6] His 1972 book, *Databanks in a Free Society*, defined our current notions of fair information practice.[7] The Department of Health, Education and Welfare gets a fair amount of credit for developing the Code of Fair Information Practices in

[5] *Technical Report No. 13: Standards for the Security and Privacy of Criminal History Record Information*, 3rd ed. (Sacramento: SEARCH Group, Inc., 1988). Updates positions taken by SEARCH on the issues of security and privacy of criminal justice information, and shapes them into one comprehensive and orderly statement.

[6] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

[7] Alan F. Westin and Michael A. Baker, *Databanks in a Free Society: Computers, Record-Keeping and Privacy* (New York: Quadrangle Books, 1972).

1973.[8] But at least in galley proofs, *Databanks in a Free Society* had that earlier. As I mentioned, we did look at the structure of the criminal justice information system. We looked at the history of constitutional common law, State and Federal statutory criminal history standards, starting with the President's 1967 Commission on Law Enforcement that calls for the development of the rap sheet. Some of you may know that was the derivation of Project SEARCH. SEARCH began as an experiment to see whether we could automate and telecommunicate criminal history information. We researched the 1973 amendments, including the Kennedy Amendment, which were the first Federal statutes to address criminal history privacy information.[9] We studied the 1976 U.S. Department of Justice (DOJ) Regulations, previously called the Law Enforcement Assistance Administration (LEAA) Regulations.[10] We examined the current status of criminal history law and policy. There is a lot of law out there right now with respect to CHRI:

- Subject access and correction – 51 out of 53 jurisdictions.[11]
- Accuracy and completeness – 52 out of 53.
- Fingerprinting requirements –53 out of 53 (although the nature of the requirements varies a bit).
- Disposition reporting – 53 out of 53.
- Sealing and purging standards – 42.
- Security standards – 42.
- Use and dissemination standards – 53 out of 53.

Largely with respect to use and dissemination, criminal justice agencies get the whole rap sheet. There is a sharp distinction between conviction and nonconviction with noncriminal justice users, and a distinction between governmental and nongovernmental users. The public gets very little access, except in a few open record States like Florida, to the entire rap sheet as it is maintained in the central State repository. The general public has no access to the results of any national search. The law is just as rich and granulated with respect to court records as it is with law enforcement. Generally speaking, court records are fully available. Statutes in a couple of places make distinctions between an automated version of a court record with a name index and physically going to the courthouse to look through the chronological record, and that has been

---

[8] *Records, Computers and the Rights of Citizens*, DHEW Publication No. (OS) 73-97 (Washington, D.C.: Department of Health, Education and Welfare, July 1973). *See*, Task Force Report, p. 11. *See also* www.aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[9] 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 Act must be made available for review and challenge by record subjects and must be used only for law enforcement and other lawful purposes. 42 U.S.C. § 3789G(b), as amended by § 524(b) of the *Crime Control Act of 1973*, Pub. L. No. 93-83 (1973).

[10] 28 C.F.R. § 20.01.

[11] The 53 jurisdictions are the 50 States, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.

upheld. The *United Reporting* decision, which I think Peter Swire talked about earlier, makes a distinction between certain kinds of noncriminal justice requestors — scholars and the media on the one hand and commercial compilers on the other. But bear in mind, it is a law enforcement record that is an issue at United Reporting, not a court record. We will talk tomorrow about the privacy law as it currently applies to commercial compilers. The FCRA is important, and stronger than some people realize. Beth Givens and I will have fun later talking about whether we like or dislike the IRSG standards, but it is a very different set of rules than those that apply through State law and through Federal regulations to the law enforcement records.

**Case studies**. We did three case studies because we wanted an in-depth exploration of three pivot points. We looked at Florida, which is an open records State, and at Washington, which is really a mixed records State. We also studied Massachusetts, which is a closed record, privacy-oriented State. SEARCH previously conducted a case study of Florida apart from what we did for the purposes of this project.[12] The truth is that in a certain sense, all of these various approaches have worked. There has not been a public outcry. Florida is truly an open records State, and frankly, we expected to see lots of problems. There have been some problems, but I think it is fair to say that any one of these approaches can work. It is really a value judgment. What kind of society do we want to live in? Do we want to live in a society where this information is readily available? Post it up on the Internet. Or do we want to live in a society where only certain favored kinds of users can get access for purposes that we think are important, such as background checks for childcare? Or do we want to live in a society that, except for criminal justice and maybe national security purposes, nobody gets access to this information?

**Change drivers**. We tried to figure out what is driving the current environment so we could make policy recommendations that make sense in that environment. We identified 10 change drivers.

- Public concern about privacy.

- The information culture. The Task Force felt that there really is an information culture today. You can get anything about anybody anytime of the day or night. Click onto the Internet. You all know the sites. They pop up, as a matter of fact, when you log onto your ISP. And there is a sense that you ought to be able to get that in this day and age. The ORC survey shows that about 50 percent of the American public, give or take a couple of points, thinks that you can get anybody's conviction or arrest record anytime on the Internet. It really isn't quite true, but there is certainly a culture that believes that we all ought to be able to get what we want, when we want it, and without much rationale or much justification for why.

[12] Paul L. Woodard, *A Florida Case Study: Availability of Criminal History Records, The Effect of an Open Records Policy* (Sacramento: SEARCH Group, Inc., 1990).

- Technological change.
- System integration.
- Criminal justice business models. The catch phrase that we developed was *data driven, problem-solving approach*. That phrase tried to capture the idea that, increasingly, criminal justice agencies are thinking about their users as customers and why they should think of users as customers given that the private-sector compilers have stolen an awful lot of their customer base, i.e., law enforcement investigative users.
- Noncriminal justice demand. It bears emphasis that today over 50 percent of the criminal history record traffic that goes through the Federal Bureau of Investigation is for *noncriminal* justice users, which is certainly a change from where we would have been 10, 15, or 20 years ago.
- Commercial compilation and sale.
- Government statutes and initiatives. The Federal government is a big place where often the left hand doesn't know what the right hand is doing. This Administration, I happen to think, gets high marks on privacy protection. The privacy advocates have criticized them for not going far enough. The industry sometimes gets upset that they go too far. To me, that probably means that they are doing the right thing. They have certainly worked on privacy and have been sensitive to it, but at the same time this government is very capable, and the Congress, too, of enacting laws and publishing regulations that have the effect of enhancing the use and the dissemination of CHRI. You see it in the privatization regulations. You see it in *Megan's Law*,[13] which is the first, along with *Jacob Wetterling*[14] and a couple of other laws that set the legal structure for the various sex offender registries. The *National Child Protection Act*,[15] which encourages and almost requires the States to do background checks to get criminal history information for folks who provide services to the elderly, the handicapped, and to children. A nursing home background law passed not long ago; it wasn't criminal history but it shows you the mindset. The government published something called *Know Your Customer*. Basically it was an attempt to deputize the Nation's banks and get them to snoop into who their customers are, what they do, what their transactions look like, and then report that to the financial regulatory agencies. They got over 100,000 comments and fewer than 200 were positive, which is absolutely extraordinary. It seems to me if you write this regulation, you go and get your friends and your family to get more than 200 positive

[13] 104 P.L. 145, 100 Stat. 1345.

[14] *Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act,* 42 U.S.C. § 14071.

[15] Pub. L. 103-209 (Dec. 20, 1993).

comments. They got 100,000-plus *negative* comments and, of course, ended up withdrawing the rule. I don't mean to pick on the Federal government. The point is, that among the change drivers are governmental initiatives that really encourage the consumption of CHRI.

- Juvenile justice reform is obviously a big part of the current equation. We covered it in the survey. We address it in-depth in our recommendations. The report discusses whether confidentiality and privacy protections for juvenile information have a payoff. Does it contribute to rehabilitation? Do we know how to rehabilitate? Is it a matter of fairness? Does a second chance make sense? We had some pretty heated discussions about that, and obviously we didn't resolve those questions, but we did agree that the relaxation of access to juvenile records is appropriate. That was not without some anxiety on the part of some of the members of our Task Force. The Task Force worked by consensus. Its recommendations do not represent the views of any one member of the Task Force or their organizational affiliation. SEARCH has now adopted those recommendations, so I guess it does represent SEARCH's view or the view of the Membership Group. We hope other groups will adopt the recommendations as well. I am not even sure that I could say at this point that it represents the views of the Department of Justice or BJS. It is first and foremost a Task Force product.

- Intelligence systems. We decided that the membership of the Task Force didn't have the right folks on it to do justice to what has been happening in that area. But we did identify it as a change driver in the sense that the new intelligence and investigative systems are so robust, and reach out across such a wide spectrum of information that they are also changing the environment. They are part of this information culture.

**Relationship between recommendations and survey results**. I am going to finish discussing how we conducted this project, and relationships between the Task Force recommendations and survey results. This was the first-ever survey about the public's attitudes toward uses of criminal history information. It is important to note that the Task Force members did not have the survey results in front of them as they crafted their recommendations. That is too bad. Maybe we should have another meeting in view of some of these findings, to see if it changes our recommendations. Obviously the Task Force started with the premise that there was a legitimate concern about privacy. You can see that one of the things the survey stands for is that the American public still cares about the privacy of CHRI. I suppose having said that, in the midst of a privacy firestorm, it wasn't so clear in the summer of 1998. I could still make the case that the public, or at least its elected representatives, don't really

care about the privacy and confidentiality of criminal history records. I could do it because in every cycle of our State legislatures, and in every Congress, we see new law enacted that opens up access to criminal history information. We felt the role of the Internet was going to be very important. And the survey bears that out. In the distinction between conviction and arrest records, we recommended a continued emphasis on that very important distinction. And you see from the survey that the American public feels much the same way.

We studied the distinction between selected noncriminal justice access and access by the general public. We acknowledged that difference, and the survey reflects that the American public recognizes some hierarchy of purposes and uses. They distinguish that from a willy-nilly access by the general public. Twelve percent of the public favors public access to the complete criminal history record for any purpose. That is a much lower number than I would have predicted, and probably a lower number than a lot of us around the Task Force would have predicted. But still we felt there was an important distinction.

Another distinction was in the use of fingerprints. The Task Force comes out strongly for it, and the American public is pretty comfortable with it. Approval of fair information practices shows the same thing. Another issue was concern about commercial compilers and majority support for applying the same protections to the private sector as to the government. We obviously brought folks from that industry into the discussion. That industry provides an important product for a variety of important services. To the extent that there is a shortfall in accountability and in privacy protection, and a difference in the way the public perceives the dissemination of that information by the government versus the private sector, there was a need to determine whether the same rules could be applied. I was pleased that the survey largely reflects that.

In the area of eroding support for special juvenile record protections, the survey shows that 53 percent of the public wants special protections. Forty percent are comfortable treating serious juvenile offenses the same as adult offenses. That is pretty much where the Task Force came out. The Task Force may have been a little less protective of juvenile records than the American public prefers. It would be interesting to see if other members of the Task Force agree with that characterization.

So, what did we do? In addition to the report, and this national conference, we established a national Task Force comprised of experts in the following areas: the repositories, the courts, commercial compilers of CHRI, criminal justice and noncriminal justice users, the media, open records advocates, privacy advocates, academics, and government officials. These were extraordinary people that came with a life's agenda and work.

We met six different times. At those meetings we reviewed the content of the report and provided

extensive input, especially about change drivers. We reviewed draft survey topics and questions. The Task Force debated and adopted 14 recommendations for CHRI and CJRI. Kent, do you have any thoughts to add at this point?

**Markus** – Second to the recommendations, the most interesting part of the report is the change drivers. It is the attempt to identify what was going on in society that forced us to say there are going to be changes unless we intercede right now. The question we asked was, "What is forcing change with respect to the privacy of CHRI right now?"

**Belair** – I agree. We probably spent the bulk of our time talking about those change drivers. It was not that we did not give a lot of attention to the recommendations, but the change drivers captured a lot of our effort and attention. We felt that it would be an important contribution. One of the reasons we spent so much time on the change drivers, was that when we started the project, we did not expect that this Task Force would actually reach consensus for any recommendation. We purposefully brought together people with fundamentally and profoundly different views about the way criminal history information ought to be handled. We thought that the Task Force would identify issues. That was our goal. It occurred to us at the meeting in Boston that we would be able to say something more prescriptive. We had been concerned that our consensus would break down if we went into too much detail. Here are some of the highlights from our recommendations.

## Recommendation highlights: What the Task Force *did* conclude

**Global rules**. To the extent practicable, law enforcement, the courts, and the private sector should be covered by the same rules for CHRI. There ought to be one set of rules, certainly at a generic level, for the collection, maintenance, use, and dissemination of the same kind of information — criminal history information — and, to some extent, criminal justice record information (CJRI), such as victim and witness information. It really didn't make any sense to have laws so different based on the source of the information.

A new generation of law is needed regarding criminal history and CJRI that considers the content, intended use, transfer, and re-dissemination of the information. To the extent practicable, the law should not pivot only on source. Source is probably a factor that needs to be considered, and as you get into detail, virtually everybody on the Task Force felt there would be circumstances where you would have some different rules for the private sector versus government; certainly with respect to use and access, and even dissemination. But that we ought not to simply say, "Okay, source is not the only factor, but a major factor." And instead develop a new generation.

**Remedies.** We discussed the legal remedies available to individuals whose CHRI is misused. It is remarkable how little case law is available. The reason is that the remedies don't work. They are not any good. The Task Force felt that if we are going to have a credible

system for handling this information, and if we are going to have privacy rules that survive into this new century, we must have effective remedies.

**Fingerprinting**. The Task Force felt that fingerprints continue to be the only viable way to support the integrity of the database and to avoid false positives and false negatives. Now, that is a challenge for commercial compilers. A number of our commercial compilers made the point that even with a name-only check and using Social Security numbers, they have a laudable record of matching the right information with the right person. Nothing in our research discredits that statement. As fingerprinting technology such as LiveScan becomes less costly and easier to use, the Task Force anticipated that the American public wasn't going to be that concerned about fingerprinting. We posited an environment where the fingerprint is used in support of criminal history information both inside and outside the criminal justice sector.

**Sealing and purging**. The Task Force recommended that CHRI should be sealed or purged when the record no longer serves as a public safety interest. We talked about the research findings that suggest a clean record period established by an individual who had been an offender, coupled with age of the individual, is a pretty good predictor that this individual is not going to recidivate. In view of that, there was interest in developing sealing and purging policies that apply, without getting into that level of detail. I was disappointed with the survey results on that. I can be very enthusiastic about surveys when they say what we want them to say. I am hoping we will be able to get an opportunity at some point to go back and look at that again because there are strong arguments to be made in support of sealing and purging in that kind of setting. That kind of discussion is what animated the Task Force.

**Privacy rights.** Record subjects should have enhanced privacy rights, including notice and access to disclosure logs. Privacy rights or fair information practice rights are sweeping the world concerning the inclusion of other bodies of information — financial records, health records, telecommunications records, and so forth. The Task Force felt that more could be done, and the recommendations in the Executive Summary and Report talk about that in more detail.

**Juvenile records.** The message is to treat records of serious juvenile offenses the same as adult records. If you cannot demonstrate some reason for treating the juvenile record as an adult record, then do not do it. But if you can demonstrate a reason, the Task Force was comfortable with the idea that they should be treated the same as adult records. Well over three dozen States have amended their laws over the last few years to relax confidentiality restrictions on juvenile records and to effectively incorporate this approach. That is also the approach in the forever pending juvenile bills that have been in the Congress.

**Profiling.** We know from other surveys and anecdotal evidence that the American public is very alarmed about profiling. In other words, taking one subject matter category of information, a criminal history record, and

enhancing it with financial records, medical records, and other types of information. You end up with a comprehensive picture of this individual. This is a lightning rod for the concern the American public has about privacy. The Task Force felt that criminal history record databases should not house that kind of information. We fought long and hard on this one.

**Integration.** The Task Force obviously wants to encourage integration. It is an absolutely necessary development sweeping the Nation, creating shared databases, shared systems vertically and horizontally for law enforcement, courts, corrections, prosecution, and governmental systems. We certainly do not want to get in the way of that, not that we necessarily could, but we think there is a privacy and profiling threat, and we do think it is an environment where there ought to be privacy and information assessments.

**Conviction versus arrest-only record.** The new generation of law, as viewed by the Task Force, uses one of our traditional principles; that there is a profound difference between a conviction record and an arrest-only record. There is a waiver of privacy attached to conviction information. And, in many instances, there is a strong public safety interest, risk management interest, in getting access to that information. The Task Force thought that less true regarding arrest-only information.

### What did the Task Force *not* conclude?

The Task Force crafted no policy recommendations for CHRI held by the media. Imagine trying to craft a set of privacy standards that tells the media, "You published on Tuesday that Bob Belair was arrested on Monday. And you can hold that for six months or the course of that particular investigation." If Bob gets convicted, you would want to refer back to the arrest, but then you can't automate it. You can't keep it in your morgue. You can't go back to it a few years later. There are certainly folks that make the argument that if you allow the media that kind of automated run of the table, then what do you really do in other places? Does it make any sense to purge and seal records? Can you really add meaningful confidentiality standards with respect to other smokestacks? Those are good questions. And we note that it needs further work. Obviously the role of the media is very important.

The Task Force drafted no policy recommendations for intelligence and investigative information for the reasons that I talked about. We decided that other groups would bring different expertise and different perspectives to taking a look at intelligence investigative records. We all felt that not only are we seeing a revolution of privacy, we are seeing a revolution in information systems. We are going to have information systems that are nimble, that have tremendous searching capabilities, and tremendous computing power. They are going to be able to effectively use and capture all different kinds of information without regard to the traditional subject matter boundaries. We need to be able to address those. And I think one possible approach is to eventually combine the intelligence and investigative recommendations with

these recommendations. Some of you may know that in a different project the Justice Department has already tried to develop an iteration of privacy recommendations for integrated systems. That all needs to come together before we encourage State legislators or the Congress to take a comprehensive look at it.

We didn't do as much work as we wanted to with CHRI and the Internet, and addressing the extent to which information that everybody feels pretty good about being public doesn't necessarily mean they want it to be posted on the Internet. Is that true? If it is true, why? And if it is true, what do you do about it? You could see that the American public in our survey has a point of view that creates a distinction between saying that it is okay that the information is public, but 90 percent of them say don't put it on the Internet. The role of the Task Force was to identify the structure of how to get there.

## Next steps

The SEARCH Membership Group has adopted these recommendations. We are going to seek support for these recommendations from other organizations. The Task Force does call for a statutorily chartered three-year commission to take these next steps. To begin to put real policy prescription into general statements such as, "There ought to be one set of rules for whatever entity is holding and disseminating criminal history information." That is an important concept. It is a platform for a lot of other work, but without that other work, you don't have a legislative vehicle. I have already talked about the intelligence and investigative system. The Task Force recommends creation of a new task force to review privacy issues raised by intelligence and investigative systems.

## Conclusion

In conclusion, I want to say that, as chairman, I think the Task Force was great to work with. It was an overachiever. It out-performed what we thought it was going to do. It is a good start, but there is more work to be done. We continue to be in an absolutely critical period here. I don't think there is anybody in this room that believes that policy and law for criminal history and CJRI is going to stay the same. It is not. It is going to change dramatically and profoundly over the next 5 years, and this is the first start at shaping what that new generation should look like. Now, if anybody has any questions or comments, we have a little bit of time.

## Question-and-answer session

**Q.** I have a question about the Task Force discussions concerning convictions versus what you characterize as arrest data. Certainly there are positive public uses for nonconviction information and some of those might include clearing a person who has been accused in the work place of being involved in an activity that they were found not guilty of. I'm also concerned about dismissed cases where there is a need for additional investigation before a due diligence decision is made.

**A.** (Belair) I agree with you. The gentlemen is making a very good point, that arrest information has a

number of important risk management and public safety uses. There is no question about that. For purposes of this presentation, I was using fairly simplified terms, avoiding that inscrutable term "nonconviction information." But not all arrest information is the same. There is arrest information where somebody has been acquitted. There is arrest information where it was just "nol-pros" or it was dropped, or that looks like arrest-only information. What you have is a missing disposition. So, I want to be clear about what the Task Force said about conviction versus nonconviction information. The Task Force did not opine that nonconviction information, arrest-only information, does not have some of the benefits that you rightly talk about. What they did say is that in fashioning the next generation of law and policy, they see a difference from a privacy and a utilities standpoint between conviction information and nonconviction information. I think that what they have done is to create the platform for specific policies that would make conviction information more widely available than nonconviction, but not necessarily cut off access to nonconviction.

**Q.** My question is along the same lines. Do you think it would be useful to make a distinction? You know in a lot of the discussions when you talk about nonconviction information between situations where you do not have a final disposition, and yet know you do? Even in the survey it didn't make that distinction between those two situations, and they are very different in terms of privacy and usefulness.

**A.** (Belair) I understand that there is a little bit of push back when you use terms loosely. I think the survey folks felt that trying to parcel out and explain to the public the different kinds of arrest-only information, acquittal nol-pros and other kinds of dismissed charges and missing dispositions, was more than you could do in a survey. But the report goes into that. Those are very important distinctions.

**A.** (Markus) I think that the distinction you suggested requires even a further distinction. If this is a no disposition situation or a situation where we have a disposition, it still doesn't take us all the way down the path because we know that even in a no disposition situation, the case may still be pending and we are waiting for the disposition to come. The trial is next week. Or the disposition is missing from the criminal history records. Even with a no disposition, we can have two entirely different situations that play at that level.

**Q.** To what extent did you consider data quality or liability in drawing your conclusions about accessibility to criminal justice data?

**A.** (Belair) We did look at data quality. In the 1980s there was a lot of attention (and rightly so) on the accuracy and completeness of criminal history records. We do not have a recommendation on it but that is an accepted part of the criminal history records scene. It is a responsibility. As to liability, I don't think there are even six reported cases in this country that involve a finding of liability on the part of the managers of a criminal history record

system for releasing information that turns out to be inaccurate or incomplete. So, I understand the construct, which is the more the public gets access to this information, the more there is a risk of the information being inaccurate or incomplete. And we know, despite our best efforts, sometimes it is. There will be uses that disadvantage individuals based on this inaccurate information and, therefore, the possibility arises of liability. It makes sense, it sounds logical, but as a practical matter it has not happened. We did talk about it but we did not spend too much time.

**A.** (Markus) I think there was a correlative point that we did spend some time on. The report says that as accessibility increases, there is an increased obligation on the part of the government to take steps to assure accuracy. That obligation went higher and higher as accessibility increased.

**Commentary from David Flaherty** — I would like to talk about the summary recommendation about the three-year commission to develop detailed model CHRI policies. There are two points that I would like to make. One, privacy advocates have argued in the United States and elsewhere for a number of years on the futility of having gathered together bodies of expertise at the State and Federal level or provincial level, whatever national jurisdiction, on privacy issues because they are extremely complicated. I come from a country (Canada) that has a privacy commissioner and provincial privacy commissioners and so forth. My colleague on the panel, John Woulds, is in the United Kingdom's Data Protection Registrar. I think more than 30 countries in the world have these kinds of oversight mechanisms with various levels of privacy to try to articulate the privacy interests that are at stake in particular situations. The one thing that was clear to me, and I think to other members of the panel, was how complicated these issues are. We went from State to State and started to think about the complexities of a huge country of 280 million people. What we hope, with that kind of a panel, is to have a specialized privacy protection commission for a period of time that would specialize in criminal history information and perhaps even in criminal intelligence issues. There is a real need to have the law enforcement, the public, and the privacy interest, all tossed into a hopper on an ongoing basis with a representative group of people. So, as each State or territory or the Federal government decides to act or modify or change existing practice of law in this area, there is some way of getting some intelligent guidance so the Federal system works.

**Q.** These records have commercial value. Commercial entities come to us all the time and want to buy these records. Quite frankly, we in law enforcement do not have a lot of ability to produce revenue. The records are very valuable. Would you look at this idea as a revenue source and then how do we share this among the courts or prosecutors or sheriffs groups that produce the records?

**A.** (Belair) Well said. The records are indeed valuable and we did look at some of the marketplace realities.

One of the change drivers we recognized was that the criminal justice community is starting to think differently about these records as an asset, as a commodity, as a way to generate revenue. Corrections folks, in States like Michigan and Ohio, have an arrangement with a number of the commercial compilers and vendors to make information available from their data systems. I believe they are generating revenue out of that. Well, far be it for me to suggest that it is bad for lawyers to generate revenue. As David said, this is complicated stuff and it might be okay to do that, but it probably isn't good public policy to do it ad hoc because it is a chance to generate revenue. The Task Force felt the way to do it is in the context of a conceptual approach. What role do the commercial compilers play? Should it generate revenue? What are the privacy risks? What are the public policy and public safety payoffs? And so it really goes to David's point. That is why it is so important to continue this work with a study commission.

**A.** (Markus) Because there is value to those records, and they are being made more available to commercial providers, one of the most difficult public policy problems in this entire area evolves from that point. The entire criminal justice system is changing as to the question of whether anybody has ever done their time, or served their debt to society. As these materials become more available through commercial providers and on the Internet, and are used to impact people's access to housing, jobs, and other things as much as 10, 20, 30 years later, we are changing the way the criminal justice system works. I am talking about whether people have done their time and have served their debt to society and are then allowed to come back and return to the society, or whether those convictions are going to continue to have an abiding impact on their lives forever. That is a key element to the increasing distribution of this information. It is a public policy choice that we have to consider as we all participate in making those records more accessible.

# Day two: The stakeholders of privacy interests

## Day two keynote address

Privacy activities of the U.S. Department of Justice
*John T. Bentivoglio*

# Privacy activities of the U.S. Department of Justice

**JOHN T. BENTIVOGLIO**
*Counsel to the Deputy Attorney General*
*U.S. Department of Justice*

I hope to give you an overview of what the U.S. Department of Justice (DOJ) is doing in the privacy area. Then I would like to reserve some time for questions and answers. Although we do have an ambitious privacy agenda in the DOJ, and more broadly within the Administration, I think it is important to give individuals who are on the front lines of these efforts an opportunity to interact with us on these issues, to ask questions and to define why we are doing what we are doing and get a chance for dialogue. I learn a lot that way too, and that is very important. I also want to thank you for participating in this conference, and for the wonderful efforts of SEARCH, the Bureau of Justice Statistics (BJS), and others in putting this conference together, and for the larger initiative they have underway. These are profound issues confronting society and the public safety community, and I am going to touch upon some of those today.

I understand that yesterday you received a briefing from some experts about how the public is increasingly concerned about these issues. Those concerns run very deep. These issues are important to the public safety community because we rely so extensively on public support and confidence in what we do. If we do not tackle the privacy issues in a thoughtful and measured way, two things will happen. First, the public will lose confidence in us, and that could be devastating. Everyone here should appreciate how important it is that the public respects and supports the law enforcement community. We rely on them everyday to get our job done. If we are perceived as heavy-handed in this area, insensitive to the privacy implications of our law enforcement and public safety efforts, they will lose confidence in us and that would be a terrible result. The second thing is that other people will step in to address the public's concern. The public safety community has enough leadership, vision, and commitment to tackle these issues themselves and it would be much better for us to do that. But I have to be candid: if we don't do that, other people will step in and address these issues for us. And that is why what you are doing today and what the Task Force has been doing for the past 18 months is so important because we need to tackle these issues ourselves, and we can come up with a very good result if we do.

## DOJ and privacy

Here is a brief overview of what the Department of Justice is doing in the privacy area. In August of 1998, Attorney General Janet Reno established the Privacy Council within the Department and created the position that I serve in, the

Chief Privacy Officer. She did that to try to give more attention and focus to these issues within the Department. So many of the activities that we engage in — whether it is investigative efforts, grants to State and local agencies to establish information sharing systems, the whole range of issues — have a privacy impact. Attorney General Reno recognized that we needed a more structured approach to these issues within the DOJ. To be candid, there are many people who care about privacy issues in the DOJ, but at base we are a law enforcement and public safety agency, and without a structure within the Department to raise these issues and deliberate about them in a thoughtful way, they may not get the attention they deserve.

So the Attorney General established the Chief Privacy Officer position and the Privacy Council to tackle some of these issues. The Privacy Council is comprised of approximately 20 senior representatives from various agencies like the Federal Bureau of Investigation, the Drug Enforcement Administration, the Office of Justice Programs (OJP), and other key components in the Department. We meet monthly to address a whole range of issues, including privacy and affirmative enforcement because we have an important role in enforcing laws that protect privacy or workplace privacy. The Attorney General is committed to leading by example, and in that sense workplace privacy is important because we need to be fair to our employees even as we discharge our public safety mission. I am also pleased that the FBI Director Louis Freeh saw the benefits of this approach and established a privacy council within the FBI. He did that on his own to his great credit. That council is chaired by Pat Kelly, a thoughtful and energetic person, who is doing a wonderful job.

Among the things that we are doing to address privacy issues within the Department, primarily through the council, is working diligently with OJP on efforts to assist State and local and tribal agencies in establishing privacy policies and practices. I will touch upon a little bit of that and other speakers may address that in this conference. But I have heard many times from thoughtful State and local law enforcement agencies that they already understand that privacy is important. What they could use is some technical assistance and support in specific areas. If we are committed to privacy, what should we be doing? What kind of principles should we establish? What kind of practices? What are the right balances between our public safety mission and our obligation to protect individual privacy? We are trying to engage on those efforts. We don't want a top-down approach. The efforts of OJP and BJS and others are very collaborative as the broad representation of this conference shows. But we need more than dialogue.

We need some assistance and some consensus on what those practices should be. OJP is putting together a number of documents like the privacy design principles and the privacy impact assessment to try to assist State and local agencies to do that. Significantly, they will not be binding. This is not something that we are going

to impose on others. But through a largely consensus process we hope to achieve some common understanding and agreement about where the line should be drawn, and hopefully those will be models throughout the criminal justice system. Significantly, unlike the private sector, we — the Federal government and the DOJ — are already bound. We are already bound by a set of fair information principles, as codified by the *Privacy Act of 1974*.[1] I raise that because one of the things that we have done within the Department is to assess our own compliance with the *Privacy Act*. That law was enacted in the mid-1970s and lots of things have changed since then. But those bedrock principles in the *Privacy Act* have not changed and we are obligated to comply.

## DOJ compliance effort

At the President's direction, we undertook a year-long review of our compliance with the *Privacy Act*. I was happy to report that we found ourselves to be almost in complete compliance. But candidly, there were areas where we were not. There were areas where systems notices hadn't been published, and where we hadn't done some important housekeeping measures. And so we have come into compliance. It is important that we did that because the *Privacy Act* embodies a set of fair information principles that are binding on us. It is particularly important that the DOJ comply with the law. We take that obligation seriously, and I was pleased with the results of our review.

In addition, we are grappling with many issues that the private sector is also grappling with concerning our electronic activities, particularly the operation of our Web sites. There are pretty clear guidelines in the *Privacy Act* about how we should address these issues, but in our effort to try to expand our E-government services as part of a broader Administration initiative, we need to make sure that we are complying with the same rules that the public sector is under an obligation to comply with. For example, we have to review our Web site policies to make sure that we weren't inappropriately collecting information from children. If you are operating Web sites or trying to use the Internet or information technology to deliver services more quickly, more efficiently, at lower cost, I would urge you to take those issues seriously. Those issues should be taken seriously, not just because it is the right thing to do, but also because if you do not, there could be a certain amount of public embarrassment if it is determined that you are not even complying with the basic rules with respect to privacy practices for Web sites.

## Public concern about privacy

All of this takes place, as you know, in the context of growing concern about privacy. And I want to touch upon a couple of issues that I think are profoundly for the public safety community. I don't have all the answers here. As I said, OJP is working on a collaborative effort to develop some principles and guidelines in this area, but there are a couple of issues that I wanted to touch upon today. The first is that it is important to

[1] 5 U.S.C. § 552A, as amended.

keep in mind, and important for the public safety community, to promote the notion that public safety and law enforcement and privacy are increasingly complementary. Beth Givens from the Privacy Rights Clearinghouse will touch a little bit upon identity theft later on in this conference. That is an area where privacy and law enforcement intersect. Increasingly there is a threat to individual privacy with respect to data security. And when you talk about Internet fraud, many of the schemes involve severe violations of individual privacy. It is important to keep in mind that our efforts to enforce the law are totally consistent with and support the notion of safeguarding individual privacy. It is important to keep that in mind because the public would strongly support our efforts in this area. So, as we go into the information age, public safety and law enforcement and safeguarding are increasingly complementary. It is important to continue to focus on that.

As I already touched upon, the issues of public confidence are important and I want to reemphasize that. I am not sure the law enforcement community has always been sensitive to these issues. We have largely pushed and looked at the equities with respect to public safety and law enforcement, and we have prevailed. The public has supported us in that notion. But we can't be too far out in front of the public in the investigative authority that we have, such as our ability to obtain sensitive records, financial records, medical records, and the like. The public is increasingly concerned about that and we need to have a more deliberative approach to these issues. The law enforcement issues are not exclusive. Frequently they should prevail, but not all the time. If we only look at the law enforcement equities, I think we lose public support and other people may step in to craft the rules for us that wouldn't strike the right balance, and wouldn't address our equities. So in this sense we need leadership from people like you to look at these issues, to really think through the privacy implications, to step back and ask, "If I were a citizen, what would I want the rules to be? Would I want there to be unfettered access? Or would I want there to be standards where we can get the information that we need or use it in the ways that we need, but under appropriate safeguards so the public can be confident in what we are doing?"

## Public safety and the private sector

Another issue that we need to grapple with that I know is on the agenda at this conference is the increasing interaction between our public safety efforts and the private sector. In the past, we never had to deal with companies that were compiling all the information that we hold so dear, and that we are under a legal obligation and an ethical obligation to protect. They are compiling that information and selling it. We need to think through these issues because if we force people to turn to those companies to compile that information, they may be getting the same information that we are taking great pains to protect, only it may not be as accurate as the information that we have. It may not be as reliable. More

importantly, citizens may not have a chance to correct the information in the private databases, where they do have some legal avenues to correct inaccurate data that is in public databases. So we have never had to face these issues before, and we need to address them sooner rather than later.

Another issue is the tension between protecting individual privacy and open access of government. We saw this played out recently with respect to financial disclosure forms for judges. Judges were understandably concerned about allowing access to their personal information that is on their ethical disclosure forms. They didn't want that information compiled by private companies and posted on Web sites. I don't think you would want that information posted about you on a publicly accessible Web site. But that information is public and the ethics rules are designed to enforce accountability. I don't think it makes much sense to have different rules so it can be accessible in one form in the off-line world, but not in the online world. One of the ways we need to grapple with that is to ask what information are we collecting in the first place? One of the issues that came up with the judges was that sensitive information could be posted on the Web. Well, if it is sensitive and it doesn't fulfill the obligation or the need for public accountability, why are we asking for it in the first place, even if it is available off-line? So we need to go back and look at the kinds of information we are collecting in the first place. We always have to be thinking when we are engaged in information collection and disclosure in the off-line world that this is going to be available sooner or later in the online world. And is that the type of information that we want? That is the right balance to strike so we are comfortable with the information we are collecting and disclosing regardless of how that is done, off-line or online.

## Future privacy challenges

Another issue we are facing is the inexorable march of technology. As difficult as the information-sharing issues that are largely on the agenda for today, they pale in comparison to the issues that will confront us in 10 or 15 years — biometrics, face recognition, and DNA analysis. These are the next set of privacy challenges for the public safety community. I will give you one brief example. Right now companies are working on face-recognition technology that could be deployed, for example, in airports. That would be a pretty powerful tool. You could imagine why that would be pretty helpful if we had pictures of terrorists, for example, and we could deploy that at airports so it would be noninvasive. You wouldn't even know it was there. And yet we could potentially catch terrorists. Now that is a pretty good idea. On the other hand, would we stop there? Would we use face recognition technology to catch drug traffickers, pedophiles, anybody who is wanted for a felony? Would we limit it to airports? Would we use it at public gatherings where the potential for violence could be significant, but maybe those gatherings are really to protest against government actions and you get into First Amendment

implications. So I don't want to underestimate how difficult the challenges are for information technology. They are going to be even more difficult as this inexorable march of technology proceeds. What we need to do is address these issues soon because we need to harness these technologies to boost our law enforcement efforts. We can catch a lot of criminals. We can reduce crimes in these ways in very effective manners, but these powers need to be exercised within appropriate safeguards. We need to make sure the public is informed about what we are doing so it is not a Big Brother type situation, so we are not trying to hide what we are doing from the public. If we are thoughtful and measured in our approach, they will support us. But we have to be thoughtful about how we do it.

## Conclusion

Finally, I want to say that addressing these problems through collaborative efforts really is the future. It is not going to work if law enforcement and the public safety community marches alone in its efforts. We are going to have to work within industry. For example, we are dealing with computer security issues these days and the industry is suspicious of law enforcement. They are concerned not only about our efforts and how, for example, hacking investigations might impact on their stock market price. But this community is filled with a lot of people who are skeptical about government powers, particularly law enforcement. We can't have a situation where we have an effective computer crime and computer security policy if it is really an adversarial process with industry. Now that doesn't mean we have to operate solely by consensus, but we need to expand the groups of people we are talking to, and that are involved in these efforts to include industry, academia, private sector, privacy advocates, and others. If we can get a consensus in some of these areas, it would be very powerful for us. We could march forward in our law enforcement efforts confident that the public and others will support us. That is a model for the future.

Those are the issues I see on the agenda for the law enforcement and public safety community in the next couple of years and beyond. Again, the technology issues are going to be with us for the foreseeable future, and are important issues for all of the careers of the people in this room. So if you have thoughts on these issues, I would be happy to incorporate those into our privacy efforts and more importantly, as you engage in the discussions today and go back within your own agencies, to think about some of these things and to really take the initiative. I have worked with the law enforcement community now for 14 years, and it is a wonderful group of committed and dedicated people. Working together we can tackle these issues in way that really meets the public safety mission that we all hold dear, but in a way that is sensitive and respectful of individual privacy. Thank you and I will be happy to take any questions.

## Question-and-answer session

**Q.** (Robert Belair) What do you anticipate the Justice Department doing over the next year or so on the criminal history record issues that we have talked about here, and also with the DNA and privacy recommendations. How does that relate?

**A.** With respect to DNA, last year the Attorney General asked the National Commission on the Future of DNA Evidence, which is chaired by Chief Justice Shirley Abrahmson from the Wisconsin Supreme Court, to expedite their review of the privacy implications of forensic DNA. While the technology and its ability to catch criminals is so powerful, the privacy considerations seem to have lagged. Questions were asked, such as: Should we test everyone who is arrested? Is DNA testing like a fingerprint (in many ways it is)? Should we retain DNA samples? The intersection of whether we start testing arrestees and keeping samples is profound because you have a complete DNA picture of someone available if you want to test that sample. So they have come up with their recommendations recently and we are looking at those right now. They did not have really definitive recommendations. They called for further study on some issues. The consensus in the law enforcement community is, at least with sample retention, that we should not destroy samples. It is going to be a tough issue for us as we confront sample retention and arrest policies. With respect to criminal history records OJP, through its efforts with SEARCH and others, is grappling with those issues. You know there are standards already on the books about how we handle criminal history information. We are going to need to start looking at enforcing those regulations in some form to make sure that everyone is in compliance.

**Q.** (Belair) The reason I mention the DNA Commission, John, is that we talked yesterday about the recommendation of the BJS/SEARCH Task Force, which is to establish a statutorily chartered, three-year, comprehensive and detailed effort to look not only at the criminal history record and criminal justice record information, which was the focus of our effort, but also to look at DNA, intelligence and investigative information, and some of the other issues that are related. It was the sense of our Task Force that, ultimately, information policy and privacy policy has to take a comprehensive look at all of that together.

**A.** The sense of the Task Force is right — that to look at these issues in isolation is a mistake. As I said, when you look at DNA, it is analogous in some, but not all ways, to a fingerprint. How we handle it needs to be considered in the context of our broader criminal history, criminal record policy. Doing it in isolation would be a mistake. The flip side is that it is hard to make progress in this area. There are a lot of task forces looking at privacy issues and they do things like I did today, which is to *issue spot*. I think that a lot of people in the room could issue spot these things by themselves. What they need is some guidance and guidelines, and that is why I really

commend the OJP effort to try to develop privacy impact assessment documents and privacy design policies because there may be some people who are already part of the choir. They don't need to be preached to. They need to be given some model music if you will — to kill that metaphor completely. Any other questions?

**Q.** You are not the first speaker to express concern about databases that private companies might compile. Could you elaborate a little bit on what those concerns are and how those databases might be misused?

**A.** I wasn't saying that those databases would be misused as much as private companies are compiling information like arrest records into databases. And that information is accessible for a fee to anyone. Yet government agencies are either under a policy or a legal obligation to protect that information from public disclosure. I was asking if that makes sense anymore. Does it make sense to protect information that in the old days was not available, and it did protect individual privacy? Whereas the current policy or law may just drive them to private companies. One, it is expensive for us to do that. Two, it is inconsistent with the notion of public records since arrest records individually are public records. And three, they may not have accurate information since there is no legal right of people to correct the information in those private databases. So we need to rethink whether the current legal or policy restrictions make sense. But I was not saying those databases are necessarily a bad thing.

**Q.** So is your concern specifically about arrest records, as opposed to other types of records?

**A.** No. I used that as an example, but I think it would apply to other records we are holding in confidence legally or as a policy matter, whereas they are available from others for a fee.

**Q.** So the issue is permissible purpose perhaps, or the existence of the database?

**A.** There are privacy issues with respect to these databases. Can people correct the information? Do they have access? Do they know what is in them? One of the concerns people have is if there are these big databases out there and they don't have any access, but that information can be used to their detriment in insurance or employment decisions. Is that fair? I am not sure that it is.

**Q.** Specifically in terms of the uses that you mentioned, the *Fair Credit Reporting Act* is protection for consumers and does require that before information is acted upon or reported out that it be current within the past 30 days. The reason why many companies resort to creating the databases is not because they want to or it is a fun exercise, but because the information is not easily accessible, although publicly available.

**A.** And, for example, if you are a private-sector company doing childcare, you may want access to that information because you want to screen your employees, which is a completely appropriate use

of that information. I am not saying they are inherently bad but there are profound privacy issues that they raise.

**Q.** Could I just follow up on your statement that maybe some of this stuff we are protecting should no longer be protected because private agencies have it. To carry that further into the issues of expungement, diversion programs, juvenile records where employers are now able to get — through these private agencies — expunged records that no longer exist publicly. You raise the issue of whether we should reexamine the whole question of expungements and diversionary programs in the secrecy of juvenile records because they are otherwise available in the commercial sector.

**A.** I think the increasing private sector effort to collect this information and make it available raises all those issues.

**Q.** Do you have any initial thoughts on those?

**A.** I have personal views, not ones that are cleared or represent the DOJ's view. I think there is a very important public policy purpose behind expunging some juvenile records, nonviolent records, to give people a clean start as they enter into their adult life. And we do face increasingly the problem of a class of people who could be permanently unemployable if old information constantly follows them around as a black mark making it difficult to employ them in various professions, particularly low-end professions. Again, those are my personal views. Where do you draw the line? I don't have a proposal for you today, but those are profound issues. On the other hand, if society is not willing to impose those safeguard obligations on the private sector, then I think the public sector needs to say, does this make any sense for us to engage in all of these efforts to safeguard it when the information is available for a fee and probably easier to get to. Again, thank you very much.

**Government holders of criminal justice information: The role of the courts**

Should the courts continue to be an open public records source for criminal history record information? What are the implications for juvenile record subjects?

Reaching a balance between public safety and privacy
*Hon. Thomas M. Cecil*

Juvenile courts today
*Hon. Gordon A. Martin Jr.*

Panel question-and-answer session

## Reaching a balance between public safety and privacy

**HONORABLE THOMAS M. CECIL**
*Judge, Sacramento County Superior Court, California*

Let me begin by making a couple of disclaimers. One, I am no longer the Presiding Judge of the Sacramento Superior Court. I have had the privilege of doing that for a number of years, but I am the former Presiding Judge of the Sacramento Superior Court as of January 1, 2000. In deference to the current Chair of the California Judicial Council's Court Technology Committee, who happens to be in the audience, I am no longer the Chair of that Committee either. I guess that allows me a certain flexibility to travel about and to participate in ventures such as this, including a number of projects I have been involved in with SEARCH.

This panel's moderator, Fran Bremson and I have talked about the title of this particular topic. Should courts continue to be an open records source? From a technological point of view, that topic title always bothered me because, quite frankly, we are not open records. As most of you know when it comes to digital records, or electronic records, the vast majority of courts in this country do not make their records available digitally. So I am viewing open records in a more narrow sense. Should we continue to provide access to criminal court files in paper form? And second, in the event that they become digital, what are the ramifications of exposing a digital criminal record for public access? In virtually every court in this country, a person has the ability to find out the criminal record of an individual. It is a fairly simple matter. All you need to know is the date of birth, current address, and Social Security number. You need to find the right court. You need to find a place to park or transportation to get there. Once you get there, you need to find the right room. You need to get in line. You need to hope that there is somebody there willing to assist you. You need to ask for the file and hard copy. You need to scour it on the premises. You need to find the page or pages you want. You need to potentially understand what you are looking at, and then you need to pay for copies. It is quite simple. And, of course, in California if you wanted to know a California record to which you are not entitled in terms of criminal history, you would only have to do that at least 58 times, one for each county, and quite frankly, more frequently than that.

Because of the time and the expense and the absurdity and difficulty of doing that, we have, and I think we all acknowledge it, some form of de facto privacy as it relates to our criminal backgrounds. Unless you are on that list, which is growing year by year, of people who are entitled to the pure criminal history, you are fairly safe and secure in terms of not having those "public" records made available publicly. There is a common law right of inspection, which must be reconciled with a legitimate countervailing public and private interest that applies to those records.

It is clear that access to criminal records — judicial records, that is — is not absolute and never has been. Courts have the power to limit access to records sought if they are going to be used for improper purposes. Courts have the power to limit access to records sought if they are being sought to gain a competitive advantage. Courts have both statutory and case law authority to close hearings and to seal all or portions of individual records or hearings. In California, we are one of the few States that actually have a constitutionally protected and created right of privacy. There are many records. They are open and available for public inspection, but only for a small period of time. An example in California is a probation report. It is available as a public record for only 60 days. And I am sure you have your own examples in your own States.

As John Bentivoglio just said, what is needed in this environment to address the impact of the digital revolution is a thoughtful and deliberative analysis of these complex issues, recognizing that there is a general presumption in favor of public access. Technology brings to all of us in the justice community a host of potential benefits: less duplication in terms of data entry, ease of communication, a higher level of accurate data, and better and fairer decisions — both pretrial, at arrest, post-trial, and post-sentencing. It gives us the potential to completely reevaluate and reengineer how we do business, and those are all worthwhile endeavors. I am sure the public would support them, but there are serious ramifications that flow from a digital universe and a digital database that is available to the public at large. I am concerned with the constant, and I don't want to overstate this, the constant call for increased public access to the courts because I am not quite sure if everybody understands what that means, or if everybody has the same definition.

If you take all the positives that come from an automated court system, you will have greater public access because you will have a more efficient court system. You will have a more cost-effective court system. You will have faster and better decisions. You will be able to do more work. And in that respect, public access to the judicial branch should be substantially enhanced. We will be able to do more and to do it better.

I don't think that the cry for public access translates into, "Give us everything you have regardless of how personal, how sensitive, how horrific." And I think that the evidence that we heard yesterday from Dr. Westin's survey bears that out: that privacy remains a critical issue to the public in this country. Dr. Westin was not exaggerating when he said that the Task Force had a critical eye on his survey instrument. I am generally pleased with the results of that survey because I like the results. I was gratified by them. I think it is important and positive that the public has a positive attitude about the judicial system. I am encouraged by the public's ability to distinguish between juvenile offenders and adult offenders. I am comforted by the larger percentage of the public who seem to think that criminal history information should be available, but in

large part, only if you have a legitimate need for it, and not just idle curiosity. But I have some serious concerns about what the widespread availability of criminal history will do to the concepts that exist in virtually every jurisdiction in this country relative to expungement, rehabilitation, forgiveness (however you want to phrase it), diversion, etc.

In keeping with my promise to the other members of the panel to keep my remarks brief, I want to note that it is not just the individual person who is either arrested or convicted that is at issue here. Certainly the arrestee or the convicted party is an unwilling participant in the criminal justice system, but there are other people that are just as unwillingly participating, whether they are the victims, witnesses, or jurors. Those people also have legitimate privacy expectations that need to be protected and respected, especially since many States, including my own, have statutory protections specifically for those people. For instance, in California if the person is convicted in a criminal case, we are not allowed to have a record available to the public that discloses the jurors' names. We find ourselves in the midst of trials in an effort to help out the court reporters referring to jurors by numbers. That is not exactly a warm and fuzzy thing to do. Apologizing when we mistakenly refer to someone by name, saying, "I am sorry Mr. Jones. I meant to say number three." The court reporter glares at you because we have to go back and redo our official transcripts and then have a sealed code that ties, for appellate review, the name of the juror to the particular number.

None of us in the justice community wants to be the entity that stubs the toe, that creates that huge outcry. I don't want the judicial branch to be the goat and I fully honor and respect what John said a moment ago that the loss of confidence that we will suffer is indeed something to be concerned with. If we breach the public trust in the area of privacy, the loss of confidence is going to be immeasurable. But there is something that will be measurable and that is as my branch of government or your branch of government are seeking funding for information technology, if we don't take appropriate steps to ensure an accurate, realistic, and well thought out balance between privacy and public safety, we don't deserve as the judicial branch to get our information technology funded. Thank you.

# Juvenile courts today

**HONORABLE GORDON A. MARTIN JR.**
*Judge, Massachusetts Trial Court*

I only have one disclaimer to make. I have now finished my 6 years as a Trustee of the National Council of Juvenile and Family Court Judges.

The juvenile courts of this country, of course, historically were not an open public records source in any sense. And it was just a year ago that we celebrated the centennial of our country's first juvenile court in Chicago. Then it was St. Louis, and Boston in 1906. By 1911, there were 19 other States and by 1925, 46 States. We must have been doing something right. Today, every State has long since had a specialized juvenile or family court with exclusive original jurisdiction for delinquency, except for what has been taken away from them by the panic legislation of the last decade.

Did anybody turn on *Good Morning America* and see the story of Nathaniel Brazill? You know about Nathaniel Brazill. Thirteen. Seems like a very good kid. Award winner. Honor student. Peer counselor. He was playing with water balloons and was sent home from school, got a gun from his grandfather, came back and shot a teacher who had two very young children. It is tragic for the teacher, his widow, and the children who will grow up without their father, and tragic for Nathaniel Brazill.

He is no longer relevant to our Task Force. He is irrelevant to our conference because once he is indicted, there is nothing we can do for that 13-year-old water balloon player. He is just an adult. One thing we have to keep straight as we deal with this topic today is that once kids are taken away from us, they are not juveniles anymore, even though they are 13, for any practical purpose we are discussing. The theory of the juvenile court was to keep children away from hardened criminals, to keep them away from adult offenders, whether as detainees and as delinquents. Since the child was charged with delinquency and not to be considered for a criminal record, the juvenile court proceedings and records were closed to enhance prospects for treatment and for rehabilitation. Five years ago, I wrote an article for the *New England Journal on Criminal and Civil Confinement,* "Open the Doors: A Judicial Call to End Confidentiality in Delinquency Proceedings."[1] I wasn't the only juvenile court judge with that approach because we were concerned whether the juvenile court would last. Anything that is done behind closed doors is subject to mistrust and misunderstanding. The general organizational statement was this: "Traditional notions of secrecy and confidentiality should be reexamined and relaxed to promote public confidence in the courts' work. The public has a right to know how courts deal with children and families. The court should be open to

[1] 21 *New England Journal on Criminal and Civil Confinement* (Summer 1995).

the media, interested professionals, and students, and when appropriate, the public, in order to hold itself accountable, educate others, and encourage greater community participation."

None of us advocated the indiscriminate dumping of kids into adult court once they committed a violent offense, because, like Nathaniel Brazill, there is nothing we can do for the indicted juvenile. Two-thirds of 1,000 people recently polled by the *Washington Post* believed that children were getting more violent, yet youth homicide arrests have dropped by 56 percent between 1993 and 1998. I consider it a tribute to the public's common sense, however, that 53 percent favored keeping what disclosure restrictions remain. It should not be a surprise that 69 percent of African Americans questioned felt the same way because the disproportionate incarceration of minorities remains a burning issue of concern to all of us involved with juveniles.

What is going on in our juvenile courts today? Forty-two States allow the names — sometimes even pictures — and court records of juveniles charged with delinquency to be released to the media and/or the public. Eleven States have followed the position that other judges and I recommended 5 years ago, of opening up delinquency hearings regardless of the age of the juvenile or the offense the juvenile was charged with. I don't think there will be any more sustained interest in our ordinary juvenile violations than has been the case in ordinary adult offenses, but it may be that there will be a puff piece or two written about the juvenile success stories that do exist.

There are two types of juvenile court records, legal and social. With the legal: the complaints, transcripts, judicial findings, and orders of the court, are all open. They will quickly fall into what Justice John Paul Stevens referred to 11 years ago as "practical obscurity" in that morass of court records. The social reports of a probation officer, the family background, and the personality of the juvenile are nothing that courts should provide. In any case, a diligent reporter will find it all out from neighbors and schoolmates. Remember again the common sense of those polled by Opinion Research Corp. Ninety percent said, "Post no records on the Internet." What they didn't say, but clearly meant, was to let those records remain where they are. Open? Sure, but in "practical obscurity." Thank you.

## Panel question-and-answer session

The role of the courts —
Should the courts continue to be an open records source for criminal history record information? What are the implications for juvenile record subjects?

**Q.** (Francis Bremson) Are you both suggesting that the solution to striking a balance between protecting the rights of privacy and providing public access is to leave hard copy records the way they are, and not make court records electronically available on the Internet or otherwise?

**A.** (Martin) You bet.

**A.** (Cecil) No. I know nothing about juvenile law other than the fact that I poorly raised two. There are many things the public would benefit from, separate from criminal histories. I mean, there are all kinds of things that courts are putting up on their Web sites, whether they are whole case files or indexes only. They are tremendously timesaving devices for the public. For instance, in my county we no longer have people coming in and sitting there going through a paper or microfiche registry. They know that in Sacramento County they can do their search online and come in with a case number. It has saved a tremendous amount of money and that is just a tiny example. I am presuming the question deals with entire case files, and I think there are some types of cases that lend themselves to that, and I don't see anything wrong with it. I don't include juvenile. I do not include family. I do not include probate. I probably do not include many things that are attributes of criminal files, but there are a lot of other things that are perfectly appropriate to be disclosed on the Internet. That is one concept of public access that is perfectly fine. Thirteen States actually have Rules of Court in place. Two States, including California, are diligently working on improving their Rules of Court related to electronic access. It has a place because many courts are State-funded. If the courts don't agree with rules that are foisted upon them by the legislature, they will simply not go digital. They won't do it if it is too cumbersome, time-consuming, or too expensive. Talking about redaction, if you have a digital record but you are going to have to hire staff to go through those records and do all this careful redaction before you release it electronically — if it is too complex — they are just not going to do it. I can assure you, at least in California, the State is not going to fund us well enough to do it that way. It better be simple. It better be clear, and we better make sure as a group that what we are releasing is not going to come back to bite us.

**A.** (Martin) My quick response was obviously in the specific context of juvenile cases. I am pleased to say that Massachusetts has kept things pretty closed, and has a very active Judiciary Media Committee. A report has recently been issued on guidelines to the public's right to access to judicial proceedings and records. Both the court and the media agreed about what

should happen and how it should happen. I think that kind of cooperation between the judiciary and reporters is a very important thing and should stay that way. I stand by my very strong statement, and I don't think I differ from Tom in that respect, that there are some juvenile records, such as the psychiatric report that will be delivered to Nathaniel Brazill's lawyer this afternoon, that should not be released by the court. I am not naïve about the press. The likelihood is that someone will leak it. That is one of the frustrating things.

We must stand for what we believe should occur. It is great for a court to have a Web site with directions to the courthouse, with some kind of cooperation at the counter when somebody arrives. I am not so keen about having things available to the midnight browser. That is all.

**Bremson –** Questions from the audience?

**Q.** Judge Cecil mentioned online access. Maryland is currently considering something that would dovetail with one of the Committee's recommendations, which is to have the same laws and rules that apply to the central repository also apply to the criminal records in the court file. We do have our records quite computerized now and in order to implement this recommendation; it will require us to severely restrict what is currently a liberal policy on dial-up access. Did the Committee consider these issues? I heard Judge Cecil say that he would recommend some dial-up access and I wonder how far you would go with that and how restrictive you would be as far as the commercial compilers and others having dial-up access.

**A.** (Cecil) I am speaking purely from a personal standpoint as a judge and certainly not from my court, my branch, or anybody else. The legislatures around this country have taken great pains to delineate public policy as to what a criminal history — a criminal record, a conviction, an arrest — can be used for. John was asked the question in response to a comment he made about commercial compilers. I probably have a slightly different take on it. There is something that should concern the public at large when the following is a reality: In Sacramento County, a county of about 1.2 million people, we have approximately 500 people a month coming into our courthouse and manually searching through criminal files, taking notes, making copies, and prancing out the door. I know that because of the laws we have in California they cannot be absolutely assured that the person they are looking for matches the file they are reviewing. I know from having talked to some of the staff who work in our court that the people who are doing these reviews are not necessarily the most sophisticated people on earth. They are not people who are making $100 an hour. They are not people who necessarily understand the minute orders they are reading, even if they can read the hand-written minute orders. They have no way of knowing if the files they are looking at are complete, if they are timely, if there has been an appeal, or if there has been an expungement. That is probably a bad example. I would hate to say the file would still be sitting there if

there were an expungement. But believe me, it is possible. What are they doing with that information? It is no big secret. They are using that information to deny housing, insurance, benefits, and jobs in direct contravention of public policy.

Personally, I could not care less if we closed down public access to individual court criminal records. If you want to find out what is happening at a criminal court, show up or watch it on TV, hear it on the radio or read it in the newspaper. But I would much prefer, totally personally, to give the money to the people who collect the information and honor the legislative commitment concerning who should have access to it. Whatever that policy happens to be, whether it is by CD-ROM, or whether it is on the Internet or through the Attorney General's office, those are public policy issues we are avoiding by allowing access to people who don't know what to do with what they have. It bothers me and maybe it bothers others. I have made that suggestion to the California Attorney General's staff and they just groaned in terms of the workload. The reason they are groaning is because they are not going to get adequate funding to do it. But that is my response.

I have one last tidbit on that. A question was raised in a forum a number of months ago about the quandary the commercial compilers may have. We are between a rock and a hard place here. You know we have all this information. We know what the rules are in terms of using it. We are not going to tell you exactly how we got it. We have a client on the other hand who wants information. We are not quite sure what to do. Do we follow the law or do we honor that client relationship and turn it over? I did not have a great deal of difficulty with that question. You know the answer is to comply with the law. If the response is going to be that the tort system in this country is in such a mess that a person is going to be held civilly liable for negligently hiring somebody who has a record that was not legally disclosable, then you ought to deal with changing the tort law and not violating existing law.

**A.** (Markus) The only quibble I have with the Judge's discussion is that it suggests that the public policy choices have all been made and carefully thought through. One of the things we have talked about throughout the conference is that many of the public policy choices that exist in statute were made a long time ago and were made in a different era, with a different context and different technology. The changes happening now are forcing us to rethink what may well be public policy choices that exist in statute. Open record laws suggest that certain records are to be made available, but remained de facto private because of the technological circumstance. We need to think more carefully about that nexus of points that the public policy choices articulated by the legislature were not necessarily articulated in the current environment.

**A.** (Martin) I want to reemphasize that the juveniles who have committed a violent act are already in adult court under the law changes of the last decade, and you do not have to worry about whether there is juvenile discretion

protecting them. It is not. They are "adults" even though they are 13-year-olds.

**A.** (Cecil) I would like to thank SEARCH for the efforts they have made, not only with this particular conference but a variety of Task Forces. Lots of high quality work is going on around this country and around the world for that matter, including Canada, the United Kingdom, Australia, the National Association of State Information Resource Executives (NASIRE),[1] the National Association of Court Managers (NACM), the Office of Justice Programs, SEARCH, and others. This type of dialogue, of drafting and redrafting — and I am not talking specifically about the surveys — the white papers for privacy principles, and the privacy impact assessment workshop, are all absolutely indispensable. I agree with Kent Markus that it is extremely complex. The dialogue is just beginning, and it better continue because it is vitally important to the country and to the public.

(Martin) I want to join you in that last comment, in reference to SEARCH and the Bureau of Justice Statistics, because the fact that you are here is testimony that this kind of discussion is necessary. Thank you.

[1] ***Editor's note:*** Now known as NASCIO, the National Association of State Chief Information Officers.

**Government holders of criminal justice information: The role of law enforcement and the State criminal history repositories**

Should the States continue to impose restrictions on access to criminal history record information held in repositories?

The view from the Federal Bureau of Investigation advisory process
*David Gavin*

Florida, an open records State
*Iris Morgan*

Criminal justice information: The heart of life on the beat
*Roger W. Ham*

Panel question-and-answer session

## The view from the Federal Bureau of Investigation advisory process

**DAVID GAVIN**
*Chair, Federal Bureau of Investigation*
*Criminal Justice Information Services Advisory Policy Board*

I am the Chair of the FBI's Criminal Justice Information Services Advisory Policy Board (CJIS APB).[1] The Board is made up of 32 representatives of law enforcement and criminal justice agencies across the country. The APB advises the director of the FBI on the management of the national criminal justice information systems that are managed by the FBI: The Integrated Automated Fingerprint Identification System (IAFIS), the Interstate Identification Index (III), Uniform Crime Reporting, and, of course, the National Crime Information Center (NCIC). The FBI director has an almost unblemished record of following APB recommendations, which makes this is a process whereby the users really do share in the management of these national systems. That shared management is very important for the implementation of those systems within the States by the State Control Terminal Officers (CTOs), and by the local law enforcement agencies across the country. When the FBI sneezes, everyone else catches a cold, so for us to have this process is very beneficial.

It also means, of course, that I am coming to you today from deep within one of the smokestacks that Bob Belair described in his talk. I want to focus on the panel question, "Should the States continue to impose restrictions on access to criminal history record information held in the State repositories?" Many speakers have commented on the complexity of these issues, and certainly that is the case. I would like to stay focused on this issue from the point of view of the FBI's national advisory process.

I work for the State of Texas at the Texas Department of Public Safety. We are one of the States with our conviction data on the Internet, so I am aware of the issues related to fulfilling a directive from the State legislature to do that. Our sex offenders are also on the Internet. We are getting more than a million hits a month on those two sites combined.

I want to have this discussion in the context of Bob's presentation and the Task Force recommendations. Two points seem to be specifically relevant. One is to collapse the separate controls governing law enforcement, courts, and commercial providers into one global set of procedures, rules, and laws. That is a paraphrase of what Bob said, but he talked about the sources of the data now driving the controls and that we need to look at the data and the use of the data. We need to set standards and controls on the use of the data

[1] Mr. Gavin's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/gavin.ppt.

according to what the data is, rather than where it came from. That is absolutely right and an honorable goal, but it is complex. The reason there are separate controls right now based upon the separate sources of the data is because the courts and law enforcement, and the emerging commercial providers, all are performing separate functions. This morning Judge Martin made some very clear comments regarding the use of the data at the courts. The data is being looked at by 500 people a day, and they are using the data in a different way. It is being created for the courts. It is a record of what happens within the court. The State repositories are creating a history of the data for use by law enforcement and criminal justice agencies, but also for use by licensing and employment agencies according to statute. So, collapsing all the global controls is a very important concept. The second recommendation we really need to look at is to maintain the emphasis on fingerprint identification for creation of records and for inquiries into databases. This data is unique because it does have a biometric attached to it.

## Repository characteristics to consider

I don't think there is much contention over what a criminal history repository is, but I want to bring forward a couple of characteristics we need to consider. Clearly, it is a repository. Data is submitted to the repository by the originating agencies. We are *not* the acting agencies that create the data. We are *not* the original source of data. The criminal record in the repository is simply a history created of actions taken by *other* agencies. It is fingerprint-based. It does have this biometric attached to it. This is universal in terms of the repositories, and it is critical to discussion of subsequent use of the data, and our responsibility in the execution of public trust. The primary purpose of maintaining criminal history data in State repositories is to support and enhance public safety. That goal is accomplished in two ways. One way is by serving the law enforcement and criminal justice agencies. We are all familiar with the use by police, courts, prosecutors, probation, and corrections. The second way is through an ever-increasing use by noncriminal justice, licensing, employment, and other entities authorized by statute. The data is being used for suitability determinations. The legislatures are creating more and more avenues of access or categories of access for entities to use this data in making determinations of whether a person should be licensed or employed or have access to vulnerable populations. The management of the repositories involves the public trust because this is the official government clearance process. We need to be very careful about keeping that in mind. Yesterday, you recall the Task Force made a distinction between the general public and governmental entities identified as having special access. As we look at collapsing the controls into a global set of controls, we have to keep that distinction in mind because it becomes more important and more relevant to the discussion, especially as it regards the commercial providers.

The primary activity of the repositories is the matching of persons to records. That is what we do. We don't match the data to other sets of data. We don't act and create, and then record. We match the person through the fingerprints to the data. For law enforcement and for other purposes, of course, we match the data through name search and through other demographic search. For noncriminal justice purposes, the most desirable means of matching persons to records is through fingerprints.

We cannot forget that the repositories are governed by State legislatures and what we are doing today is having a national discussion to provide guidance that might be used by those legislatures. SEARCH's *Technical Report 13* [2] provided very effective national guidance at that time. The creation of the three-year Task Force that is being recommended by the current group can have that same sort of effect by having the same sort of discussion and coming out with the same sorts of recommendations for the current issues now before the repositories. Many of those issues are being driven by technology.

## National strategy for record exchange

I want to emphasize a couple of things in terms of the national discussion. First, of course, there is a national strategy for the interstate exchange of criminal history record information right now. The Interstate Compact[3] now governs use of the Interstate Identification Index (III) for noncriminal justice purposes. SEARCH Executive Director Gary Cooper likes to say that he started working on the Compact when his daughter was a toddler and now she is about to get her advanced degree. In October 1998, the Compact passed the Congress and now I believe seven States are signatories, with Connecticut soon to be added.[4] Obviously it has to go through State legislatures and that process is going to take some time, so the fact that there are only seven is not indicative of the acceptance of the Compact concept by the States. This is a process that occurred over a long period of time in which the States had continuing, extended input. We can certainly say it was the consensus of the States to head this way. The national systems involved are the III and the National Fingerprint File (NFF). III is the national index, managed by the FBI, of the criminal histories in the State repositories. The NFF is the concept under which the States submit only the first arrest fingerprint card to the FBI creating that index entry so that at the national level there is the index entry. But additional data, the subsequent data, is then maintained by the State. When an inquiry comes in for the data, the FBI does not respond with all the data. The FBI points back to the State and the State responds.

[2] *Technical Report No. 13, Standards for the Security and Privacy of Criminal History Record Information*, 3rd ed. (Sacramento: SEARCH Group, Inc., 1988).

[3] The National Crime Prevention and Privacy Compact, which establishes formal procedures and governance structures for use of the Interstate Identification Index for noncriminal justice purposes, became effective April 28, 1999.

[4] For up-to-date Compact information, *see* www.search.org/policy/compact/privacy.asp.

## Role of the National Crime Prevention and Privacy Compact

The role of the National Crime Prevention Privacy Compact, the official name that was used when it was passed, is significant from the point of view that it does create the national strategy for the maintenance of these records. The signatory State legislatures agree that this is the national strategy. They agree to common procedures for responding to the interstate noncriminal justice inquiries, and share criminal history data according to the laws of the receiving State. They agree to require the submission of fingerprints for these interstate noncriminal justice background searches. This is all in place. This is certainly in its beginning stages in terms of maturation, but it is the result of a long arduous process. There is the expectation that the States are going to sign onto this. So, what is the relevance? As we talk about privacy, and as we talk about bringing this global set of controls to the different domains, we need to be mindful that this is Federal law right now. This is where the States are headed, and if in our review of privacy there are issues that impact the Compact, they need to be brought forward. The Compact creates a Compact Council that has regulatory authority. This is not an advisory board. They have Federal regulatory authority over the noncriminal justice use of III.

## Regarding the data

Let's think about the data in the criminal history repository. Is the data ready to go public? Other speakers have highlighted some of the issues. The answers to these questions are the continuing responsibility of the State repositories and are important to the effective use of this data. Accuracy is less a problem than timeliness, completeness, usability, and the effect of this data being used by untrained users interpreting the rap sheets. We need to look at the use of the data. Why are we going to consider lifting the restrictions on the State use of the data? Is it to provide suitability determination information beyond that which is already provided by statute? Is it an answer to the general call for more data, or greater access to government data? Is it to provide the commercial providers with information? The key question is, "What is the mission of the central repository and is it evolving?"

## Positive identification

I'll highlight positive identification. I have mentioned it previously. This is a key component of the role of the repositories. It depends upon the availability of fingerprint capture and comparison technology. I am sure this morning is not the time to have the argument regarding fingerprints versus name searches, but there is a name check effort that has been studied. The *Name Check Efficacy Study* has been published by SEARCH and BJS that adequately lays out the issues there.[5] These bullets identify the other considerations regarding fingerprint searches versus name searches:

[5] *Interstate Identification Index Name Check Efficacy: Report of the National Task Force to the Attorney General,* NCJ 179358 (Sacramento: SEARCH Group, Inc., July 1999). See www.ojp.usdoj.gov/bjs/pub/pdf/iiince.pdf.

- Technology now can begin to deliver on the need for efficient positive identification.
- The role of the III.
- The Role of the Interstate Compact.
- States agreeing on fingerprint identification.
- The need for emergency access by name.
- Positive identification as a public safety responsibility.

As we talk about collapsing the smokestacks and creating a global set of controls, how does this factor in? How do we use the fingerprints? Are we going to make greater access to the criminal history repositories by name or do we consider requiring a fingerprint requirement from the commercial compilers? And, of course, the privacy concerns might be similar to the use of driver's license photos in the issue that was discussed yesterday.

In conclusion, even under the global set of controls, we need to be mindful of the fact that law enforcement systems, courts records systems, and commercial provider records systems serve different purposes. Perhaps an answer to the panel question is not simply to lift the restrictions, but to figure out how to collapse the smokestacks while maintaining the respective purposes that have been placed on those separate entities.

# Florida, an open records State

**IRIS MORGAN**
*Senior Management Analyst*
*Criminal Justice Information Services*
*Florida Department of Law Enforcement*

My name is Iris Morgan. I work with the Florida Department of Law Enforcement (FDLE) and I want to talk to you today about Florida, an open records State.[1] Florida is, of course, one of the most renowned open records States in the country. Florida has been an open records State for a number of years. Florida Statute Chapter 119 actually enacted Florida's Public Record Law in, I think, the mid-1970s. Florida is government in the sunshine at its best. All government entities in Florida are bound by Florida's public record law, including State and county municipal departments. It includes the boards, divisions, etc., that are created and established by law. It also includes any public or private entity acting on behalf of any government agency. Each of those is also required to abide by the public record law of Florida.

The term "public record" is not limited only to traditional written documents. It also includes tapes, photos, films, sound recordings, software, email exchanges, and every possible form of material regardless of the physical form, the characteristics, or the means of transmission. Any document circulated for review, comment, or information, whether in its final form or in a draft document, is open for public consumption in Florida. So email exchanges are open for public consumption.

The only exceptions must be defined by law or embedded within State statute. In Florida statutes, we have a specific requirement for the exclusion of sealed or expunged criminal history records in the release of information to the general public. Certain sealed records are available under certain types of license and employment considerations, but as a general rule of thumb, that information is not available for public consumption. Just like the sealed and expunged data, documents related to active criminal investigations or intelligence information are protected from public consumption. This is information that is not available under Florida's public record law. Personal information about law enforcement officers, such as their Social Security numbers, photos, driver's license numbers, and home telephone numbers are restricted from public review. In like fashion, other law enforcement agents in Florida, such as correctional officers, state's attorneys, statewide prosecutors, and others, are also protected from having that type of information disseminated. In many cases, the family members of those criminal justice

[1] Ms. Morgan's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/privacy%20conference.ppt.

agents also find that same privileged information.

Just like other States, there are many State statutes in Florida that allow access to both State and national criminal history information. These State statutes, and I think there are 300 or so in Florida, have been approved by the Attorney General and allow for both State and national information to be provided. Those include record checks on teachers, school personnel, and concealed weapon permit holders, along with a variety of other professions such as doctors. Each of the record checks under these conditions requires the submission of an applicant fingerprint card for positive fingerprint comparison at both the State and national levels. In 1999, Florida processed over 400,000 record checks under these guidelines. Approximately 11 percent of those record checks did, in fact, result in the identification against an existing criminal history record.

## Records available for noncriminal purposes

In addition to over 300 State-level requirements for State and national record checks, a number of statutory requirements in Florida require State-level record checks only, which are not forwarded to the FBI for processing. The majority of those record checks come under the public record law as well as specific statutory authority. The bulk of those record checks are name-based record checks. They do not require the submission of applicant fingerprints in order to provide that information. Instead, those record checks are based on the name, race, sex, date of birth, and other demographic information provided by the requestor. Those include record checks from private employers who are interested in pre-employment checks. It might include individual's parents who are interested in checking out babysitters before they hire those individuals. It also includes, in many cases, idle curiosity or checks on neighbors and friends. Florida's public record law allows that type of record check to be conducted.

In 1999, we processed over 1 million record checks for Florida-only data. The bulk of those were name-based record checks. Approximately 23 percent of those record checks resulted in a potential match against an existing criminal history record; a good bit higher than the fingerprint-based record checks I mentioned earlier. There are several reasons for that. One is that these record checks are on nonprofessional-type positions and personnel. In many cases those record checks are being conducted on persons where there is a perception or a known existence of a criminal history record, and the requestor is simply trying to obtain a copy of that criminal history record. So it is an existing record. It is known. They are just trying to obtain the information on that record.

Florida record checks may be requested under Florida's public record law and under State-level record checks. There are a variety of methods to request that information. Obviously, the FDLE accepts the applicant fingerprint cards for the fingerprint-based record checks for processing at the State level, or processing at the State and national level. We also accept

correspondence from the public, which includes demographic information on the individuals. We have a modem connection where we accept electronic transmission or request for criminal history data. And we currently have an Internet project under way whereby we will allow the general public access to criminal history information via the Internet. We return criminal history record responses in the same manner. We will print results, whether it is a nonidentification against an existing record or a possible identification against an existing record. The criminal history record itself will be printed and returned either by routine mail or provided by our interface modem connection. We are also returning Florida criminal history data through the Internet. The Internet project is currently in a pilot stage. It will not be open for public consumption for some time, but we are satisfied with the way that project is going.

A key point concerning Florida criminal history name-based record checks is the necessity of making sure the audience understands that the information you are providing them is based solely on the data they have given to you to make the identification. We provide a caveat on every criminal history record check we process that is not fingerprint supported. We advise them that this information may be the same, but it is not based on positive fingerprint comparison, and therefore, leaves some room for doubt. FDLE routinely processes and encourages requestors to submit fingerprint cards for positive confirmation of identification. We routinely process those requests at no additional cost to the individual. I would like to also point out that Florida processes what is called "personal reviews" at no cost to an individual. Personal review allows an individual who has a criminal record to review their criminal record to ensure its accuracy and content. We process those routinely, and provide the information to the requestor so they can confirm that the information contained in the criminal record is accurate. Of the 1 million record checks we have conducted under Florida's public record law or under State law requiring state-level record checks, approximately only 1 percent or about 1,000 customers have asked for a secondary validation to confirm or deny the identity of the individual. A very limited number of secondary requests have been provided to FDLE for confirmation.

## Hot files on the Internet

Since 1996, Florida has posted sexual predator data on the Internet.[2] In 1997, we began adding the sex offender data to the Internet. Currently there are about 2,000 sexual predators in Florida and about 18,000 sexual offenders in Florida. There are a number of hits against this data set. The public in Florida is very interested in knowing whether the individual next door is a potential sex offender or predator. Since October 1997, we have had well over 1 million hits against this Internet site.

In July 2000, Florida plans to begin posting "hot file" data on the Internet. Hot file data includes stolen

[2] *See* www.fdle.state.fl.us.

property that has been reported to law enforcement, wanted persons, fugitives, and missing persons. When we started this project, we created a task force of local criminal justice agency representatives to discuss the feasibility of posting hot file data on the Internet. The law enforcement agencies in Florida were very supportive of posting the information on the Internet. In fact, we have a number of counties in Florida, Polk County being one of the most aggressive, that have been posting their wanted persons data on the Internet for some time. And I think they have about 1 million hits a month.

A number of agencies are concerned about whether they want to participate in this process. They are looking at whether they want to pursue implementation or posting of their records on the Internet. Obviously, Florida is a repository for that information and we will bow to the judgment of the local agency. If they don't want to have their records posted on their Internet, we will not post them. But most of the agencies in Florida will actively participate in the posting of the information to the Internet so they can get hits from local residents in Florida. The key is to have more eyes watching and trying to assist law enforcement in locating fugitives, missing persons, or stolen property. If a person wants to purchase a piece of property, they can pop onto the Internet and run a check on that item. If it has been stolen, they can provide that tip information to the local agency. Obviously, they would be discouraged from taking action themselves, but they could provide that information to the local agency.

# Criminal justice information: The heart of life on the beat

**ROGER W. HAM**
*Chief Information Officer*
*Los Angeles Police Department*

My name is Roger Ham and I am a civilian Deputy Chief and the Chief Information Officer of the Los Angeles Police Department (LAPD).[1] I wanted to begin by saying this task force had some difficult times, and we want to thank Bob Belair for his role in chairing the task force. However, Bob failed to mention the law enforcement role. Col. Tim DaRosa of the Illinois State Police and I were really in charge of giving this task force some guidance, and we felt that it was a challenge similar to that of herding calves. But we got through this. And today I wanted to give you a little bit information about the LAPD and how we use criminal justice information.

Los Angeles is the heart and soul of a five-county area, and that county area is the twelfth largest economy in the world. We cover 460 square miles and we have 13,000 employees. Today we are really looking at reinventing ourselves in a number of ways — one being technology. We are going to spend over $400 million for new technology for the LAPD. Those funds came from taxpayer bonds, the Community-Oriented Policing Services Making Officer Redeployment Effective (COPS MORE) project initiatives, and general fund budgets. Many would ask why we need all the technology and what are the goals of this technology? Consider that the LAPD handles over 6,000 911 calls a day, 8,000 nonemergency calls, and dispatches over 5,400 calls for police service each and every day of the year. When you look at our goals and the technology involved in our goals, you can see that our goal is to increase the efficiency and safety of our officers while providing more and faster information to the responding units even before they get to the call. The benefit is improved public safety, as well as reduced response time.

We have a second goal, and that is to provide criminal justice information to staff personnel with the intent of better information being available for online records, detectives, and parole. The benefits we get from that are obvious. We get better crime analysis, better tracking, and a higher level of performance. It is truly our goal to prevent crime and to reduce the fear of crime in Los Angeles. When you think about public safety, success is measured in seconds, whether apprehending a criminal or saving a life. And this technology gives us that critical advantage. Some of the technology integrates into this criminal justice information system. This is the heart of LAPD. This is the information that drives us to our successful enforcement of the law. We get this information through our departmental systems. We are able to interface. We have local area

[1] Mr. Ham's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/cio2000.ppt.

networks and we have computer systems and mainframes that store this kind of information. Also, we connect via a lot of our city systems. We tie into our county neighbors, county sheriffs, and county courts on juvenile indexes, consolidated criminal history information files, and more. We also have access to our state system. This is our California Law Enforcement Telecommunications System (CLETS) access. This is how we access the National Crime Information Center (NCIC). In California, all of our agencies go through CLETS. It ties into our Federal systems, where we have the Federal system information available.

## New millennium technology

This is some of the new technology we are developing for the next millennium:

- Local-area and wide-area network systems – 4000+ workstations.
- Field Data Capture – Laptop Report via Wireless Network.
- Data Architecture.
- Videoconferencing Case Filing.
- Fiber Optic Network – Dual OC48 Backbone with OC3 Drops.
- LAPD Online (www.lapdonline.org/index.htm).
- Detective Case Tracking System.
- Voice Radio System.
- Data Radio System.
- Dual Communication Centers.
- FASTRAC.
- Digital Crime Scene Photographic System.
- Electronic Mug Shot System.
- Laboratory Information Management System.
- Online Barcode Tracking System.
- Live-Scan Fingerprint Network.
- Virtual Investigation System.
- Airborne Live Video.

We are concerned with the privacy of the information because we are the largest user of this information. These are some of the technology projects that are currently going on in the LAPD. Many of these projects are the backbone, created so we can move data. We can move criminal history information and mug shots across the county. We want to be able to give that officer every opportunity to solve the crime. We want to give the officer correct information in a timely fashion.

The task force understands the rapid rate of change in technology today. And as the rate of change in technology continues to accelerate, it will be the basis for new opportunities for all of us. It will also be the basis of management challenges. However, as the rate of change in technology continues to accelerate, the need for professional management increases as the risk of mismanagement of these systems escalates. I have learned that an opportunity missed often becomes a threat. Many of our systems were designed in the 1970s, and that logic was applied to many of the systems we have online today. One of them is our Criminal Record Offender

Information (CORI) system. CORI is defined in the penal code and includes the rap sheet, the summary of arrest, pretrial proceedings, nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release. The interesting thing is that in California we are not authorized to use this information for the purpose of licensing, employment, certification, or a record review. So in those areas, we cannot use it. We use it for our criminal investigations.

We have many issues with our criminal justice information system (CJIS). Obviously we get concerned when there is incorrect information. Many citizens of Los Angeles come to our records unit and say, "I am not the person that is on file. They are using my name and every time my name comes up, I have a real problem with law enforcement." Or, "I can't get a loan." So these kinds of things really do concern us, and the LAPD does try to help these people to really use their fingerprints to validate the information. We also have an issue of sealed records in law enforcement. I will discuss that in a few minutes. Another issue is multiple identities. We have had a number of issues with twins that make it difficult to identify the correct person. We have mistaken identities. An issue that came up in the 1970s is our access limitations; right to know versus need to know. And we have all discussed that.

## Information access and hiring decisions

Some of the issues I would like to talk about really have affected us. (Many times it is a good day if you are only on the editorial page, and your department is not on the front page *and* on the editorial page.) One issue is concerning our Rampart investigation and the infamous Rafael Perez. Many of you who have read the papers understand the history of Rafael Perez and the fact that we now refer to him as convicted-criminal-serving-time Rafael Perez. We found out information that we did not know during our investigation. We hired police officers. They were hired based on conviction information. We did not have access through our CLETS to the rap sheet information. I find that interesting because we look at past performance as an indication of future events to come when we evaluate these police officers for the ability to serve. We have gone through this with our legal staff and we cannot seem to get around the issue of using CLETS and not doing a thorough background by using the rap sheet information. We also found that in many backgrounds there are sealed records (past juvenile arrests, convictions, bankruptcies). These issues really do get to the heart of the matter when you are hiring somebody. People can have their bankruptcies sealed. We have to be able to deal with that and unseal them to know what information we have. It is quite clear in the state of California that CORI is not a tool to be used for hiring purposes.

## Conclusion

In conclusion, we really believe, in the LAPD, that privacy is vital for all of our citizens. We believe it is a right. It is important. Because of the difficulties of obtaining good information, many times the information is not correct

and has to be verified, and in the wrong hands this information really can destroy lives. We believe that is why it should be mandatory to use fingerprints in this system, and that biometrics such as fingerprints are probably the easiest and the best way to go. We believe law enforcement agencies such as LAPD must have open access to all records for high-integrity positions, whether it is police officers, Federal agents, or definable civilian employees that are in high-security jobs. And also, we truly do believe criminal justice information should be for law enforcement purposes only. That is what it was originally set up for, that is what we use it for, and that is our law enforcement view. However parochial it may be, that is our view.

In closing, I would like to quote Ella Wheeler Wilcox and his poem, "Some ships sail to the east, some to the west. On the same shifting winds that blow. It is the set of the sail and not the gale that determines where we go." You know our success is not going to be dependent on outside circumstances because all of you know that winds of technology are changing today and are going to continue to blow. If we are not very careful, they will blow us off course. But I will say today that it is dependent on how well we work together to address our differences on the issues. Thank you very much.

## Panel question-and-answer session

### The role of law enforcement and the State criminal history repositories: Should the States continue to impose restrictions on access to criminal history record information held in repositories?

**Q.** I am Gary Cooper, California Department of Justice. I have a question for David Gavin. When Ron Hawley introduced this panel, he talked about the right to know, and indicated that we really control our records. Yet Iris talked about idle curiosity. You spoke about global rules, procedures, laws, and the regulating authority of the Compact Council. Can you tell me how you set up these global rules, and how the Compact Council really regulates noncriminal justice dissemination in light of state statutes?

**A.** (Gavin) The Compact Council was created in statute and has regulatory authority. Of course, regulations need to act within the purview of the law. It can create regulations that guide the use of the Interstate Identification Index for noncriminal justice purposes and make interpretations regarding the use of the records. It is constrained to do nothing that affects the criminal justice use by the FBI and the States of that same system for law enforcement purposes. It acts as a regulatory body over all of the noncriminal justice use, with certain exceptions that are identified within the Compact. It is the first time we have had a single regulatory body at a national level for noncriminal justice use. It is going to become a focal point for issues related to the interstate use of the State repository records as States sign on to the compact, because as they sign on, they are agreeing to the general rules. I am sure I am not the best person to speak, but it is a new body. It is a new tool and its regulations can have an impact on privacy. It is a body that needs to be well represented in the ongoing discussions. I invite anybody else in the room that is on the Compact Council to make remarks as well.

**Q.** I am from Pennsylvania and I would like to direct my question to Iris Morgan. You mentioned the issue of personal review with respect to the records you keep in Florida. If someone takes advantage of the opportunity to personally review their criminal record, where does the burden lie at that point of the challenge, and what do you accept as proper verification that the charges listed in your records are accurate?

**A.** (Morgan) The personal review process in Florida requires that the individual submit a fingerprint card for positive comparison against the State repository. The actual content of the record itself is at the burden of the local agency that contributed that information. If the individual suspects or has a question about the integrity of one of the sets of information submitted by a contributor, he or she is required to contact that contributor for corrective

action. The contributor then modifies the information, if appropriate, as it is contained in the state repository.

**Q.** I am Beth Givens, Privacy Rights Clearinghouse, with a question for Iris Morgan. You mentioned idle curiosity; the casual requestor who is looking for information on the neighbor or maybe someone he or she is dating. Do you inform the data subject that a request has been made or do you keep a log so that when the person does check his or her own record, they know who has accessed it, like we can with our credit reports?

**A.** (Morgan) In fact, we do not notify the individual who is being checked. We do maintain a dissemination log of the individuals who have made a query against, or received a copy of the criminal history record. That information is also available under the Public Record Law if the individual wishes to obtain a copy of the recipients of that information. As far as idle curiosity, I do want to clarify one point and mention that the information provided under Florida's Public Record Law is limited only to Florida's data. It does not include the national data as contained in other state repositories. We are looking only at Florida's data.

**Q.** I am Ramon DeLaGuardia from the California Attorney General's Office. I have a question for Chief Roger Ham. I am not sure about your point on CORI. My understanding of California law is that law enforcement gets just about everything on a peace officer applicant's background.

**A.** (Ham) We are not authorized to use CORI for that.

**Q.** (DeLaGuardia) You want online access to that information?

**A.** (Ham) We want to be able, when we are doing the background investigation, to call that information up. That is correct.

**Q.** (DeLaGuardia) I see. But we can provide hard copies relatively quickly.

**A.** (Ham) I don't know if we have been able to get those in the past, but we would like access, and I don't see what the difference is between hard copy and having access when you are in the background process.

**Q.** (DeLaGuardia) Well, we have certain court injunctions that we do remove information on detentions and exonerations, but everything else you can get and we preclude it from online access. But ask and you shall receive.

**A.** (Ham) Well we would appreciate that. We wish we would have known that.

(Ron Hawley) I was going to ask a question about what States might be experiencing groups coming together to discuss access and privacy and those kinds of issues. I am suggesting maybe here is a good place to start in California. Time for one last question.

**Q.** I am with an investigative agency in New York City. I am also a member of the American Society for Industrial Security Committee on Privacy and Personal Information Management. First, I would like to congratulate the Florida Department of Law

Enforcement for the quality of information they provide to end users, as well as Ms. Andrews in Maryland. My own home State of New York, although it does have a Department of Criminal Justice, does not allow (or limits) the access of criminal record information to the private sector. The situation we have is that the courts in many situations are charging inflated prices to do criminal record searches. In many instances they are taking an excessive amount of time to complete them, and providing less than accurate information. I think a distinction must be made when determining whether to provide information to outside agencies or the private sector. There should be a distinction between private organizations that are actual record compilers, where they are bulk storing information from repositories and then third-party selling it, and record providers, who search by individual single names through local or State repositories, and provide them to employers or end-users for a permissible business or purpose (i.e., under the *Fair Credit Reporting Act*). Do you have any comments on that?

**A.** (Gavin) I would say that is in line with the task force recommendation that there be a new view as regards the data itself rather than the source of the data. In Texas, our experience is that if a record is public, it is public, and if we provide a single inquiry response, then we also have to provide the database for a reasonable fee. So, I think that is something the States are grappling with and perhaps the follow on work of the task force or the next body that looks at this needs to look at the purpose for which the data is being requested.

**Privacy advocates**

Privacy and criminal history record information:
Is there still a role for privacy in the Internet age? What should it be?

International perspective: A European view of privacy protection
*Dr. John N. Woulds*

Data privacy — Law enforcement's access to your information
*James X. Dempsey*

Identity fraud and the case for privacy protections
*Beth Givens*

Panel question-and-answer session

# International perspective:
# A European view of privacy protection

**DR. JOHN N. WOULDS**
*Director of Operations*
*Office of the Data Protection Commissioner*
*United Kingdom*

I am going to begin my presentation with a disclaimer.[1] I would not call myself a privacy advocate. Privacy advocacy is part and parcel of my job, but I really describe myself as a privacy regulator. That term characterizes the European approach to privacy protection or data protection as we sometimes call it. It is the existence of an authority with statutory powers to take regulatory action over the use of personal information. I am going to describe very briefly the European approach to information privacy. Then I want to tell you about one or two case studies where we have applied our general approach to privacy protection in the criminal justice sphere, and the results we have achieved in that respect. I will return to the European approach and its relevance to the U.S. and then conclude by saying something about the way this approach might have helped the work of the Task Force.

When I was first asked to talk at this conference, I was asked to speak on the topic of why the European Union wants to prevent the exchange of records with the United States. It is impossible to answer that question without incriminating myself in some way or another. So I am not actually going to deal with that question in the sense of answering it. I will discuss why the question has been asked rather than answer the question itself.

I am Director of Operations for the Office of the Data Protection Commissioner in the United Kingdom. That body was established under an Act of Parliament with statutory regulatory powers over the use of information. We deal with issues of information privacy across the whole economic sphere, and that includes both public and private sectors. It ranges from criminal justice to banking, finance, and business activities as well. The same general principles apply to the use of personal information across the board. You may be surprised to know that we are not based in London but in a small town near the city of Manchester. Manchester is about 200 miles northwest of London and has a population in the greater urban area of 2.5 million people, so it is a very big

[1] Dr. Woulds' accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/natconf.ppt.

urban conurbation. It is also the cradle of the industrial revolution, birthplace of the first stored program computer and home to the best soccer team in the world. I know there are some soccer fans in the audience here today.

We have a lot of experience in the Data Protection Commissioner's Office in dealing with information privacy issues in the criminal justice sphere. Our approach to privacy protection is really based on the general European approach, which is characterized as a general law to protect personal information, applying across all sectors. The basis is a set of fundamental principles, with specific rules, that regulate the processing of personal information. That includes the transfer of personal information outside the UK and outside the European Union. The law establishes rights for individuals with legal remedies for individuals if those rights are infringed. Very importantly, it establishes an independent supervisory mechanism with enforcement powers to take action when things go wrong or when it is anticipated that information is likely to be processed in a way that infringes on people's rights.

These are the basic principles on which our law is founded. These are taken from the UK law, and that is more or less the basis to all European data protection law. Information, personal data, and personal information should be processed fairly and lawfully, processed only for specified and lawful purposes, and only used in ways that are compatible with those purposes. The ways the information is used should be adequate, relevant, but not excessive for the purpose. The information should be accurate and kept up-to-date but kept for no longer than necessary for the purposes for which it is held. The information should be processed in accordance with the rights of data subjects and in no other way. It should be kept secure and transferred outside the European Union only if there is adequate protection in the country that is receiving the data.

Various people yesterday talked about fair information practices and the fair information principles, and you will see a lot in common with this basic standard, which underpins all European law on data protection. We have a lot in common with the Fair Information Practices that other people have talked about. The difference being, perhaps, that this is an actual enforceable standard.

## Rights for individuals

In reference to rights of individuals, probably most important is the right of access. That is the right to know if an organization is holding personal information about you, and the right to have a copy of that information on request. There is also the right to have inaccuracies corrected, and the right to have the information blocked, deleted, or destroyed in appropriate circumstances. In certain circumstances, there is the right to prevent processing of personal data and to prevent decisions being made about you that are based purely on automated processing without any manual intervention. And

finally, there is a right under the law to have compensation for any damage, or to seek compensation for any damage caused by an infringement of the law.

To recap, the central approach is that there is a general law to protect personal data applying across all sectors that underpins the approach to information privacy across both public and private sectors. Examples of sectors that are covered, and in which information privacy issues do tend to arise are: business generally, commerce, finance, marketing, employment, taxation, social security, health, police, and criminal justice. The basis of the approach is this general law to protect information privacy.

I have talked about the European approach. I would not for a moment claim that this is unique to Europe and I certainly wouldn't ignore the situation in Canada, where the approach is very similar to that in Europe. What is important in the European context is that it is all underpinned by European law, in particular, the European Data Protection Directive, which all 50-member states of the European Union base their data protection law on. The European Union directive applies to the processing of personal data; it establishes individual rights and legal remedies; it sets out rules for the lawfulness or legitimacy of processing transfers to countries outside the European Union; data quality; confidentiality, and security; and importantly, it requires independent supervision. All of these features are present in the UK law.

At the heart of all this is the issue of balancing rights. Other speakers have talked about this during the course of the last two days. The individual has rights to privacy, rights to a private life, right to know what is happening, right to know who holds information about them and what they are doing with it, and a right to freedom of expression. Other individuals, the state, and business have rights too. These rights have to be balanced against the rights of individuals. There is no absolute right to privacy and this is the classic data protection issue. How you strike the right balance between the rights of the individual on one hand, and the rights of others on the other. That is what we try to achieve in setting out these general data protection laws to create that right balance and to find ways of judging that balance in different circumstances. That is common to all approaches in countries where there are general data protection laws. As I said, there is no absolute right to privacy.

## Information privacy in criminal justice

I want to turn now, after that very brief summary of the European approach to information privacy, and talk about some specific case studies where our experience in the UK Data Protection Commissioner's Office has been applied to one or two issues in the criminal justice sector.

The first one is retention of criminal records. What we call a criminal record is what I have learned to call a criminal history record here. There was a lot of discussion in the Task

Force about the relative merits of purging or sealing criminal history records. There was general agreement that in the right circumstances, and with the passage of time, an individual had a right that his criminal history should no longer be available. But the question of whether the record should be sealed, with the possibility of opening it up at a later stage, or purged altogether, was something on which I think it is fair to say we didn't find total agreement around the room. There were those who argued that it was wrong to purge records. The problem with purging records is that there might be a reason to look back into an individual's criminal history at a later date, but once a record has been purged, that is no longer possible. Sealing the record was the appropriate course to take.

We took a different view on this in the UK based on the principle that information should be retained only for as long as it is necessary for the purpose for which it was obtained or processed. After lengthy negotiations with the various bodies in the UK who do hold criminal records (all in the public sector), we agreed on deletion of criminal records after a lapse of a certain period of time. The period of time depends on the severity of the offenses for which the individuals were convicted. Information is retained only up to those periods of retention, which are defined in this policy. Any retention of records by police force or other agency beyond those limits would then come under the jurisdiction of the Data Protection Commissioner, who could order deletion of the record in those circumstances. That is one example where our application of the general data protection law has had an influence on the policy in relation to criminal history records.

The next case study is interesting because it involves the transfer of information between the United Kingdom and the United States. Some years ago, a consortium of police forces in the United Kingdom decided to set up a nationwide system of automatic fingerprint recognition, supported by a database of fingerprints obtained from arrested persons. Through back record conversion, the whole fingerprint database held on our national criminal record collection was automated. Principally for financial and technical reasons, that database was set up and is still maintained in Tacoma, Washington. That collection of records currently holds about 4 million print records — a very large collection of sensitive personal information. Large volumes of fingerprint data are transferred daily between the UK and the USA, both in real-time and also off-line. I have seen the operation of this system from both the UK and from the central database facility in Tacoma. It is very impressive from an operational point of view. But, of course, because of the different approach to privacy protection in the UK and the USA, the Data Protection Commissioner had to be satisfied that the sensitive personal information in that fingerprint database held in the USA would have a standard of protection equivalent to what would be required under UK law.

We *were* satisfied and occasionally we make spot checks to ensure that security arrangements and operational systems were maintaining that level of protection. That is a real example of the application of the European Union directive of not transferring data outside the European Union without being sure that the data we are receiving has adequate protection.

## Different perspectives

I would like to make a couple of points about the differences in privacy protection in our two countries. In Europe we have an omnibus data protection law, a general law that applies across all sectors. Whereas, largely speaking, in the USA privacy regulations are sector-specific. We have a harmonization basis across the whole of the European Union through the European Union Directive. Here, there are initiatives at both the Federal and State level. An early version of the Task Force report said that as of July 1999, 7,302 privacy bills have been introduced into State legislatures in the 1999 legislative cycle, and there were 1,406 laws where consumer privacy provisions have been passed. That is quite a staggering figure. If I wanted a reason why getting involved in privacy issues is a profitable occupation for lawyers in the United States, then that is a good enough reason.

I won't go any further except to say that an important part of the privacy protection approach in Europe and in the UK is the existence of the powerful supervisory authority that has powers to take action when things go wrong or has powers to intervene when systems are being proposed or developed. That authority is essentially absent in the United States. I am not going to try to argue which is the best approach, or which is right or wrong. It is not as simple as that. What it does highlight to me though, and one of the things I have learned from the Task Force work, is that the situation as regards privacy protection in the United States is far more complex than some of my colleagues in Europe would have me believe.

But I am not a lawyer. I am a practical person and it seems to me that the answers to the practical questions are what are important. What level of protection for information about me can I expect? How can I find out who has information about me and what information they have? What control do I have? Do I have any choice? Can I secure change if things are wrong? What remedies do I have if I object to what is happening or if things go wrong? What mechanisms are there to safeguard my private life? There are many different ways of answering these questions. The important thing about the European approach is that the general data protection, or privacy protection law provides a basis for answering these questions, no matter what sector we are dealing with — whether it is criminal justice, or direct marketing, or banking, or whatever.

Why is this relevant to the United States? The answers are fairly obvious: the growth of the global economy, the removal of technical barriers to the free transfer of information

from one country to another, international cooperation between governments and government agencies, and the multinational operation of companies. This brings into play the EU restriction on transfers of data stating that data should not be transferred to countries that do not have an adequate level of protection. That is what has led to the negotiations between the USA and the European Commission on the Safe Harbors principles proposal that Peter Swire talked about yesterday.

## Conclusion

I would like to conclude by referring to the SEARCH Task Force. I was privileged to be invited to be a member of the Task Force as one of a small number of participants from outside the United States. The others were my colleague David Flaherty and Ann Couvikian, both from Canada. I think we brought a slightly different perspective to the work of the Task Force than the other members. They were all great people to work with, even though on some of the issues we held directly opposed views. I learned a lot about privacy protection in the USA. I think the Task Force benefited from all these interests that were represented, including the privacy advocates, the privacy regulators, like myself, and those who come from an international perspective. What I tried to do in dealing with the questions that were posed was to look at it from a European point of view, even though it might not be entirely appropriate in the USA. Nevertheless, it gave a particular perspective on the issues. I hope that was useful to the Task Force and I certainly found it challenging.

Finally, I will come back to the question that was posed to me at the beginning. Why does Europe not want to exchange records with the USA? I found this wonderful quotation from the actor Peter Ustinov. “This is free country, Madam. We have a right to share your privacy in a public place.” Now, if I thought that really was the approach to privacy protection in the USA, then the question answers itself. But I don’t believe that and it is quite clear that is not the case. It is also quite clear from the survey results, which we had presented to us yesterday, that is not what the American public wants either. In any event, it wouldn’t be allowed under European law. Thank you.

# Data privacy — Law enforcement's access to your information

**JAMES X. DEMPSEY**
*Senior Staff Counsel*
*Center for Democracy and Technology*

I am going to focus on privacy as it affects criminal justice information, looking out at the next 5 to 10 years.[1] As you all know, privacy is a hot topic right now. It has clearly risen to a fever pitch in Washington. What will come of that remains to be seen, but last week both Orrin Hatch, the Chairman of the Senate Judiciary Committee, and John McCain, the Chairman of the Senate Commerce Committee, stated their intention to move privacy legislation this year. They will have competing bills and numerous other bills will be introduced. One of the interesting things about the Hatch bill is that he actually combines commercial data privacy issues and law enforcement issues. In the past, we tended to treat the issues concerning commercial databases separately from Fourth Amendment issues and the issues concerning government databases. We are now seeing them merged in the real world, and legislatively they are merging as well, which is one of the focuses of the SEARCH Task Force report.

The three policy issues I would like to focus on today are: the impact of the new technology on the criminal justice system, policy conclusions we can draw, and specifically, what the implications are for privacy. John Woulds and others have talked about the Fair Information Practices. I think of the Fair Information Practices as something that originated in the United States in the 1970s.[2] They have basically become globally recognized, and enacted into law on a comprehensive basis in Europe. I have broken these principles down into nine different categories: Notice, Consent, Collection Limitations, Use and Disclosure Limitations, Retention Limitations, Accuracy and Completeness, Access and Correction, Security, and Accountability. You can break them down in different ways. The Federal Trade Commission (FTC) in its recent report on information privacy really boiled them down to four — notice, choice, access, and security.[3] But I think it is more useful to break them out in more detail as I have. You see elements of these principles appearing in almost all the regulations or guidelines governing information systems. These fair information principles define the issues that have to be confronted as you consider how to administer the systems you deal with. Some of them, however, are less relevant to the criminal justice system. For example, a certain amount of the information collected

[1] Mr. Dempsey's accompanying presentation can be accessed in conjunction with this speech at www.cdt.org/privacy/govaccess/.

[2] They were developed in 1973 by the U.S. Department of Health, Education and Welfare.

[3] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress* (May 2000), *available at* www.ftc.gov/reports/privacy2000/privacy2000.pdf.

in the criminal justice system is collected without notice. Some of the information is collected without consent, since it is obviously a coercive system. But that only heightens the importance of other of these principles in the context of criminal justice.

I will give you two examples of the way these principles gain heightened importance within the criminal justice system as a result of the Internet and other communications and information-sharing developments. Take simply the issue of security. Anybody who holds personally identifiable information has some responsibility to protect that information and to ensure that it is only used in accordance with the rules under which that system abides. If you are turning to the Internet — as most institutions are as the way to share your information — that vastly heightens the importance of security of those systems and how you control access. Many system operators from large to small organizations find that what they thought was a private portion of their Web site has been accessed by somebody from the outside, and personally identifiable information has been disclosed. For example, a university hospital system recently was unaware that its Web-based medical records information was available from the outside until somebody brought it to their attention. So the security issue is hugely heightened. The other issues — retention, accuracy, and completeness of information — are also heightened, because we are seeing information that had previously been only in government databases and under the control of government agencies moving out into private-sector databases. The question that arises is, How do you ensure the accuracy and completeness of information? How do you ensure that disposition data, if it is added at the governmental level, gets into a private sector record?

## Privacy and justice technology

My slide presentation today is part of a much more extensive presentation that is on the Web site of the Center for Democracy and Technology, www.cdt.org. It focuses on a system called Digital Storm. Digital Storm is the Federal Bureau of Investigation's vision of the future in terms of how they will collect, process, and store investigative information. As we move further into this digital environment, law enforcement agencies like the FBI have available a wide range of sources of information. In this networked environment, essentially any private or public source of information can be drawn upon by law enforcement, and each data source presents the various issues of standards for access, notice, consent, accuracy, and so on.

One point I want to make, notwithstanding the complexity of this issue and the amount of information available, is that it is critically important not to assume that the cat is out of the bag in terms of privacy. You may have heard Scott McNealy, President of Sun MicroSystems quoted as saying, "You have no privacy. Get over it." At some level, as a statement of current reality, that quote may be partly true. But at a more fundamental level, Mr. McNealy's comment was

of limited value because we have to recognize that we are recreating this technology every single day, we are redesigning these systems every single day, and it is possible to build in privacy. Just as we have ignored privacy, and to some extent built privacy out, we can build privacy in and regain that privacy. We can reinsert some of those fair information practices and principles into the design of systems from the outset.

The trend toward integration is also underway. Far be it from me to appear at a SEARCH conference and say anything negative about integration of criminal justice information systems, but I have some questions about the benefits and risks of integration. I am not sure the privacy aspects of integration have been thoroughly thought through. There is an intuitive appeal to the idea of integration, if you define it as the ability of one institution in the criminal justice system to draw upon information from all the other participants in the system. The ability to create a single or networked source of information that could be drawn upon by police, courts, correctional authorities, probation, prosecutors, and others is appealing. I do, however, question the impact on privacy, particularly when you consider the potential misinterpretation of data — we know that data becomes harder to interpret the farther it gets from the source. There seems to be an unstated assumption that more information is going to produce better decisionmaking. I think there has to be a little bit of a pushback to that.

## Information sharing between the government and the private sector

Another major trend we are seeing in the criminal justice information system and in government information systems generally, is the increasing cross-sharing of information from government to the private sector and from the private sector back to the government. Many agencies of the U.S. Government rely upon private sector look-up services. For example, the Financial Crimes Information Network at the Treasury Department uses approximately 15 commercial databases. The U.S. Secret Service uses approximately 13. Information, in some cases compiled and collected from government databases, is then repackaged and sold back to the government. I am not saying that is necessarily a bad thing. Clearly, the providers of those systems are meeting a market need, but again it raises a host of new questions that are going to be debated both in Congress and in the courts over the coming 5 years. For example, the recent Supreme Court decision in *Reno v. Condon*[4] upheld the Federal Driver's Privacy Protection Act, which was Federal legislation limiting what the States can do in selling their Department of Motor Vehicles data. The interesting thing about that decision is that it mentioned the word "privacy" only in referring to the name of the statute. They did not hang their decision on a right to privacy. To the contrary, they treated information as

[4] 528 U.S. 141 (2000). The decision upholds Congress' right to restrict States from selling driver's license data without driver consent.

a commodity just like soybeans. They said information is something that Congress can regulate, and they can regulate it in the hands of the States when the States are managing databases and when States are participants in the interstate commerce in information. The good news for those who have a business selling this information is that the Supreme Court did not say anything about privacy rights in this information. The bad news is that the Supreme Court said this is a market that can be regulated for whatever reason Congress and the other legislatures may choose to regulate it.

Upcoming, I think there will be two big issues on this question of regulation of the sale of information. The first will be the property question and we can have some debate if you want during the Q & A session, but one of the arguments often made by private sellers of information is that this information is their property. You can find support for that in what the Supreme Court said in *Reno v. Condon.* That is actually what our law has said for decades, if not for hundreds of years: Information is property. But saying that information is property settles absolutely nothing, because then the question becomes, "What are the rules for the use, disposition, and sale of that property?" We have rules for the use, disposition, and sale of any other kind of property, whether personal or real. In the real estate realm, we regulate property — we have many rules about trusts, landlord/tenant relationships, and more. So to say that information is property doesn't get you very far in the debate. You still have to decide what the rules are going to be. The second issue is the argument that information in the hands of private entities enjoys First Amendment protection, or that those entities have a First Amendment right or commercial speech right that cannot be infringed upon by the legislature. That is a huge and brewing issue, and more difficult than the property issue.

## Fair information principles and justice information

This brings us back to the question of fair information principles and how they relate to criminal justice information. Privacy is much more than secrecy. Privacy as we use the word in the United States really is about personally identifiable information and how it is used, and to what extent individuals can control how their information is used. That includes public record information. It includes information the individual has voluntarily given to somebody for one purpose. We recognize that there is some right on the part of the individual to control the reuse of that information. So the statements, "It is public record information" or "I own this information," really do not settle the privacy debate. They only begin the debate.

The final point is that it is daunting to realize how little we really know. When we talk about these principles, including the use, disclosure, and retention limitations, and the data quality requirement, and particularly when we are talking about criminal justice information, it is disappointing how little we know about how this information is actually used, and what the value of it is.

So much criminal history information is now available and being used for employment screening purposes. I don't know if we know how employers use this information, or how they respond to naked arrests. Are they really doing what they are supposed to be doing in terms of not basing an employment decision upon naked arrests? How are people actually handling drug arrests? So many of these criminal history records, whether arrests or convictions, relate to drug offenses. A huge sector of the society probably has a drug record now. We don't want to say that those people are excluded from gainful employment ever again, but I don't think that we have very clear rules, and certainly we have nothing close to a national standard, on what is disqualifying, when it is disqualifying, or what it is disqualifying for. Obviously with sex offense records, particularly sex offenses against children, empirical data shows that there is a high relevance of that information, and that there is a high correlation between past conduct and likelihood of future misconduct. But once we get out of those areas and into other criminal offenses, I don't know if we have adequate data. We are talking about a system where private and public data is increasingly mingled. We are talking about situations where the concepts of government controls and government responsibilities in terms of accuracy, completeness, and purging, are being lost as that information gets into private-sector databases. I don't know if we have any good way to enforce those principles in the private sector, but that is where we have to go. We should really get there pretty soon. I would like to see more work done. I hope SEARCH can do more work on some of these underlying questions about the reliability of this data as we think about setting privacy access use standards for the next 5 years, let alone for the next century. So with that plea, I thank you.

# Identity fraud and the case for privacy protections

**BETH GIVENS**
*Director*
*Privacy Rights Clearinghouse*

I want to thank SEARCH for inviting me to speak at this conference. And I want to commend you on this conference and on the work of the Task Force. It's a pleasure to be here and to learn of your findings.

My name is Beth Givens, Director of the Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy program established in 1992. The topic of my presentation is identity theft.[1]

We began to work with identity theft victims in 1993 and have developed several guides, available on our Web site at www.privacyrights.org. We operate a consumer hotline and have been contacted by tens of thousands of consumers over the years — on everything from junk mail to Internet privacy. But the issue that has consumed most of our attention is identity theft.

The most common form of identity theft is when someone obtains the Social Security number (SSN) and perhaps a few other pieces of information about an individual, and uses that information to impersonate them and obtain credit in their name. The imposter might apply for credit, rent an apartment, get phone service, buy a car — and then not pay the bills, giving the victim a bad credit rating. Victims must then spend months and, typically, years regaining their financial health.

Based on credit bureau statistics, we estimate that there are going to be 500,000 to 700,000 victims of this crime in 2000. The Federal Trade Commission calls this the fastest growing crime of our time. Alan Westin mentioned yesterday that an Opinion Research Corporation Survey (for Image Data) found that 1 in 5 households had experienced identity theft.

We recently conducted our own survey of identity theft victims with another nonprofit group in California, the California Public Interest Research Group (CALPIRG). We learned that the average amount of time it took before the victim became aware someone was using his or her identity to obtain credit was 14 months. The average time it took to clear up the credit records was 2 years.

Today I want to talk about another kind of identity theft, what I call the worst-case scenario of identity theft. That is when an imposter commits crimes using the identity of someone else and gives that person a criminal record. For lack of a better term, we're calling this "criminal identity theft." My presentation is in five parts:

[1] Ms. Givens' accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/IdentityTheft-Prevention-Navy.ppt.

1. A description of this crime and a few case histories.

2. The work of an ad hoc task force in California that has been studying ways in which the victims can clear the record.

3. Information on two legislative bills that have been introduced in the California State legislature as a result of our task force's efforts.

4. The unresolved issues of the information brokers.

5. Some recommendations for changes in the information broker industry to ease the plight of criminal identity theft victims.

## Description and case histories

The reason I call this the worst-case scenario for identity theft is that there are no established guidelines for regaining a clean record. At least with credit-related identity theft, the victim deals with three credit bureaus and in most cases a finite number of fraudulent credit accounts. While the process is daunting for victims, it ends for most victims, albeit 2, 3, 4 years down the road.[2]

Credit-related identity theft victims usually find out about their plight when they are trying to obtain credit themselves, something many individuals do every few years, and for some, even more often. Another way consumers discover they are victims is by being contacted by a credit issuer who spots a suspicious-looking application. A third way is when individuals check their own credit report, which more and more consumers are doing these days.

But the victim of criminal identity theft may not know that someone has burdened them with a criminal record until they are stopped for a traffic violation, the officer runs a check on their driver's license number, and they're arrested on the spot. Or perhaps they apply for a job, are turned down, and obtain the results of the background check because the employer is actually complying with the *Fair Credit Reporting Act*[3] (something that is not being done across the board, and which I'll talk about in a moment).

Another example is what happened to a young law school grad in San Diego: she showed up for her first day of work, was handcuffed and taken to jail. The background check done by her new employer, the San Diego County District Attorney's office, revealed a warrant for her arrest — possession of marijuana, by the person who stole her wallet and assumed her identity.[4]

Certainly, consumers are not checking their criminal records once or twice a year, as we recommend that people do with their credit reports. In fact, there is no easy way for individuals to do so.

Credit-related identity theft can ruin your life for a couple years. Criminal record identity theft can ruin your life forever. It is virtually impossible to wipe

[2] See the PRC's identify theft publications at www.privacyrights.org/identify.htm.

[3] 15 U.S.C. § 1681 *et seq.*, as amended.

[4] Valerie Alvord, *"When dreams turn ugly: Stolen identity put her budding career in handcuffs," San Diego Union Tribune*, Aug. 29, 1999.

the slate clean. Let me give you a few case histories.

**Case 1:** Bronti, a man in southern California, worked as a retail store department clerk after he finished his stint in the Air Force. He was let go after the holiday season and didn't think much of it. He knew he could get other clerk jobs easily. But he was wrong. He applied for job after job and was turned down. Without employment, he lost everything and eventually became homeless. He got another job opportunity selling men's clothing. But when he showed up, he was told they changed their mind. He demanded to know why he was let go. That's when he learned of his erroneous criminal record. He was listed in a database used by all the department stores in Southern California that he was wanted for arson and shoplifting. When he put two and two together, he realized that the individual who stole his wallet several years ago had been using his identifying information when arrested and released. Bronti contacted us in 1996 and has been instrumental in our learning about this worst-case scenario of identity theft, and in working with the legislative process to pass laws to prevent his situation from happening to others.[5] Since then, we've learned of many more such situations.

**Case 2**: Pamela, who lives in the Los Angeles area, was impersonated by her sister who was arrested on drug charges. Pamela is of college age and has not been able to get any employment except a minimum wage job where a friend of the family hired her. She has attempted to clear her name through the court system but has not fully succeeded.

**Case 3:** José, a San Diego resident with roots in Mexico, was returning to San Diego from Tijuana, just south of the border. He was detained in secondary inspection, and arrested because his Social Security number matched someone who had committed crimes in the San Francisco area, 400 miles to the north. He was transported to San Francisco and held in jail for 10 days, all the while protesting that they had the wrong person. When finally they compared his prints with those on file, they released him because they realized they had the wrong person. He sued and won a small settlement for the wrongful arrest.

**Case 4**: Many of you may have seen NBC's *Dateline* on April 18, 2000 — the story of Scott Lewis of Ohio.[6] This isn't identity theft, but the effect was the same. He, like Bronti, had been gainfully employed but had been laid off. He didn't think he'd have a problem getting a new job but he did. He lost everything, including his wife and baby, and ended up living with family members. Through an encounter with a private investigator who offered to help him, he learned that the sheriff's department had made a clerical error, assigning his Social Security number to the record of a murder suspect. When the sheriff's department was apprised of the error, they corrected the record immediately. Scott thought his run of bad luck was over, but it wasn't. The

[5] *See,* David E. Kalish, "Dogged by bogus data," Associated Press, Sept. 24, 1997, at www.bergen.com/biz/privacy9709240.htm.

[6] *See,* "Stolen identity: Could it happen to you?," at http://stacks.msnbc.com/news/397082.asp.

private eye suggested that they look at the records of an Ohio-based information broker, and found that it still had the erroneous murder record on its files. The company did remove the error. But when an attorney helping Scott asked for the names of all the companies that this information broker had sold the erroneous record to, they said they didn't have that information.

You are probably wondering just how much of this is going on? How many individuals are saddled with wrongful criminal records because of identity theft or other types of errors in criminal records?

There are no hard and fast figures. I got a call from the records manager in the police department of a major Southwestern city just last week. She said they put a couple people in jail wrongfully each month because of identity theft. They've started releasing them and cutting them a check to compensate them for their misfortune.

As I mentioned earlier, we recently conducted a survey of credit-related identity theft victims. We asked those individuals if they had to deal with wrongful criminal records. We were very surprised to find that 15 percent, or about one in six, said they had obtained a criminal record because of the actions of their imposter. By the way, you can read that report on our Web site. The title is *Nowhere to Turn: Victims Speak out on Identity Theft.*[7]

Do I think this problem is insignificant, happening to a very few unfortunate individuals? No. Do I think it's a problem that's going away? No, I think it's only going to grow as databases grow and as they are merged with other databases. There is no such thing as a perfect database.

## California Identity Theft Task Force

What is being done about this critical problem? Bronti's case prompted a few of us in Southern California to establish an ad hoc identity theft task force in order to study the vexing problem of criminal identity theft, and examine the kinds of changes that are needed legislatively in order to enable such victims to clear their names.

Our informal group has met several times since August 1999 to brainstorm and come up with legislative proposals. The task force is comprised of the Los Angeles District Attorney's Office, the California Attorney General's Office, the Judicial Council of California, the Department of Motor Vehicles, the Los Angeles Police Department, the Los Angeles Sheriff's Department, myself and another consumer advocate, and two victims, one being Bronti.

## Legislation

Our work resulted in two bills being introduced in the California Legislature this year. Each has fared well so far in the legislative process. Assemblywoman Susan Davis's AB 1897 establishes an expedited court process to enable individuals to petition the court to obtain a determination of factual innocence and get the

[7] CALPIRG and Privacy Rights Clearinghouse, Janine Benner, Beth Givens, and Ed Mierzwinski (Sacramento: CALPIRG, May 2000), available at www.privacyrights.org/ar/idtheft2000.htm.

record sealed, expunged, or destroyed. This bill would fine-tune and expand some of the statutes already in place. Most importantly, it establishes one's local jurisdiction as the starting point for this process.

Assemblyman Tom Torlakson's AB 1862 is backed by the California Attorney General. It would enable the creation of a database within the California Department of Justice to record information about bona fide victims of criminal identity theft. When such an individual is, say, applying for a job where they know there will be a criminal record background check, they can inform the employer that they are a victim of identity theft and let the employer know that this database can be accessed to verify that fact. The job applicant would have personal identification number access to the database and could authorize others, such as employers, to access the database also.

Both these bills are still young in their legislative life and are being fine-tuned as they progress.[8]

## The role of commercial information brokers

There is another piece to the puzzle — and that is the commercial sector information broker. In both Bronti's and Scott's cases, they were denied employment time and time again because it appears that the employers had obtained the wrongful criminal record information about them. I think it is significant that these two individuals were not informed by their employers of the results of their background checks. I will return to that in my closing recommendations.

Our identity theft task force in California has come to the conclusion that we need to address the role of the information brokers — but we have not yet had time to do that. So I'm going to jump ahead of our group's discussion and offer my own suggestions on ways to deal with the difficult issue of criminal identity theft.

## Recommendations

The FCRA governs background check notification procedures when third parties conduct them for employers. This law needs to be amended to require that job applicants be given the results of background checks in every instance — not just when the employer uses the report to make a negative decision about them. This is a loophole that I think results in a great deal of noncompliance with the FCRA. It's all too easy for the employer to say that they didn't use the background check when making the negative decision — that the individual didn't have the requisite skills, or that the job pool had other individuals with more qualifications.[9]

[8] ***Editor's note***: These legislative bills were passed into law during the 2000 California State legislative session. Information about the California Attorney General's Criminal Identity Theft Registry can be found at its Web site, www.ag.ca.gov/idtheft/general.htm.

[9] For the Federal Trade Commission's (FTC) guidelines on how employers must comply with the FCRA, *See* www.ftc.gov/bcp/conline/pubs/buspubs/credempl.htm.

There's another loophole in the FCRA that needs to be plugged. In this day and age of Internet access to public records data, employers don't have to use third parties at all to conduct background checks. They can go online and do their own. If they were to run a check on Bronti, they would find his criminal record and have no idea that an imposter created it. So employers must be required to disclose the results of background checks that they perform themselves, and provide the source of the information to the job applicants.

When we get calls from individuals who suspect that there may be negative information "out there" somewhere in databases preventing them from being hired, we suggest that they conduct their own background check by hiring a professional background checker or private investigator — which is how Scott discovered that he had the rap sheet of a murderer. There is now a service called PrivacyScan (www.privacyscan.com) that caters to such individuals.

There are numerous Web sites where you can access public records and credit headers. These are just a few that I've found. (FYI, Web sites such as these can be accessed by employers who do not use the services of a third-party employment background check company. When an employer conducts its own applicant investigations, it is not bound by the FCRA and does not have to notify an applicant if it has made an adverse decision based on the results of the background check.)

www.docusearch.com

www.infoseekers.com

www.1800USSearch.com

www.infotel.net

www.knowx.com

As I mentioned earlier, I believe there is a great deal of noncompliance with the FCRA. Otherwise, how do you explain Scott's situation where he was repeatedly turned down for employment but not told why? There must be much stronger penalties for noncompliance.

I recommend that the FTC do an investigation of the background check process and look at whether the FCRA is being adhered to regarding consumer investigative reports. The study should look specifically at the problem of criminal identity theft and ways that the FCRA can be amended to rectify this situation.

Yesterday, both Bob Belair and I alluded to the Individual Reference Services Group's (IRSG) voluntary guidelines. IRSG is comprised of 14 information brokers who signed onto a set of voluntary regulations with the FTC in 1997. I have been critical of these regulations from the start as not adhering to the Fair Information Principles (FIP) of Notice, Choice, Access, Enforcement, and Accountability, among others.[10]

[10] For more information on the FIPs, *see* www.privacyrights.org/ar/fairinfo.htm. *See also* the IRSG Website at www.irsg.org. The IRSG has indicated that it intends to dissolve as of January 2002, due to the July 2001 implementation of the *Gramm-Leach-Bliley Act*, Pub. L. 106-102, codified at 15 U.S.C. § 6801-6810, and the regulation of

For example, consumers should be able to obtain the actual copy of a report about them as compiled by the information broker for a reasonable fee. The IRSG agreement says that individuals should only be told the nature of the public record information that it makes available in background checks, plus the sources of that information.

The reason I believe the information broker should provide the data subject with the entire record, whether it is public or nonpublic information that has been compiled, is that it might report on the wrong Jane Smith, or it might have an imposter's record in an innocent person's name. Access at a reasonable price to the total report is necessary for the individual to know what others are seeing about them. This then ensures accountability of the information broker. You might be interested to know that U.S. Senator Dianne Feinstein (D-California) has introduced an identity theft bill, S.2328, which enables individuals to obtain a copy of their own dossier from information brokers at a reasonable price.[11]

In closing, I welcome the suggestions that any of you might have on ways we can address and solve the difficult problem of criminal identity theft. Too many people's lives have been ruined because of this crime. We must find solutions and find them soon. This crime is not going away.

credit header information.

[11] The bill was reintroduced by Sen. Feinstein in the 107th Congress as S. 1399, "The Identity Theft Prevention Act of 2001." For details, *see* http://thomas.loc.gov/.

## Panel question-and-answer session

Privacy and criminal history record information:
Is there a role for privacy in the Internet Age? What should it be?

**Q.** I have a question about the Data Privacy Directive and the Safe Harbor; the approval of the Safe Harbor approach for the United States and Europe by the European Union Article 31 committee. Do you think the approval of having this implemented will have an impact on the debate in the United States? Will it create more pressure for domestic legislation?

**A.** (Woulds) I hesitate to say whether it would have an influence in the United States. Clearly it is a step forward. Agreement has been reached and approval has been given to the Safe Harbors Agreement. I wouldn't venture into the discussion in terms of U.S. politics.

**A. (**Dempsey) It has been curious how little impact the European Directive and the Safe Harbor negotiations have had on the debate in the U.S. The Safe Harbor is an agreement between the European Union and the U.S. government stating that industry in the United States would voluntarily comply with certain Safe Harbor requirements that accord more protection to the data of European citizens than to the data of American citizens. This agreement was reached as a condition of engaging in cross Atlantic data transfers, such as credit card processing, insurance information, or information that a multinational corporation would collect in Europe on Europeans and ship to the United States for processing, use, or clearance of credit card transactions. The U.S. industry has agreed to treat that European data in accordance with the European Directive, or to give it equivalent protection. Saying that if it can be done for the Europeans, it can be done for the citizens of the United States has had remarkably little impact on the U.S. privacy debate. We are going to have to find our own way. The United States is not likely to adopt a European privacy commissioner model. We will continue sector-by-sector legislation, although I think we are tackling some really huge sectors. We have a financial information privacy process underway. It is not as good as privacy advocates want but probably more than the financial industry wants, and it is turning out that financial information is a huge chunk of the pie. We have a similar process underway for medical records. We are beginning the process of debating legislation regulating the online collection of information. All of that is proceeding with very little reference to the European model per se, although we must never forget that the European and U.S. principles are really the same. We all agree on that list of principles whether it is broken down into four, six, eight, or nine. Those are the basis of U.S. policy and the U.S. debate. How to translate them into actual reality is a hard issue. John and his colleagues in Europe spend full time trying to figure that out. We are also trying to figure that out in the United States.

**Q.** I am with the Justice Research and Statistics Association. A number of the conference speakers have talked about how technology is basically doing away with some of the effective protections of privacy. The issue I would like to raise is that in this country we do not have a national identity card. Instead, we have de facto substitutions of driver's licenses and Social Security numbers. We do not have a national registry, so we use the postal service database and commercial services to track people's movements. We are using technology to backdoor these kinds of things that are done in other countries. The issue I am raising for the panel is that it is hard to create protections for things that we pretend we aren't doing while we still do them through technology.

**A.** (Dempsey) You are right.

**A.** (Woulds) It is true that the advance of technology poses threats to privacy, but it is also an opportunity to provide solutions to privacy protection. One of my Canadian colleagues, Ann Couvikian, who was a member of the Task Force, has been a very strong advocate of the concept of privacy-enhancing technologies. She has produced a number of papers dealing with this topic and advocating the development of technology that enhances privacy rather than is a threat to it.

**A.** (Givens) If you want to see a kind of science fiction futuristic view of what society might be like when it is organized around a national ID, take a look at the movie *Gattaca.* The movie has plot holes big enough to drive a truck through, but it is an interesting concept.

**A.** (Dempsey) By the way, there is an initiative underway under the sponsorship of the U.S. Department of Justice. John's reference to Ann Cavoukian reminded me because Ann has been working on it, and her Canadian office has been very helpful. I think it is called "Privacy by Design." They have developed a set of principles for the design of criminal justice information systems and I think their report is entitled: *Privacy Design Principles for An Integrated Justice System*..

I am pretty sure Paul Kendall, who is the General Counsel at the Office of Justice Programs, and Ann Gardner, the Attorney-Advisor in OJP, have been working on that.

**Q.** I agree with Beth Givens about the FCRA. A problem we have had for a long time is that industry that doesn't go to a third party and pay a fee is not required to follow the fair information principles that are outlined in the FCRA. I think that is an excellent suggestion, and I would like to see that happen. The second question I have for Mr. Dempsey or Ms. Givens has to do with the bill to allow crime identity victims to register. As an information provider, we do address these issues with the victims, but one of the issues we face in dealing with information from the courts is that there is no facility at the court to record that identity theft has taken place. Is it appropriate to create a separate database or would it be more appropriate — like all other holders of information — to require that data record to include information of dispute?

**A.** (Givens) That may be the long-term solution. We are feeling our way along on this one. There is a bill, in fact, thanks to Bronti Kelly. There has been a lot of press on Bronti's situation so I use both his first and last name with his blessing. Last year he was instrumental in getting a bill passed in California, but it only went part of the way. It says that the record must state that the *conviction* was attributed to the wrong person. However, a lot of criminal-related identity theft is retained in *arrest* records. The criminal was arrested and released and then didn't show up at court. So that law does not go far enough. That law does not go far enough. That may be where we end up but we are going to begin doing it this way. In looking into solutions, I called a number of information compilers. One individual suggested a separate database that had security protections behind it. You would make sure that whoever was in the database was a bona fide victim. He thought that would be a good solution, and I hadn't even prompted it. I thought it was interesting that the idea [for a criminal identity theft registry] came from the commercial sector.

## The media perspective

Can and should the media's dissemination of criminal history record information be regulated?
*Prof. Jane E. Kirtley*

# Can and should the media's dissemination of criminal history record information be regulated?

**PROF. JANE E. KIRTLEY**
*Silha Professor of Media Ethics and Law*
*School of Journalism and Mass Communication*
*University of Minnesota*

I am cognizant of the role I play here, both for this conference and in my service on the SEARCH Task Force during the last 2 years. I am grateful to both SEARCH and the Bureau of Justice Statistics (BJS) for allowing me to be the gadfly in this lengthy and difficult discussion. A columnist for the *London Times* wrote last year that the rarest sentence in the English language is, "Nice program, but I thought the speeches were too short." Now in my case, given the limited amount of time I have, perhaps some of you will come away making that remark about what I have to say.

I want to start by congratulating most of the people in this room. Having listened to Alan Westin's report on his survey yesterday, I was delighted to hear about the high level of public confidence in government and law enforcement and its diligence in protecting personal privacy. Great! You have won! You have persuaded the public that you have achieved a high level of excellence in showing respect for privacy. How did you do it? I am mystified.

I submit that the relationship between the press, the public, and the government and privacy is always difficult, certainly insofar as the press has been concerned regarding access to criminal justice records. We have never had what I would characterize as a perfect relationship. Other journalists and I have engaged in a never-ending battle to open up government to oversight, and records are an important target in that battle. As you probably know, in a number of States in the last few years, the Society of Professional Journalists and other media groups have conducted what they refer to as "freedom of information audits." They send journalists to parts of the State where they are not well known to request access to government information. This is clearly public information under the open records laws. You can understand what the experiment is about. They are trying to determine whether the average citizen requesting access to records to which he or she has a clear legal right will be discriminated against because he or she is not a journalist. Time and time again it was revealed that this indeed did happen. Clearly publicly available information was denied to people who were not known. Most frequently, I am sorry to say, information was denied by law enforcement operations. If they didn't outright deny the information, the requestor was peppered with questions such as, "Who are you? Who do you work for? Why do you want this?" Under existing laws, the questions were illegal and completely

irrelevant to that person's right of access.

Things are changing, of course, as we have been hearing the last couple of days. The advent of computerization and online access has led to thoughtful, protracted discussions and debate about whether the old rules of access that worked imperfectly should be reexamined and revamped. Whether the question of how an individual is going to use the information should become a relevant question, and one that becomes a threshold issue to this right of entitlement to public information, has also led to thoughtful debate.

## Misuse of information

Most of what appears to be driving this discussion, in my judgment, is the fear of what we heard characterized yesterday as "misuse of information." This is a term that has come up again and again in the course of this debate. I have a number of degrees in English Literature, Journalism, and Law, and I confess I am not sure what "misuse" means. Do we mean publication in a newspaper? Do we mean basing the denial of housing or a job on a criminal record? Or, do we mean a telephone solicitation that occurs during dinnertime? I don't know the answer and I suspect no one in this room knows the answer, because we haven't defined our terms very well. Don't even get me started on the issue of defining the term "privacy." We must force ourselves to define these terms because otherwise we run the risk of criminalizing conduct indirectly. I am using the word "criminalizing" advisedly. We are prohibiting conduct by cutting off access to information that has historically been publicly available, and we are not grappling with the genuine social issue that is posed. Instead, we are closing off access to information. It is the chicken's way of approaching the question and I don't think it is appropriate.

It brings me finally to the issue of the press, which is what I am supposed to be talking about this afternoon. The question I was asked to address was, "Can the media dissemination of criminal justice information be regulated and should it be?" You know my short answer. "No! Of course not!" The Supreme Court has ruled many times that there is a strong presumption of unconstitutionality for any prior restraint on media dissemination of lawfully obtained information. This is not hard. This is not rocket science. This is something the Supreme Court has said in an unwavering pattern of cases since the 1930s.

## Carve-outs

In the last term the Supreme Court issued some opinions with which I have some difficulty. Most notably, they upheld the California statute in the Los Angeles Police Department case that limits access to arrest records to certain categories of requestors. Included in that favored group of requestors, of course, is the press, so you might think that I would have no problem with a statute or court ruling like that. But I tend to share the view of Judge Diarmuid O'Scannlain of the Ninth Circuit U.S. Court of Appeals, who made the observation that if the goal of these statutes is to protect privacy, then these kinds of carve-outs serve

that interest very abysmally. To his mind, publishing somebody's arrest in the *Los Angeles Times* is a far greater intrusion into that individual's privacy than selling that information to driving schools, attorneys, or detox facilities that might actually help the individual rather than humiliate him. I don't like carve-outs for the press, and I have studiously fought against them during my entire career. Many of those in the press have criticized me; especially folks in Illinois who have made a practice of getting carve-outs in a variety of statutes that typically provide special access rights to the press but not to the general public. My view is that the press and the public should have co-extensive rights, partly for the practical reason that Judge O'Scannlain says — once it is in the paper, it is in the public domain — but also because by creating these carve-outs there is a great danger. The danger is that we are giving the government the power to decide who is the press, an increasingly difficult and problematic task with the proliferation of new media, many of whom do not look or act like the traditional press.

Putting aside my parochial concern, I worry profoundly about this drive to close down information to the public because of the risk that those who will be looking at it are just engaged in "idle curiosity" — the term that we were using before — or other nefarious schemes. What exactly is the danger that we are seeking to avert here? What are the horrific privacy interests that are implicated by access to criminal history information? You may have seen in the *Washington Post* yesterday in their international roundup section about a law passed in France that prohibits the press from photographing suspects in handcuffs. The idea is to protect the presumption of innocence, and that was the justification we heard yesterday for some of the movements to close off access to criminal history information as well. It reminds me of a justification that we have heard repeatedly, and it calls to mind a couple of cases. One of them, of course, involved Richard Jewell, an individual who was wrongfully accused of having been the Olympic Park bomber, and was subjected to a great deal of press publicity.

The case in New York last year involving an individual who was brought out on a perp walk for the purposes of being videotaped by Fox Television is another example. He had been arrested, but not yet charged, and was brought out for this perp walk. Subsequently, he brought an invasion of privacy suit, based on constitutional grounds, against the government for subjecting him to this. The judge in that case wrote a rather vituperative opinion in which he said that there was absolutely no public interest in bringing that perpetrator out for the purpose of allowing Fox Television to raise its ratings. The judge, unfortunately, reflects a commonly held view, that the American public today has a high level of confidence in what you are doing in law enforcement and that is to your credit. But I think they are tending to forget that part of the reason they can have that high level of confidence is because of the nearly 200 years of experience we have in this country of having open and accountable criminal justice systems. I

suggest that the people who drafted the Bill of Rights would be profoundly shocked to think that personal privacy is now being used as a justification to hold people in secret, to keep arrests secret, to keep the faces of perpetrators off televisions, all in the name of protecting their privacy. I think we could look at many totalitarian societies where those kinds of secret arrests are commonplace, and which we deplore in this country with good reason.

Sometimes I wonder if I am railing at a tide that has already turned. Has the day passed when I can make these arguments in any way, shape, or form that will persuade anyone to stop and think as they are looking at how we juggle the issue of public access to criminal history information? I really do believe that public access serves the interest of not only informing the public for the interest of public safety, but also in protecting the rights of those who are accused. I recognize that increasingly that is not the popular view. I know that in some respects, maybe I should have given up 10 years ago when Justice Stevens in the *Reporters Committee* case wrote about the practical obscurity that Judge Martin reminded us of today.[1] There is a heightened expectation of privacy if information is only available in scattered sources. I have always thought that was an incorrect characterization. I think it is an expectation of nondiscovery, not privacy, and I don't like the idea of cheapening the word "privacy" in that way. I am losing on this issue, and we must be very careful to make sure the public doesn't ultimately turn out to be the loser as well.

## "Protecting" the records

The term I kept hearing during this entire debate and over the last couple of days was "protect." We must "protect" these records. We in the government must protect these records. I hope that as you are protecting these records, you will think a little bit about what kind of records you are collecting and maintaining in the first place. Our keynote speaker this morning talked about this subject.

The first issue rests on what information is in government repositories and whether it ought to be there. If it is highly sensitive and not serving a government purpose, I would be the first to argue that you should not have it and you should not maintain it. But if it is there and is serving a government purpose, then the presumption in my view is that it should be open. In this desire to protect the public from itself, and to protect the public from the press, we are rapidly going to eviscerate the important rights of the public and the press to engage in government oversight. I wonder, in this zeal of the government to protect the public, who will protect the public from the government?

My plea to you as I wrap up my remarks is to go very carefully as we try to reexamine these questions. Be careful what you jettison as you set out to protect this amorphous idea of privacy.

[1] In *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), the Supreme Court recognized there is a statutory privacy interest, under the Federal *Freedom of Information Act*, in automated, comprehensive criminal history records.

A couple of days ago when I first got to Washington, I went to the Library of Congress and was looking at an old kinescope of a play that was aired on the Kraft Television Theatre in 1957. It was called the "Night of the Plague," and was set in Britain just after the Second World War and involved biological warfare. At one point, one of the characters made an observation that I thought was very telling, "Error is never very far away from the most carefully calculated schemes." I hope we will all do our best not to engage in any error as we calculate these very important schemes. Thank you.

### Question-and-answer session

**Q.** I hope the press and media continue to maintain access to public record information, including criminal histories. From an ethics point of view, what are your thoughts on a journalistic organization that purchases 25 years of criminal record information for whatever initial purpose the request was made, and then turns around and markets that information to online users who are willing to set up an account and pay $3 per name search?

**A.** (Kirtley) Are you asking me from an ethics or a business perspective? I ask that seriously. I was smiling when I said it but I am quite serious about that. As I am sure you know, the Society of Professional Journalists and many other media organizations have very elaborate ethics codes that deal with what journalists should and should not do. One of the fixed and immutable ideas historically was that the business side works one side of the street, and the editorial side works the other side of the street and never the twain shall meet. Increasingly with media convergence, we are getting more and more news organizations that now have more multimedia capabilities and serve multimedia purposes. A couple of years ago Business Week got access to information that they were only entitled to use for the purposes of employment review, but actually ended up using it in a news story. This issue of blending the editorial and business side is something that causes other journalism ethicists and me a lot of concern. It is not so much a legal issue, at least in the way you posed the question, but I think it blurs whatever valid distinction there is between the First Amendment rights of the newsgathering side, and the rights of the business and advertising side.

**Q.** I am a District Court Judge from the State of Washington. I have more of an observation, and I agree with the professor on many of her comments. In my former life, I was an attorney for a metropolitan newspaper and we did a lot of work in investigative materials. I argued a case in front of the Washington Supreme Court on reporters' privilege. My concern is similar to the professor's. We have to remember that one of the clearer objectives here is the right of the people to really know what is going on in the government. Every time we talk about accountability, we talk about judicial decisions and the right of the public to know whether those decisions are really accurate and are based upon good information. In part, I believe that relates to the ability of the public to know what the judicial officer is doing. I realize this is anecdotal, but just as one

example, in the State of Washington we had a person who had been convicted of several drunk driving charges and a past conviction for vehicular homicide. A judge in one of the jurisdictions granted that person extreme leniency. It is very important for the members of the public to be able to judge what the judge is doing, and that involves the ability to get access to the court records.

**A**. (Kirtley) Thank you. When I was listening to the judicial panel this morning, I was concerned about some of the comments. It is important not to lose sight of the fact that although statistical information and general kinds of redacted material can tell you a lot about how a system is operating, often the reality of what is going on in a judicial system — and I would submit in a law enforcement system — really does depend upon the kind of individually identifiable information that some people, in the name of protecting privacy, are seeking to close off. Journalists have been fighting the battle of trying to keep access to those records open for quite some time, and to a great extent we are losing it. I think we are losing partly because of the public's visceral reaction to privacy. They can put themselves into the position of a record subject and immediately relate to that in a way that they didn't in the old days when national security was the exemption du jour. Journalists have not done a terribly good job in making this case, and in some respects have actually been acting almost in concert with many of the privacy advocates in telling stories that certainly need to be told about things like identity theft, but failing to also tell what the down side is to closing off access to our public institutions.

**Criminal history record consumers**

Should certain categories of consumers be allowed access to criminal history record information? What are the determining factors?

# The use of criminal history records by employers

**DR. DONALD F. HARRIS**
*President*
*HR Privacy Solutions*

[SLIDE 1] I would like to thank SEARCH for inviting me here, and I would like to thank all of you for still being here as we move through this afternoon. [1]

[SLIDE 2] I will start with a bit of my own background that is relevant to the presentation. I cut my teeth on criminal justice records at the Department of Corrections in New York City where I had to hire 1,000 correctional officers from 10,000 candidates on a civil service list within 1 year to avoid riots in the jail. That has been the most challenging and real life kind of management crisis I have had to face. Nothing has matched it since. I got to consume, if that is the word, a lot of rap sheets. And the diet is difficult as you will see. I went from that to work for Metro-North Commuter Railroad operating out of Grand Central, where we also did background checks using an outside service, Fidelifacts.

Bill Sharp and Tom Norton, his boss from Fidelifacts, were instrumental in helping to think through some of the issues that pertain today and bring me up to date on the *Fair Credit Reporting Act* (FCRA).[2] A lot has changed since I was doing criminal checks back in the late 1970s and early 1980s. So if I do make any errors on interpretation of the FCRA, Bill is responsible. That was a joke by the way. Thanks a lot, Bill. I do really appreciate it.

Over the last 5 years, through the International Association for Human Resource Information Management (IHRIM), I have promoted the idea of developing an HR code of practice or set of guidelines for employers that take the principles of fair information practice and apply them to the workplace. I am taking that very approach here in this presentation. I am going to take the principles of fair information practice, one by one, and apply them to employment practices, focusing on the use of criminal justice records in selection decisions. The results will be something of a scorecard, and will fit in with some of the previous presentations, providing a bit of in-depth case study from an employer's perspective.

## Relevancy

[SLIDE 3] I am going to start my discussion of fair information practices with the notion of relevancy. I do that purposely because I think relevancy is the toughest area, and one that affects all of the other areas. It is a basic principle of fair information practice that if the information you are collecting is not relevant for the purpose that you are collecting it, you should not be collecting it.

[1] Mr. Harris' accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/SEARCH%202000ppt.

[2] 15 U.S.C. § 1681 *et seq.*, as amended.

There is a social consensus that certain criminal history *is* clearly relevant to selection decisions for certain jobs and should be available to employers. We see laws to this effect. We see the polls that were reported yesterday. If we really wanted to underscore it, we had the recent horrendous slaying of five people in a New York City fast food restaurant, apparently by people who had a record of working at fast food places and holding them up. The factors entering into relevancy are: types of criminal offenses, the recency of the criminal history, the age of the criminal offender at the time, patterns that may appear if there are more than one offense, and the job responsibilities. What job is the person applying for?

First, one has to ask if certain criminal history is relevant for *all* jobs, such as violent crimes against individuals. Does any history of violent crimes render an individual unsuitable for any job? Will negligent hiring suits create a category of unemployable criminals? I would add negligent hiring suits as one of the major drivers that perhaps was not mentioned and not highlighted enough in those selected by the Task Force. It is a very powerful driver, certainly in the employment area. It is not government laws or statutes that are driving it. It is much more specific than increased demand for criminal justice records. Employers face a very clear liability. There have been so many killings, and particularly mass killings, in fast food places. If there is not some pressure to try to prevent those kinds of activities developing out of what has happened in New York recently, I would be surprised. But where do you draw the line in terms of violent crimes? If an employee takes the life of another employee, every employer probably could be sued by someone using the argument that they were not vigilant enough to check whether the person had a history of violent crimes. I don't know the answer to that question, but it is a tough one.

Another tough question is whether an employer should be allowed to not hire anyone who has *any* record at all? Aside from Title 7 of the FCRA, imagine the situation where you have no protected classes. I don't know what State or if there are any places that have no protected classes under Title 7, but if there were, how would we feel as a society about having an employer say they are not going to hire anyone who has ever brushed up against the law? There is nothing illegal about that as far as I know, although from State to State it may vary. Certainly variance in states laws is another factor that we will return to.

[SLIDE 4] I would like to make some other points on relevancy. If you really want to tackle the relevancy nut as I have called it, there are 28,000 different jobs according to the *Standard Dictionary of Occupational Titles.* There are tens of thousands of criminal offenses, whose definition varies from State to State. If you are talking about figuring out mapping the crime to the job in any comprehensive way, then you have a huge job ahead of you. It sounds something like the human genome project perhaps. There are certainly clear-cut cases where laws have been passed to protect the

children, or protect people in nursing homes, etc. Once you get past those easy cases, relevancy becomes very difficult to determine. There aren't many guidelines for determining relevancy, or any that are substantial in my opinion, or that I am aware of, for employers.

Furthermore, you have problems complicated by the gap between the actual history, and the record of what happened. In that regard you have conviction information but you may not have the arresting information. You may not have the charging information. You may just have a partial picture. Plea-bargaining gives you one set of results that may not accurately reflect what happened. Even if you have all of the possible available criminal information, the record may not tell the full story of what really happened. If you spent a lot of time, you might find out something relevant to that hiring decision after all. For example, what does a conviction for criminal trespassing signify? If you have been in law enforcement you know that often drug-related offenses are involved, but certainly not always. There could be a myriad of reasons why someone might be convicted for criminal trespass, including conscientious opposition to social injustice or war.

[SLIDE 5] Interpreting the ambiguity that exists within the records can consume a lot of resources for employers. It takes time and money to delve into this if you want to be fair, and not pass up a good candidate or deprive someone who should get a job. It is a disadvantage to the candidate, and it places a premium on the knowledgeable interpretation of criminal history records. Employers are not in the business of knowing the intricacies of the FCRA or State laws relating to arrest records, or the classification of crimes in 50 or more jurisdictions. Yet that is the position employers are placed in, that often leads them to outsource the investigation process to people who are knowledgeable.

What are the alternatives? A selection decision in itself is basically judgmental. You are making a prediction. You do not really know how a candidate is going to perform, what they will or will not do. Is there a better way for employers to find out what is relevant in a criminal history record? What about using an infomediary combining investigation and job analysis skills? There are now investigative agencies, but the investigative agencies typically don't know that much about jobs in all their myriad varieties. Is it possible to combine those kinds of skills and knowledge? Could this be done in an expert computer system? Could there be guidelines for relevancy? I think there should be guidelines for employers in determining what is relevant in a criminal history record.

Maybe it is time to think out of the box. What about the possibility of a certificate of employability system where the candidate basically comes with something where the decisions have been made, such as a classification scheme depending on certain categories of crimes? That may open a host of other privacy issues and I am not promoting it. I am just saying that maybe it is time to look at some other ways to approach this issue, since leaving

relevancy decisions up to employers is fraught with so many problems.

## Notice

[SLIDE 6] Other problems exist in relation to notice. As another basic principle of fair information practice, the FCRA requires notice to candidates before an investigative consumer report can be performed. This is a very positive step. The FCRA amendments in 1997 strengthen this by requiring both a pre-adverse action disclosure, and an adverse action notice.

However, there is a question here, as Beth Givens noted. What has the enforcement been? How much compliance is there with this? It is hard to tell the practical effect of this FCRA notice requirement when selection decisions are basically done sub rosa. Employers do not want to have complete openness about the selection process. They do not want to say why they didn't hire someone. It is inherently a judgmental process. There may be many factors. It may be that someone else is better qualified, and hopefully that is the major decision basis in all cases. I don't know if any studies have been done on the issue of determining whether well-intentioned pre-adverse action disclosure, adverse action notice is really being followed, or is effective. I would be very interested in seeing the results of a study like that.

There is also the problem that if the employer does his or her own in-house background check and deals directly with the State agencies, no notice is required to a candidate. That is a serious issue. The notice required under the FCRA has some holes from the point of view of fair information practice. It is very well suited to the basics of not hiring an inappropriate candidate, but it does not really address the issue such as what criminal history will be relevant or constitutes an automatic job rejection. It does not tell what will be done with the information after the selection decision. It does not really address the issue of future circumstances where an employer may decide to make additional checks. I think those are significant misses in the notice requirements.

## Consent

Consent is another basic principle of fair information practice. There is authorization under the FCRA before an employer can proceed to obtain a report, but I would argue that consent really doesn't apply in employment in the way that it does in other contexts, because there is an imbalance of power between an employer and an employee. It tends to be a somewhat coercive situation. If you are an applicant for a job you are not going to question the conditions of the notice or what is going to be done with the records afterwards. You are not going to raise these issues. You do not have room to bargain and you cannot tell the employer that you may withdraw consent to do these reports at some point in the future. Whatever the FCRA calls it, consent in the pure or classic sense does not apply in the job-screening process, where the applicant is in many ways more of a supplicant.

## Fairness in collection

[SLIDE 8] My next topic is fairness in collection. I would like you to start by

imagining that you are dealing with a candidate who has some criminal history, but it is irrelevant to the job. Is it a fair information practice to be collecting derogatory, stigmatizing information? It is not like all the other information, the positive information and, hopefully, true information that you collect about credentials, qualifications, experience, background, ability, and what the person can contribute. You are collecting derogatory information. It falls into the category of, for example, employers in interviews who ask what is your worst characteristic? What is the worst thing you ever did for a previous employer? If you have not been prepared for this, you might blurt out something. Is asking that question really a fair information practice? I would suggest certainly not in cases where people have an earlier record that is irrelevant that they do not want to reveal. Why should they be forced to reveal it?

Furthermore, the standard provision on employment applications is that if you don't provide the full truth, and you falsify or omit anything, it would be grounds for not being hired. It seems a bit excessive to me with this category of information in mind. I think that language could be similar to information about disabilities. You do not ask if someone has disabilities. You ask if the candidate has any disabilities that affect his or her ability to do this particular job. Of course, in the real world you probably can't ask the candidate to tell you whether the criminal history is relevant or not — we've seen how complicated that is — but it is something to think about.

With regard to *any* criminal history, I have to ask, is it a fair information practice to collect such information from the candidate? Because of the way the system works, you have to go from jurisdiction to jurisdiction, State by State, and county by county in some cases to find out where the person lived and check all those sources. An employer ends up collecting a ton of information they wouldn't be interested in otherwise. Where the person has lived, and a list of all the jobs they have held is not relevant to the hiring decision. You end up doing a credit check, as we did at Metro-North, not because we cared about the person's financial status. We didn't want to see it. We did not keep it. We left it with Fidelifacts. We did not keep it on premises. We thought it was irrelevant, but we recognized its utility. We were forced into having a credit check done in order to find missing gaps in the employee's story where they may have covered up a certain time in their life, or a certain county somewhere that has a record that could bear significantly on this job. That is a problem in the system that creates an enormous overhead and over-reaching in terms of fair information practice.

[SLIDE 9] I have touched on the major problem areas. Access, on the other hand, has been improved dramatically. I am going to skip over that. For those of you who aren't familiar with this subject, this presentation will be up on the Web site.

[SLIDE 10] Accuracy also has been addressed and improved by some of the 1997 amendments to the FCRA, although some States still have time restrictions that can prevent one from getting a complete

picture. A 7-year credit history limit still exists in New York State, for example.

## Secondary uses

[SLIDE 11] Another critical area is secondary uses. The Federal Trade Commission published guidelines in 1999 stipulating areas in which employers can use criminal checks.[3] I have a lot of problems with employers using them for retention or reassignment decisions, particularly if you think of that as a secondary use for someone who has already been screened and hired. Notice forms may allow the employee to get new reports at any time. There are no limits on what the employer can do with this or when they can get them. I think there should be some tightening of that. Maybe legal counsel within an organization has to authorize it specifically, somehow log it, and control the process rather than just hand a blank check to the employer. At any time you as an employer can go into and get my records. There are no limits as far as I can see on this.

[3] *See* www.ftc.gov.

[SLIDE 12] Storage and retention is another key area. There are very few restrictions, if any, concerning where employers store criminal history records. Some people could be putting them in personnel files. That tags the person throughout their career. Keeping them in sealed envelopes is an alternative, or keeping them off site. Have a separate filing system to guard against the negligent hiring suits. How long you should retain these files is also rarely discussed. There is very little in the area of best practice regarding this issue.

[SLIDE 13] Few requirements or guidelines exist in the area of proper security safeguards for criminal history records used in the selection process. This is another negative mark on the scorecard of the use of criminal history records by employers.

[SLIDE 14] Lack of transparency about an employer's practices and uncertainties surrounding accountability and complaints are also problems. Is someone in the organization designated to hear complaints about the use or abuse of criminal history information? Has there ever been any FTC investigation or enforcement, or any empirical studies in this area?

## Conclusion

[SLIDE 15] In conclusion, there are significant privacy concerns around relevancy, the quality, and extent of notice that is provided, fairness in collection, secondary uses, and storage and retention. The FCRA is an extremely important and valuable piece of legislation from the point of view of protecting privacy and providing guidance to some extent to employers, but it is really not sufficient by itself. It is an imperfect instrument for protecting privacy in terms of the full scope of fair information practices. It hones in on the report side of it — the credit report.

I have focused on the privacy issues confronting the use of criminal history information by employers. I haven't particularly focused on the problems of employees or applicants. Employers find the current

system and procedures for checking criminal history records too complicated, confusing, costly, and time-consuming. When you want to hire people, whether it is the Los Angeles Police Department, the New York City Correction Department, Metro-North, or any place, you want the employment decision reached yesterday. You don't want to wait a day, a week, or a month for records to come through, cases to be sorted through, interpretations to be given, or for things to be figured out. You want to move on. That is what is important to the organization. Finally, adequate guidance is needed. Guidelines for employers are needed in this area.

Thank you very much for your attention.

# The perspective of a noncriminal justice user of criminal information

**LAWRENCE F. POTTS**
*Director, Administrative Group*
*Boy Scouts of America*

When they invited me to present at this conference I asked, "Why me? I am a Boy Scout." Bob Belair said, "Larry, it is because you *are* a Boy Scout that we want you. We want your perspective." So here it is. This is the perspective of a noncriminal justice user of criminal information.

To help me get a feeling for the audience and maybe to give you a little exercise, I would like to see by a show of hands who was either a Boy Scout or a Girl Scout as a youth, or an adult leader with one of those organizations. Could you just raise your hand? Wow. I'll put my hand up there too. I think I am probably preaching to the choir here about those kinds of organizations. But those of you who served as youth know how important the volunteer leaders were in the quality of your experience in scouting. The essence of those two great organizations is the volunteer. Those of you who were volunteers for either one of those two organizations know how demanding that role can sometimes be. The Boy Scouts have about 4.5 million youths. Helping us to communicate with them are 1.1 million volunteers. We are tremendously dependent upon volunteers. Although I can't speak for the Girl Scouts, it is probably a similarly sized organization.

Those of us who are involved in the youth movement have a tremendous and abiding interest in the quality of leadership in our programs. As large as the Boy and Girl Scouts are, we are not unique. There are lots of national organizations like us: the Camp Fire boys and girls, the Big Brothers, the Big Sisters, Boys and Girls Clubs, youth programs for the YMCA and YWCA, youth programs for the American Red Cross, the Catholic Youth Organization, and other religious youth organizations. I could go on and on about the number of organizations involved in using volunteers to help them operate and deliver services to youth.

All of these organizations are interested in getting the highest quality of volunteer. At the same time, they have an abiding interest in privacy. They are not interested in violating privacy. Should anybody be able to check into the background of a person? We heard that questions asked yesterday and today. It is being debated lots of places outside these halls. I really cannot offer anything on that issue.

Should organizations like those that I have mentioned have some sort of access to background information systems? Should they be able to get a background check? I can unequivocally say yes. I don't think that should be news to anyone. It is not just my opinion. Look at the *1993 National Child Protection Act* passed by Congress, signed by the

President, and endorsed by the 1994 Crime Bill.[1] Look at the *Volunteer Protection Act of 1997*.[2] There has been lots of legislation in the States about access to criminal background systems for organizations like ours. There are several registry laws such as the *Jacob Wetterling Act*, the *Pam Lychner Act*, and *Megan's Law*, that have both Federal and State implications.[3] All of these statutes seek to make criminal background check information more accessible to organizations like the Boy Scouts of America (BSA) and other organizations so that we can provide the best possible leadership and improve the quality of mentoring and youth development programs for all of America's youth. I was pleased to see the results of the survey that were presented yesterday showing that 88 percent of those surveyed felt the same way. There is not much question that certain groups should have access.

## Uneven access to technology

Technology is developing very quickly around the keeping and transmitting of information databases, and speeding access to those databases. The ability, however, of States and the Federal government to come up with the funding to keep up with this technology is not uniform across the country. Access to high technology is uneven. In some States access is very high tech and in others it is not. The increased speed and accessibility has also increased the need for improved responsibility in handling and managing that information. We have heard a lot about that in this conference, but most of it has focused on what States, repositories, and databases need to do internally. The organizations seeking access need to come up with guidelines. It has major implications for people like us. Nonprofit organizations are not all big. They are not all national and they are not all sophisticated. Lots of organizations do not even understand the issue of doing criminal background checks. If we begin to criminalize or do things that will make it much more difficult to do background checks, they will shy away from it. They won't do them. Our real objective is to do responsible checking, making sure that the best possible people are giving guidance to our youth. I include the elderly and disabled populations. And again, that is not my view. That is a legislative view.

Outside of Federal government, the threat of legal action is often a policeman for public policy. Civil organizations like the Boy Scouts and corporations are always trying to protect themselves from civil liability. The BSA has a vested interest, more so than just wanting to do it right. They also have a vested interest in not wanting to be sued, even though we are talking about volunteers. Generally, if we bring someone in that has a criminal background record that we should have known about, it is called wrongful employment. If we have to go the next 10 or 15 years

---

[1] Pub. L. 103-209 (Dec. 20, 1993).
[2] Pub. L. 105-19 (June 18, 1997), 111 Stat. 218.
[3] *Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act*, 42 U.S.C. § 14071; *Pam Lychner Sexual Offender Tracking and Identification Act of 1996*, Pub. L. 104-236 (Oct. 3, 1996), 110 Stat. 3093; *Megan's Law*, 104 P.L. 145, 100 Stat. 1345.

waiting for the courts to develop a set of guidelines and policies, then there are going to be a lot of ramifications and some unintended consequences. We need to develop policies and guidelines for outside organizations as quickly as we can.

## Recommendations

What is the future agenda in this field? I really cannot say, but I am going to share with you some things I think we need. Some of these go right along with the recommendations of the report, some go right along with the comments we heard earlier, and some are just a little bit different.

1) We do need passage of the Federal National Crime Prevention and Privacy Compact at the State level. We heard about that today. Without it there is no real national effective criminal background check. Today you can go only as far as the State level. We need national checks given the mobility of the population. Ron Hawley indicated that we had seven Compact member States. That is good news to me. I thought we were only at six, but we really need to get all the States on board with the compact.[4]

2) We need low-cost, high-speed, responsible access to criminal background check information. Today, I am sorry to say in spite of all these technological advances, we have high-cost, slow speed, and only marginal access to the information.

3) We need legislators and people like you to know the cost of access is, in many cases, just as important to nonprofits as physical access itself. In fact, the cost of access can become an effective block to obtaining criminal background check information on volunteers for some organizations.

4) We need a central policy to put some reasonable and uniform standards or guidelines as to access to criminal background check information. We need a policy to establish guidelines for the many and varied approaches to balancing the need for certain groups to access the system to protect our children, our elderly, and our disabled against the right of privacy and against the responsibility of handling information. This is related to Bob Belair's presentation about the three-year commission to do detailed guidelines and reviews. It is needed for outside the criminal justice system as much as it is needed on the inside. Essentially, we need to teach people in these agencies how to handle criminal background check information they couldn't even access a few years ago. And many today can't access.

In closing, I would like to thank Bob for inviting me. I wanted to also thank him for inviting some of the other individuals with rich and a varied background and outlooks. I think it has really helped the entire conference and helped the discussion in the privacy area. Thank you.

[4] For the status of State approvals of the Compact, *see* www.search.org/policy/compact/privacy.asp.

**Commercial providers of background information**

Should commercial providers be regulated and, if so, how?
In the same manner as courts and law enforcement,
or by other specially applied regulations?

Panel introduction and overview of Individual Reference Services Group
*Emilio W. Cividanes*

Commercial providers of background information: Overview and recommendations
*Peter L. O'Neill*

Commercial providers of background information and existing regulations
*Stuart K. Pratt*

# Panel introduction and overview of the Individual Reference Services Group

**EMILIO W. CIVIDANES**
*Partner, Piper, Marbury, Rudnick & Wolfe, LLP*

One reason Ron Plesser was asked to moderate this panel — and I was asked to do so in his stead — is because of our role in creating the Individual Reference Services Group (IRSG), which has been mentioned several times in the past 2 days. After I discuss that a little bit, I will turn it over to our two panelists, Peter O'Neill and Stuart Pratt.

The IRSG is comprised of leading companies in the business of providing information that assists users in locating and identifying individuals.[1] In close consultation with the Federal Trade Commission in 1997, the IRSG developed a comprehensive set of 11 self-regulatory principles backed by audits and government enforcement, which really is more voluntary regulation than self-regulation. A number of areas are covered by the principles. Companies that sign on to the IRSG principles, for example, commit to acquire individually identifiable information only from sources known to be reputable. They commit to educate the public about their database services through a variety of ways. They commit to furnish individuals with information contained in their services, and products that specifically identify them unless the information is publicly available or a matter of public record. In that case, the companies provide the requesting individual with guidance on how they can obtain the information from the original source, which is the best place to make any corrections and changes.

## Self-imposed restriction

The core of the IRSG's self-regulatory efforts, however, is the self-imposed restriction on use and dissemination of nonpublic information about individuals in their personal (not business) capacity. The focus in most of the policymaking has been on credit header information, but this information can cover criminal history information as well. The IRSG members who supply nonpublic information to other individual reference services provide such information only to companies that adopt or comply with these principles. The principles define the measures that the IRSG member companies will take to protect against the misuse of this type of information. The restrictions on the use of nonpublic information are based on three possible types of distribution that the services provide: 1) at the very restrictive level, a selective and limited distribution, 2) at the commercial and professional distribution and, 3) at the general distribution. The

[1] *See* www.irsg.org. The IRSG has indicated it intends to dissolve as of January 2002, due to the July 2001 implementation of the *Gramm-Leach-Bliley Act*, Pub. L. 106-102, codified at 15 U.S.C. § 6801-6810, and the regulation of credit header information.

quintessential general distribution is a Web site type of operation, and at the other end — the quintessential selective and limited distribution — the customer is usually a law enforcement agency. Not exclusively, but that is a quintessential type of user. In the limited and selective distribution of nonpublic information, companies state what uses their information is appropriate for and provide such products only to qualified subscribers. The subscribers are required to state their appropriate use, the purpose for using the information, and to agree to limit the use and re-dissemination of the information to those stated purposes. The subscriber's qualifications and intended uses are reviewed and screened before the information is made available to them.

The principles are enforced in a three-fold way. First, through their public commitment, the signatory companies are responsible under existing deceptive practices law if they fail to live up to these principles. Second, because the three major credit bureaus are members of the organization, the principal suppliers of the nonpublic information — the credit header information — require by contract that all companies buying nonpublic data from them for resale abide by the principles. Non-complying companies risk losing access to the current data. Third, companies abiding by these principles are subject to annual outside assurance review. The signatory companies have to have annual outside review. Qualified, independent professional services, mostly accounting firms and security consultants conduct these reviews. Reviewers use criteria developed by PricewaterhouseCoopers[2] and the summary of those reports are made publicly available upon request. But it has been subject to some criticism as all approaches are subject to criticism. The *Fair Credit Reporting Act*, which has been around for over a quarter of a century and the subject of amendments in 1996, is also a subject of criticism, but we are going to shift over to a discussion of how the FCRA operates in this area in terms of criminal history. For those purposes, Peter O'Neill will give us that summary.

[2] PricewaterhouseCoopers is a global organization that provides a number of services, including audit, assurance and business advisory services. www.pwcglobal.com/.

# Commercial providers of background information: Overview and recommendations

**PETER L. O'NEILL**
*Chief Executive Officer*
*CARCO Group, Inc.*

I am going to try to stick to the topic that was posed to me by SEARCH. Should commercial providers of background information be regulated?[1] When I spoke to Bob Belair and SEARCH and realized that most of you are from the criminal justice services business, I decided to focus my attention on criminal history records rather than cover all types of information gathered during an investigation. But first it is important that we break this topic down. There are two types of organizations that provide background investigations of individuals: consumer-reporting agencies that provide consumer reports under the purview of the Federal *Fair Credit Reporting Act* (FCRA)[2] and other entities that provide reports that don't meet the FCRA criteria of a consumer report. It does not mean that an entity cannot perform in the capacity of a consumer-reporting agency one day, and the next day perform functions outside the scope of the FCRA, which primarily focuses upon consumer reports. It is not left to a person or entity to deem itself a consumer-reporting agency or not a consumer-reporting agency. That is really important for you to understand. When one conducts criminal history record checks, he/she can be asking for information on two individuals, and in one they are functioning as a consumer-reporting agency and in the other they are not. The purpose for which the criminal history record search is performed determines whether, in that instance, one is acting in the capacity of a consumer-reporting agency.

Those of you from criminal justice services may have heard the term "consumer-reporting agency." Let me explain to you that it is a word that has really been made famous or infamous by the Congress in the passage of the FCRA way back in 1971. I want you to understand that the name "Fair Credit Reporting Act" is a misnomer. Congress did a disservice to us when it named this law the Fair Credit Reporting Act. For 29 years I have been fighting not only with lay persons, but members of Fortune 500 company legal departments, when they tell me they do not come within the purview of the FCRA because all they are asking us to do is criminal history record checks. So, I take Congress to task for the 29 years it has put a label on this law, which has been misunderstood not only by lay people, but also by many attorneys and users of consumer reports. They had a chance to correct this deficiency in 1996. They

[1] Mr. O'Neill's accompanying PowerPoint presentation can be accessed in conjunction with this speech at www.search.org/conferences/priv_tech_2000/pon.ppt.

[2] 15 U.S.C § 1681 *et seq.*, as amended.

didn't do it. They had a chance to amend this in 1998 and they did not. It is unfortunate.

### What is a consumer report?

Let me define for you what a consumer report is. Keep in mind as you hear the last couple of words of this definition that these are words of the Congress in 1971. It is tough to hear them 29 years later when we are in a politically correct society. "A consumer report is any written, oral or other communication of any information by a consumer-reporting agency bearing upon a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living." Think of how outrageous it is today for a human resources department to pass that verbiage on to an applicant. What is his or her mode of living? Do you mean is he living with a woman out of wedlock? Do you mean are two men living together? These are the words of Congress that exist today. When we do an investigative consumer report, the employer has to provide this information to the applicant. These words are required when a person is: 1) applying for insurance, 2) seeking credit, or 3) being considered for employment purposes. There are also some other exceptions that I am not going to bother you with. Because of the criminal justice focus of this group, we are only going to speak about *employment* because when you grant credit, you rarely do a criminal history record check. When one applies for an insurance policy, it rarely requires a criminal history record check.

The word "employment," as defined by Congress and the FCRA, covers four functions under this term: hiring, reassignment, retention, or promotion. Let's suppose that you have two candidates for promotion and both have been with the company for 10 years. Before you promote one of them to vice president, you decide to request a background investigation on them; you want to make sure there are no skeletons in the closet. If the background check is performed by a third party, it is a consumer report. A consumer report results from a three-party function. You have an employer, an applicant (or employee because it could be a post-employment situation), and you have the third party. When that third party is the provider or producer of that information, that third party is a consumer-reporting agency. That can be the ex-deputy sheriff or what have you, or it can be a company that functions like our own, which solely provides consumer reports. When one performs that investigative function, be it your law firm or otherwise, for permissible purposes as defined by the law, it is a consumer-reporting agency and, therefore, comes within the purview of the FCRA and its regulations. However, as somebody mentioned earlier, when you have an investigation done in-house by the human resources, security, or the legal department, the protections afforded under the FCRA are not available. It is a glaring area where victimized people have little redress. When one performs a consumer report, it is not necessarily just information relating to credit. A consumer report could include education verification, employment, professional licenses —

like a doctor, lawyer, CPA, or what have you. All of these become a consumer report if they are done for permissible purposes, which are defined by Section 604 of the FCRA.[3]

## Should our industry be regulated?

I submit to you that, unequivocally, the answer is no. That is probably what you would expect from someone in my business, but I think you will be surprised to learn as we walk our way through this law, that it provides an enormous amount of protection for the individual's right to privacy. You are going to find out that the individual has remedies in Federal and State court. A paper trail is available to detect and prosecute a person that violated this law, if necessary. There are tremendous safeguards, and that is really the basis for my opinion as it regards additional regulation.

Let's look at some of the benefits under the FCRA as they relate to the protection of privacy. We are going to look at it from the user's (employer's) perspective, from the subject of the investigation's (the consumer or individual) perspective, and from the consumer-reporting agency's perspective.

Before an employer can order a consumer report, it must have a permissible purpose. In other words, you may work for an employer, but that doesn't mean that your employer can order a consumer report on you. It must have a permissible purpose. The employer must certify to the consumer-reporting agency that it will only order consumer reports for permissible purposes as defined by Section 604. It must also tell the agency the specific reason for which the report will be used, i.e., continued employment. The employer cannot simply sign a blanket certification without identifying the specific reason(s). You have to check the box and say what particular reason or reasons you are going to order a consumer report. Then, as a user or an employer, you have to certify to the consumer-reporting agency that you will use the report for its intended purpose(s) *only.* You cannot get it for employment purposes and use it later for some other purpose that was not earlier identified or is not intended within the law. Next, you must certify that the usage of this report will not violate Federal or State equal opportunity law. And finally, you promise the consumer-reporting agency, or certify, that you will not take any adverse action against the subject without providing advance notice, a copy of the consumer report that you used wholly or partially for this decisionmaking, and finally, without giving that consumer a three-page document prepared by the Federal Trade Commission (FTC) explaining their rights and providing places where an aggrieved party can seek redress.[4] This is what the employer must do.

The employer must also certify that it will notify the applicant that a consumer report may be obtained for employment purposes. In the case of an investigative consumer report, the

[3] For the full text of the FCRA, *see* www.ftc.gov/os/statutes/fcra.htm.

[4] Mr. O'Neill provides a list of several different Federal agencies authorized to enforce the FCRA in his slide presentation. *See* www.search.org/conferences/priv_tech_2000/pon.ppt

employer must also certify to the agency that it will disclose to the applicant that this type of report will include information relating to his/her character, general reputation, personal characteristics, and mode of living, as applicable, and, further, that it will disclose the nature and scope of the investigation to the consumer upon written request. This is what the investigation may cover. Then, the employer must get written permission from the applicant. We have the disclosure requirement under the 1971 Act, and under the 1996 amendment to the Act, the requirement that permission has to be granted. A disclosure is all that was required under the 1971 law. Now we are required to have written permission. The disclosure must be clear. It must be on a separate piece of paper so someone can't say that they got a job with XYZ Company, were given 10 pages to fill out, and didn't pay attention to the fine print. It must be clear and conspicuous. When that person sees the FCRA authorization and disclosure form, he or she knows up front that they may be the subject of a consumer report. They know what it covers. They have given permission to have this done. I think the Congress and the FTC did a great job on the 1996 amendment.

## Adverse/Pre-adverse action

Then what happens if the user of the report, the employer, gets back a report that contains adverse information? Adverse information is anything in the world the employer deems to be "adverse." The employer is the determiner. It says, "because of the adverse information, I, the employer, may take adverse action against you." That triggers the requirement for pre-adverse action notice. The applicant is required to get a copy of the report and a summary of rights. The applicant has a number of days to address this issue so, if there is a mistake, that issue can be rectified before the job is given to somebody else. That is a new part of the law passed in the 1996 amendment. In the 1971 law, you could take remedial action, but the 1996 amendment is much more prophylactic in nature. A person cannot be turned down for a job, find out a mistake was made, and then have the employer say he is sorry, it was the repository's or the consumer-reporting agency's fault. For example, I went to New York University law school. There is another school in New York called New York Law School. If the consumer-reporting agency went to the wrong law school, I would have an opportunity to let them know a mistake was made before being turned down for a job. This is an outstanding protection for the individual's right to privacy and for their opportunity to gain employment.

If the aggrieved party, the applicant, wants to challenge this, the applicant has several days, based upon the nature of the job, to address this issue. If they do not address it and the employer takes adverse action, then it must tell the applicant they are taking adverse action. It must state that this action is based wholly or partially on the information contained in the consumer report, and make the applicant aware of certain rights and remedies. It must provide the name, address, and, if you are a national company like us, a

toll-free number of the consumer-reporting agency that provided the report. It must also be stated that the consumer-reporting agency did not make the decision. The employer made that decision. If the subject challenges the information in a consumer report and wants to see the entire reporting file held by the consumer-reporting agency, he/she has a right to do that. This is what the employer must do for the individual. In taking the adverse action, the FCRA gives several agencies authority to enforce its requirements.

What are the consumer-reporting agency's obligations in connection with this law? Number one, a section used in the 1971 law deals with "obsolete information." In 1996, Congress took the position that a consumer-reporting agency may not report derogatory data or adverse information for those anticipated to earn less than $75,000 a year, beyond a 7-year period. The thought process of Congress was that these people who earn less are least able to hire counsel, and to redress a wrong if they have been involved with the criminal justice system in terms of indictments that didn't result in convictions, or acquittals, or *nolle prosequi*. Yet, it is not in society's interest to see these people become wards of the state or return to a life of crime. Even though the consumer-reporting agency lawfully obtains this information, it may not disseminate it to the end user — the employer. If you think a consumer-reporting agency can't get caught, think about it for a moment. Somebody has a no conviction history and they know that they were indicted two or three or four times, and they get turned down for the job. It is a "no brainer." They see the report and the report is clean. The absence of that information in the report and the fact that the person is turned down may very well suggest that somebody picked up the phone and whispered that the subject was indicted three times, but no conviction resulted. If the employer cites some other fictitious reason for its adverse action, it isn't going to fly with the courts, I can assure you. There is a great deal of protection from the consumer-reporting agency side. In addition to that, when consumer-reporting agencies report a criminal history record, they have to do one of two things. They have to notify the subject simultaneously that they have obtained adverse information and are going to pass it on and divulge exactly to whom they are passing it on — not to just a prospective employer. Or, alternatively, they have to take measures to ensure that the information is current and up-to-date at the time it is reported.

## Consumer protections

Now let's turn to the protections for the consumer, the individual, and the applicant. Consumers (applicants) have to be told if the data was used against them. They can find out what is in their file. They can dispute the accuracy of data in that file. If they dispute it, it has to be reinvestigated by the consumer-reporting agency at its own cost. If the consumer-reporting agency cannot re-verify the accuracy of the information, it has to be deleted from the file. The consumer-reporting agency has to retrieve that information and give the user a new report with the disputed information removed. If, in

spite of the reinvestigation, there is still a dispute by the applicant, he/she has a right to, in 100 words or less, set forth his or her side of the story, which becomes part of the consumer report. Recipients of the consumer report get a copy of that so they can make a value judgment. Whose version does the employer want to accept? Is this a reason to turn somebody down? In essence, the consumer has these protections and outdated information beyond the 7-year window for those earning $75,000 a year or less has to be deleted, and the information contained by the consumer-reporting agency cannot be sent out to anyone who doesn't have permissible purpose and authorization. Finally, the consumer can seek damages for violations both in Federal and State courts.

In summary, I believe the FCRA provides strong protection for the consumer's right to privacy. It requires a detailed paper trail. It provides civil and criminal remedies and sanctions. I don't think any further legislation is needed in this area. However, I have recommendations. When Congress next addresses this issue, I strongly suggest it change the name of the law and delete the word "credit." That has been a terrible problem for us because attorneys and lay people say it doesn't apply because a credit report was not ordered. The FTC has done an outstanding job, particularly since the 1996 amendment, with its informal staff opinions. They are terrific. They are very beneficial. However, the FTC has not gone far enough. The FTC could see better compliance with this law if it would search out in the 50 States the names of entities that have private investigative licenses. Daily, competitors tell me they are not a consumer-reporting agency; they just search public records. Or, "I am a private investigator; I am not a consumer-reporting agency." These entities need to be contacted by the FTC to educate them that when they perform a certain function, as defined by the FCRA, that provides a consumer report, they *are* a consumer-reporting agency. Finally, I think the FTC, not just dealing with Fortune 500 companies, should try to make as many employers as possible aware of the FCRA. It drives me crazy when a prospect states: "No, our law firm does this," or that the report is attorney/client privileged, or this is not a consumer-reporting issue. Of course, it is a consumer-reporting issue. I would like to recommend strongly to the FTC that they have a group of apostles or disciples that are believers. They are adhering to the law pretty well but they have to get the employers and those who don't believe that they come within the purview of the law that, in fact, they do. And finally, I would ask the FTC for better oversight. Feel free to audit us and feel free to sanction us. We need that to get the maximum benefit out of the *Fair Credit Reporting Act*. Thank you.

# Commercial providers of background information and existing regulations

**STUART K. PRATT**
*Vice President*
*Government Relations*
*Associated Credit Bureaus*

Thank you all for giving me the chance to be on your panel today. I was also given the honor of being a part of the Task Force that SEARCH put together as they prepared the report. I applaud the efforts of you and the SEARCH Task Force to not only seek the input of the judiciary — the administrators who handle this information from the State or Federal governmental perspective — but also to seek the input of the commercial side of the industry in this country, and in some ways the trade associations. I work for the Associated Credit Bureaus (ACB), which is as poorly named as the *Fair Credit Reporting Act* (FCRA)[1] because today the ACB represents employment and tenant screening companies as well as traditional credit bureaus. It represents a whole range of companies that produce consumer information products. These information products are credit reports for risk management, and they help prevent fraud in the e-commerce world and with traditional retailers.

A wide range of companies use information in one way or another in this society to try to prevent crime, manage risk, and predict future performance. These are the kinds of information companies we represent. Peter O'Neill has already compartmentalized our discussion today very well. The kinds of databases we represent do not house criminal history information as you would think of it. In fact, we are the specialized companies that obtain information and then aggregate it with investigative data through other traditional data sources, and provide that to the employer who is going to make that employment decision. I think Peter has already discussed some of the protections and controls of the FCRA on that process and I couldn't agree more. In some ways I think that helps answer part of the question, "Should various parties who receive this kind of information be regulated?" One answer is that they *are* regulated. A statute under the FCRA governs a whole range of employment screening purposes where information is used. Peter pointed out there are some areas, for example, where the employer doing the work themselves is not covered in the same way. But where you have a third-party company (a consumer-reporting agency) producing an employment report, that company is governed under the FCRA. I was one of the lobbyists who worked on that law. I should have talked to Peter. I would have known the title was wrong and then we could have gotten that changed along with everything else. By the way, it only took us 8 years of debate to resolve the 1996 amendments on the FCRA, so Congress is moving at

[1] 15 U.S.C. § 1681 *et seq*., as amended.

its usual rapid pace through these things.

Again, I applaud all of you here today for giving us a look at criminal histories and for giving those of us in the commercial sector a chance to hear the range of views and concerns. The concerns include giving consumers a second chance in our society, civil liberties of individuals, and the propriety of this particular type of information. In preparation for this program today, I made some phone calls and talked with our members. I asked if they are storing this data or if they are using it for secondary purposes. When they obtained a criminal history from whatever data source were they using it again and again? The answer was no, absolutely not. There are controls within the FCRA that govern how and when a public record item in an employment report can be used. In most cases our members will simply comply with one of two choices. The choice is to ensure that it was updated within the last 30 days.

## Challenge of identity theft

I suspect, although I was not here, that Beth Givens has already discussed one of the challenges in criminal histories with regard to identity theft. In some cases the criminal record itself is polluted by the problem of ID theft, and sometimes the Social Security number and other information is not associated with the right person. One of the challenges we have in going forward is to make sure there is a system of remedies. In that way our members would share the same burden many of you have, and many of the repositories of criminal history data in the commercial marketplace. We should address that issue. We should make sure there is a system by which a consumer can remediate and fix that quickly and efficiently. I have certainly run across some of those myself. You get calls from time to time saying, “My brother is in prison under my name.” That is one of the dilemmas you have with inefficiencies of large databases, and it must be solved.

## Why have commercial providers?

On the other side, why have those databases? Why have a commercial venue? I will give you some reasons I think are important to many of us. How many of you are parents in this room? I see lots of hands go up. That is normal. If I didn’t get a lot of hands up, I would ask how many of you are aunts and uncles, and eventually I would get to you one way or the other. The point is, criminal history records are important and the companies we represent are important because they build the core competency to number one, to make sure it is done right, is the right record, has gone through the right vetting process, is held confidentially, and is only used for the single purpose for which it was intended to be used. Those are some of the core competencies you find in the commercial marketplace. That is really the nexus between the marketplace, and I think a good solid statute that is on the books — the FCRA. These companies help home health-care provider companies to evaluate those individuals who are going

to households to take care of the elderly. These are the companies that are going to help ensure that the school superintendents are hiring bus drivers who have the appropriate record. These are the companies that are going to ensure that a pedophile isn't working at a day care center. There are societally important, necessary, uses of criminal history information, which are not intended to close out the opportunity for an individual to find their way back into society and live a normal life. But if somebody were to ask me, as a parent of two small children, if a pedophile should work in a day care center, the answer is no. There are a lot of other jobs that are appropriate for a pedophile, but working in a day care center is not one of them. Many employers have almost a fiduciary responsibility under a range of other laws to ensure that the type of employee is a safe and sound employee.

Those are the types of uses our members are engaged in. We produce consumer reports. One type of consumer report is a criminal history record. Whether you are a private investigator, and whether you just misunderstood the title of the FCRA, whether you are a company like Peter's (and we represent companies like Peter's), you are a consumer-reporting agency under the FCRA for employment screening purposes. There is no way around that fact. To that extent, ensuring that the licensing agencies for private investigators are cognizant of the fact that many of their clientele, many of the professionals they license, need to be educated in this area, just as they seek education in a range of areas. This is not to denigrate the private investigative side of the business. They fulfill vital functions in insurance fraud investigations and that sort of thing. Those are the companies we represent. In some ways that is the public policy side of the question when I speak to members of Congress or meet with State legislators or talk about access to public records or criminal histories.

## We seek to be responsible

Are we responsible? The answer is yes we seek to be responsible. One of the reasons the Individual Reference Services Group (IRSG) was created was to address a void where information was being used in the context of whether it is private investigators or other types of databases out there in the marketplace. The question was asked that if it is not an FCRA-governed purpose, could there be an investigative appropriate use of criminal history information? There can be an employment screening. An FCRA-governed use of criminal history data as well. The IRSG helps to fill that void in a self-regulatory environment.

Let me emphasize a couple of points about IRSG. I do this because some of our largest members are members of the IRSG. This helps answer the question of who will have access to my information. Should I be able to build a Web site and display criminal history data on it? Today I found five or six Web sites on the Internet that do that. It is not hard. Do we endorse that? I don't see how a company on the Web can deliver a criminal history check without the proper notices. In each of these cases, there were no FCRA-style notices, and no

qualifications. In many cases, the companies selling the criminal history were saying that they are helping to make sure your housekeeper is honest, or helping to make sure that your childcare provider is the right choice for your children. All of that sounds good. The key, though, is to make sure there is a system in place to address the question of fairness. That part of the FCRA is very important. Was the data accurately recorded? Was the data accurately identified? Was it appended to the right individual? Did you make the right decision? Did a consumer then have an opportunity to exercise their rights under the law? This is the way the data should flow.

A series of rights, protections, and controls has to be appended to the use of the information. This is the great balancing act we have ahead of us with criminal history information. If you balkanize it, remove all commercial providers of information, or move it back into the States or counties completely, many of our members would have to pursue a wider range of contacts to try to find the right person, court, or agency, with whom they have to contract to access the information.

We argue that responsible, commercially viable governed databases of information should exist, whether it is governed under a voluntary system such as the ISRG or whether it is governed under the FCRA. Some of the devil of the details is in the difficulties I heard around the table during the Task Force report. In many ways we supported that process, we supported the dialogue, and we are very happy to be here today. I suspect we will continue that dialogue to work on a responsible system of managing criminal history information to make sure that even through the commercial marketplace, we can meet societal needs.

## Conclusion

Concluding remarks
*Robert R. Belair*

# Concluding remarks

**ROBERT R. BELAIR**
*Chair, National Task Force on Privacy, Technology and Criminal Justice Information*

Let me first thank Kent for doing a wonderful job over the last couple of days. We very much appreciate it. I want to thank BJS, Jan Chaiken, and Carol Kaplan. BJS has provided financial support and that is very important. They have also provided substantive leadership and guidance and we greatly appreciate it. Most of the speakers, but not all of the speakers you have heard over the last couple of days, have been from the Task Force. I do want to thank the members of the Task Force. They worked extraordinarily hard. They brought very diverse opinions to the table. They operated with great goodwill, and I think we did produce an extraordinary set of recommendations and a report. We will finish the report. We did want to wait for the conference though, because we felt that we would enrich the report with the proceedings yesterday and today. I feel that is right.

Let me just stop with this thought. In 1975, I attended my first SEARCH conference. I was then at the White House Committee on the Right of Privacy. It was at a time when we had really just figured out how to automate the criminal history record. And the question was, therefore, now that we have got this automated record that we can telecommunicate, what do we do? We all felt in 1975 that we were at the start of something very special. Eleven years later, by 1986, we had moved from having virtually no State laws to every State having laws that addressed confidentiality, accuracy, access, and so forth. I have this same feeling about this conference and where we are in the year 2000. I think that by 2010 we will have a whole new generation of criminal history law that will address the Internet and criminal histories. It will address integrated systems and criminal histories. And, most importantly, it will take a coordinated, consistent approach to criminal history information regardless of source, whether held and compiled by the commercial sector, the courts, or law enforcement. It will balance privacy and information needs, taking into account the subject matter of the information, the uses of the information, the public safety risk management payoff, and the privacy issues.

All of us here today are at the start of something very special. We are going to be working hard this year and next year and I hope over the next several years as this process unfolds. We look forward to working with all of you. And again, thank all of you very much.

# Contributors’ biographies

# Contributors' biographies[1]

## Robert R. Belair

SEARCH General Counsel Robert R. Belair is a Partner with the Washington, D.C., law firm of Mullenholz, Brimsek & Belair. Mr. Belair is also Chief Executive Officer of Privacy and Legislative Associates, a legal and policy consulting firm. The principal emphases of his practice are privacy and information law involving administrative, legislative, and litigation activity. His practice includes counseling in all aspects of privacy and information law, including credit and financial, educational, criminal, juvenile, medical, and employment records; telecommunications; defamation; intellectual property, including software copyright; constitutional law; and criminal justice administration.

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

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.

## John T. Bentivoglio

Mr. John T. Bentivoglio is an Associate Deputy Attorney General at the U.S. Department of Justice (DOJ). Mr. Bentivoglio serves as the senior adviser to the attorney general and deputy attorney general on computer and high-tech crime, health care fraud, and e-commerce. He also serves as the department's Chief Privacy Officer, a position created in 1998 to provide greater high-level attention within the department to privacy issues.

Prior to joining the DOJ, Mr. Bentivoglio served from 1986-92 as a professional staff member to the then-chairman of the U.S. Senate Judiciary Committee, Sen. Joseph Biden Jr. (D-Delaware). From 1993-96, he worked for the Washington, D.C. law firm of Miller, Cassidy, Larroca & Lewin, which specialized in white-collar criminal defense.

## Francis L. Bremson

As the Courts Program Director for SEARCH, Mr. Francis L. Bremson manages two major court

[1] ***Editor's note:*** The contributors' biographies are to be considered current as of the time of the conference, May 31-June 1, 2000.

projects funded by the U.S. DOJ: the Court Information Systems Technical Assistance Project, and the Drug Courts Evaluation and Management Information Systems Training and Technical Assistance Program.

The Courts Project, funded by DOJ's Bureau of Justice Assistance, seeks to develop practical resources for State and local court efforts to automate and integrate information systems, both within the courts and among courts and other justice agencies. Mr. Bremson also provides staff support to the 22-member National Task Force on Court Automation and Integration, which oversees the project.

The Drug Courts Program, funded by DOJ's Drug Courts Program Office, offers expert assistance to drug courts in planning, designing, developing, procuring, and/or implementing drug court evaluation and management information systems.

Prior to joining SEARCH in 1997, Mr. Bremson held a variety of management positions in State and Federal courts. He served as: Circuit Executive for the Ninth U.S. Circuit in San Francisco; Director of the Alaska Judicial Council in Anchorage; Regional Director of the National Center for State Courts in St. Paul, Minnesota; and Director of the Cleveland, Ohio, Court Management Project. He also served in government marketing positions for legal publishers LEXIS-NEXIS and Legitech.

Mr. Bremson holds a bachelor's degree from Hobart College. He obtained his J.D. from the Georgetown Law Center. He is also a Fellow of the Institute for Court Management.

### Hon. Thomas M. Cecil

Judge Thomas M. Cecil has served on the Sacramento County, California, Superior and Municipal Courts since March 1989. During his tenure on the bench, Judge Cecil has presided over each criminal department in both the Municipal and Superior Courts. He was selected Presiding Judge for the courts in September 1997 and served in that role through 1999.

During the 5 years that preceded his selection as presiding judge, Judge Cecil conducted felony trials, primarily homicides. For 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 Department's legal staff.

As an attorney, Judge Cecil practiced in a variety of areas, including bankruptcy, general business litigation, and corporate, family, and political law. He also served as Special Counsel to the Joint Select Committee on Municipal Liability Insurance (1976) 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 a member and past chair of the California Judicial Council's Advisory Committee on Court Technology. Judge Cecil is

currently a member of the Council's Advisory Committee on Trial Court Presiding Judges.

Judge Cecil holds a bachelor's degree from California State University, Fullerton, and a J.D. from the McGeorge Law School, University of the Pacific, where he serves as an Adjunct Professor teaching courses in Advanced Criminal Procedure and Sentencing and Post-Conviction Remedies.

### Dr. Jan M. Chaiken

Dr. Jan M. Chaiken served as Director of the Bureau of Justice Statistics (BJS), U.S. DOJ, from his appointment by President Clinton in 1994 until January 2001. As BJS director, Dr. Chaiken focused on the use of modern information technologies to provide the public with quick and easy access to research data, to facilitate the rapid interstate exchange of criminal history information, to advance implementation of the FBI's National Incident-Based Reporting System (NIBRS), and to improve computerized tracking of arrestees and defendants going through the criminal justice process.

Dr. Chaiken has been presented with two distinguished national awards in recognition of his efforts at BJS. He was the 1999 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*, the only nationally recognized, competitive award for contributions in the field of criminal justice information management. Dr. Chaiken was also the 1998 recipient of the Institute for Operations Research and the Management Sciences' (INFORMS) *President's Award*, which recognizes effective and important contributions in the public interest.

Prior to joining BJS, Dr. Chaiken worked for 9 years as a principal scientist in law and justice at Abt Associates in Cambridge, Massachusetts, one of the country's largest for-profit government and business consulting and research firms. There, he contributed to a number of criminal justice projects and was instrumental in the development of NIBRS.

Dr. Chaiken came to Abt Associates from the RAND Institute, where he pursued research on modeling the criminal justice system, studies of the criminal investigation process, and analysis of career criminals.

Dr. Chaiken earned his Ph.D. in mathematics at the Massachusetts Institute of Technology. He was an Assistant Professor at Cornell University's Mathematics Department, and he also served as an Adjunct Associate Professor at the University of California, Los Angeles' System Sciences Department.

### Emilio W. Cividanes

Mr. Emilio W. Cividanes is a Partner in the Washington, D.C., law firm of Piper, Marbury, Rudnick & Wolfe, where his practice areas are business and technology, and electronic commerce and privacy.

Mr. Cividanes is primarily involved in the practice of personal privacy, information dissemination, and telecommunications law. He counsels clients, engages in advocacy before Congress and Federal agencies, and litigates cases before the courts.

Mr. Cividanes has lectured in the United States and abroad on privacy, computer law, and related issues. He is co-author of *Privacy Protection in the United States; A Survey*, and of a chapter on privacy in *Internet and Online Law*. He also serves as an Adjunct Professor at Georgetown University Law Center.

Prior to joining the firm, Mr. Cividanes served as Counsel to the Technology & the Law Subcommittee of the U.S. Senate Judiciary Committee.

Mr. Cividanes holds a bachelor's degree from Haverford College in Pennsylvania and a J.D. from the University of Pennsylvania, where he served as Comment Editor for the *University of Pennsylvania Law Review*.

### Gary R. Cooper

Gary R. Cooper has served as Executive Director of SEARCH, The National Consortium for Justice Information and Statistics, since 1983. As Executive Director, Mr. Cooper represents 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 of the National Fingerprint File Pilot Project.

Mr. Cooper was appointed by California's Governor to the California Commission on Personal Privacy in 1981. He currently serves on the Board of Directors for the National Foundation for Law and Technology. During his more than quarter-century with SEARCH, Mr. Cooper has served as the Deputy Director and Director of the Law and Policy Program.

Mr. Cooper's law enforcement career began as a Patrol Officer for the City of Sacramento. He has held various research and planning positions with the California Council on Criminal Justice and the California Crime Technological Research Foundation. Mr. Cooper 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 holds a bachelor's degree in political science from the University of California, Davis.

### James X. Dempsey

Mr. James X. Dempsey is Senior Staff Counsel at the Center for Democracy and Technology (CDT). Mr. Dempsey joined CDT in 1997. 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 U.S. foreign policy documents.

From 1985-94, Mr. Dempsey was Assistant Counsel to the House Judiciary Subcommittee on Civil and Constitutional Rights, where his primary responsibilities were FBI oversight, 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 on crime issues, including the Federal death penalty, remedies for racial bias in death sentencing, information privacy, and police brutality. Mr. Dempsey has spoken on civil liberty issues in Russia, Poland, Hungary, Bulgaria, Guatemala, Chile, and Argentina.

From 1980-1984, 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 is co-author of *Terrorism & the Constitution: Sacrificing Civil Liberties in the Name of National Security* (with Prof. Davie Cole of Georgetown Law School). He graduated from Yale College in 1975 and from Harvard Law School in 1979.

### Timothy D. Ellard

Mr. Timothy D. Ellard, Senior Vice President at Opinion Research Corporation (ORC), specializes in research design, execution, and reporting. Mr. Ellard has more than 35 years of project management experience.

Mr. Ellard joined ORC in 1964 as a survey director. He was named Vice President in 1968 and Senior Vice President in 1970.

Mr. Ellard served for a number of years as head of ORC's Marketing Research Group and has also led the Government Research Group. He managed ORC's western office in San Francisco for 10 years, returning to ORC's Princeton, New Jersey, headquarters in 1991 to direct Survey Operations.

While Mr. Ellard has reduced his general management responsibilities at ORC, he remains on staff and continues to consult on engagements.

Prior to joining ORC, Mr. Ellard worked in brand management for The Proctor & Gamble Company, gaining special expertise in sales promotion and new product introductions, as well as product planning and package design.

He holds an A.B. in Social Relations with honors from Harvard College, and an M.B.A. in Degree Statistics and Industrial Management from the Wharton School of the University of Pennsylvania.

### Dr. David H. Flaherty

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

Dr. Flaherty previously served as British Columbia's first Information and Privacy Commissioner, independently monitoring the administration of the government's *Freedom of Information and Protection of Privacy Act*. Appointed by the government of British Columbia in 1993, Dr. Flaherty served a 6-

year, nonrenewable term in office.

Dr. Flaherty has more than 20 years of experience with privacy protection and access to information 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.

Dr. Flaherty has been a full-time academic in the United States and Canada since 1965. He received a bachelor's degree in history with honors from McGill University (1962), and a master's degree (1963) and a Ph.D. (1967) in history from Columbia University. He taught at Princeton University from 1965-68, and at 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 his appointment as Information and Privacy 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; from 1978-79, a Visiting Fellow at Magdalen College, Oxford; from 1985-86, a Visiting Scholar at Stanford Law School; during the 1992-93 academic year, a Fellow of the Woodrow Wilson International Center for Scholars in Washington, D.C.; 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 for the Standing Committee on Justice and Solicitor General of the Canadian House of Commons for its report on the functioning of the 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 public-sector privacy and data protection laws work in practice. In addition, he has also 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 writings emanated from his role as Information and Privacy Commissioner, and discussed the principles and practical application of information and privacy law in British Columbia.

### David Gavin

Mr. 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 advisory process, he has served as Chair, Western Regional Working Group; Chair, National Crime Information Center Subcommittee; and is currently Chair of the Advisory Policy Board. His education includes a master's degree from the University of Texas at Austin.

### Beth Givens

Ms. Beth Givens is Director of the Privacy Rights Clearinghouse (PRC), a nonprofit advocacy, research, and consumer education program located in San Diego, California. The Clearinghouse, established in 1992 with funding from the California Public Utilities Commission's Telecommunications Education Trust, is a project of the Utility Consumers' Action Network, a nonprofit consumer advocate regarding telecommunications, energy, and the Internet.

The Clearinghouse maintains a complaint/information hotline on information privacy issues and publishes a series of consumer guides on a variety of related privacy topics. These publications and other materials are available online at www.privacyrights.org. (Many of Ms. Givens' speeches are accessible at the Web site through the "Other PRC Resources" link.)

Ms. Givens frequently speaks, conducts workshops, and is interviewed by the media on privacy issues. She has testified on privacy-related public policy concerns before the California Legislature, the California Public Utilities Commission, the National Telecommunications and Information Administration, the U.S. Comptroller of the Currency, and the Federal Trade Commission.

In addition, Ms. Givens has participated on several task forces studying the privacy impacts of technology on society, including: the California Legislature's Joint Task Force on Personal Information and Privacy; the California Judicial Council's Subcommittee on Privacy and Access; the Internet Policy Committee of the San Diego Public Library; and the Mayor of San Diego's City of the Future Task Force.

Ms. Givens is author of *The Privacy Rights Handbook: How to Take Control of Your Personal Information* (Avon Books, 1997), and *Citizens' Utility Boards: Because Utilities Bear Watching* (1991). She is co-author of *Privacy Piracy: A Guide to Protecting Yourself from Identity Theft*, and *The California Channel: A New Public Affairs Television Channel for the State* (1989), a two-year study on the feasibility of a cable television network for State government. Ms. Givens is also co-author and editor of the PRC's 22 fact sheets.

Ms. Givens holds a master's degree in communications management from the Annenberg School for Communication, University of Southern California (1987). She has a background in library and information services, with experience in online research services and library network development (M.L.S.,

University of Denver, 1975).

### Chief Roger W. Ham

Chief Roger W. Ham is the first Chief Information Officer (CIO) of the Los Angeles (California) Police Department. He serves at the deputy chief level and commands five divisions: Emergency Command and Control Communications Systems, Communications, Information Resources, Crime Analysis Section, and Systems Development Task Force. Chief Ham manages a professional and operational staff of more than 900 people, 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 of the Information and Communications Services Bureau. Chief Ham directs and manages a technology budget of more than $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 on a synergistic approach through which all units under his command work together toward the LAPD's shared vision and goals.

Chief Ham has almost 30 years of experience in technological development. His career began at the Mobil Oil Corporation, where he worked as a project engineer managing command and control of field operations through automated systems.

Chief Ham also served as bureau commander, communications administrator, and information systems manager for the City of Huntington Beach, California, Police Department for more than 21 years.

Chief Ham holds an M.B.A. from the University of Southern California and a B.S. in Electrical Engineering from California State University, Long Beach. He has served on many professional and business organizations.

### Dr. Donald F. Harris

Dr. Donald F. Harris, President of HR Privacy Solutions, is an internationally recognized expert, industry leader, author, speaker, and conference producer on topics relating to privacy in the employment context. He has managed sensitive data and developed privacy policies for major private and public-sector organizations during a 25-year career in human resources, payroll, and labor relations.

Founder and Chair of the International Association for Human Resource Information's Privacy Committee, and Co-chair of the HR Data Consortium, Dr. Harris holds a Ph.D. in Philosophy from Columbia and an M.B.A. in Information Systems from New York University.

### Ronald P. Hawley

Mr. Ronald P. Hawley has been Chief Operating Officer of North Carolina's Office of Information Technology Services (ITS) since November 1999. Mr. Hawley came to ITS from the North Carolina State Bureau of Investigation (SBI), where he served as an Assistant Director. At ITS, Mr. Hawley leads a management team that provides for the IT needs of North Carolina's State and local governments. He is

responsible for the day-to-day operations of ITS' three major sections: Computing Services, State Telecommunications Services, and Business Technology Services.

Mr. Hawley began serving in July 1993 as Manager of SBI's Division of Criminal Information, which operates the State's law enforcement telecommunications network and its fingerprint-based central repository of criminal history record information. Shortly after this assignment, Gov. James B. Hunt Jr. appointed Mr. Hawley to co-chair the Criminal Justice Information Network (CJIN) Study Committee. In 1994, the committee recommended that North Carolina's criminal justice information be integrated. Since that time, many of the committee's recommendations, including the legislative establishment of a CJIN governing board, have been initiated. North Carolina Attorney General Michael F. Easley appointed Mr. Hawley as his department's CJIN representative. Mr. Hawley has also served as CJIN vice chair and, most recently, as chair. These responsibilities led to his membership as the CJIN representative to the Information Resource Management Commission. His participation has led to several committee appointments by Lt. Gov. Dennis Wicker, commission chairman.

Mr. Hawley's contributions to criminal justice information system efforts in North Carolina have been recognized throughout the Nation, resulting in his appointment to leadership positions in several national organizations working toward integration of criminal justice systems. He was a member of the FBI's Criminal Justice Information Services Advisory Policy Board and chaired its Security and Access Subcommittee.

In addition, Mr. Hawley served as Vice Chair of the SEARCH Membership Group and Board of Directors. His peers selected him as the 1998 recipient of the *Board of Directors' Award for Meritorious Service* in recognition of his contributions to SEARCH and to more effective management of criminal justice information.

The North Carolina Department of Justice, recognizing changes in information systems support mechanisms, began a study to determine a proper organizational structure for its IT specialists. As a result, several of the State's IT sections were merged into one organizational unit. Mr. Hawley was asked to direct the new unit, first as Acting Chief Information Officer and then as the State's Chief Operating Officer.

This new challenge is Mr. Hawley's first for a North Carolina agency other than the Department of Justice. He began his career as an SBI Special Agent in August 1973, only eight days after obtaining his graduate degree from the University of Maine. Mr. Hawley performed his undergraduate work at Campbell College (University). He held numerous assignments during his 26-year career, including Special Agent in Charge responsible for field investigations in two districts.

### Prof. Jane E. Kirtley

Ms. Jane E. Kirtley has been the Silha Professor of Media Ethics and Law

(endowed by former Minneapolis *Star and Tribune* publisher Otto Silha and his wife, Helen) at the University of Minnesota's School of Journalism and Mass Communication since August 1999. Ms. Kirtley joined the university's faculty after serving for 14 years as Executive Director of The Reporters Committee for Freedom of the Press in Arlington, Virginia.

Ms. Kirtley speaks frequently on First Amendment and freedom of information issues in the United States and abroad, including in the Czech Republic, Poland, Russia, Belarus, Latvia, Mongolia, Hong Kong, and Chile. Her column, "The Press and the Law," appears monthly in the *American Journalism Review*.

Before joining the Reporters Committee staff, Ms. Kirtley was an attorney for 5 years with the law firm of Nixon, Hargrave, Devans and Doyle in Rochester, New York, and in Washington, D.C. She is a member of the New York, District of Columbia, and Virginia bars. Ms. Kirtley also worked as a reporter for the Evansville, Indiana, *Press* and for the Oak Ridge *Oak Ridger* and Nashville *Banner* in Tennessee.

Ms. Kirtley's many awards and honors include induction into the Medill School of Journalism's Hall of Achievement in 1999 and the FOI Hall of Fame in 1996. In 1993, she received the *John Peter Zenger Award for Freedom of the Press and the People's Right to Know* from the University of Arizona.

Ms. Kirtley holds a J.D. from Vanderbilt University School of Law (1979). She holds a bachelor's and master's degree in Journalism from Northwestern University's Medill School of Journalism.

### Prof. Kent Markus

Prof. Kent Markus is a Visiting Professor at Capital University Law School in Columbus, Ohio, where he teaches Administrative Law, Remedies, and a seminar on the Role of the Prosecutor. Prof. Markus also serves as Director of Capital University'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 Deputy Chief of Staff at the U.S. DOJ and as the highest-ranking advisor to Attorney General Janet Reno. During his 5 years at DOJ, Prof. Markus was responsible at various times for: implementing nationally the *Brady Handgun Violence Prevention Act* and the *Violent Crime Control and Law Enforcement Act of 1994*; establishing and directing the Community Oriented Policing Services (COPS) Office; managing DOJ's congressional dealings; and serving as DOJ's point person on crime policy in general, with special attention to juvenile crime, gun violence, and criminal record systems.

Prior to his DOJ service, Prof. Markus was Chief of Staff for the Democratic National Committee. Previously, he served as Chief of Staff for former Ohio Attorney General Lee Fisher. Prof. Markus, a Cleveland, Ohio, native, worked earlier in his career at law firms in Australia,

Alaska, and Washington, D.C., before heading 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 Tip O'Neill, and for former House Rules Committee Chairman Richard Bolling.

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 in 1983 to the Massachusetts Trial Court. He headed one of the Nation's frontline urban district courts, which handled the most gun, drug, and domestic violence cases in the State. Judge Martin 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 on the Massachusetts Commission Against Discrimination before organizing the firm in which he was a partner until becoming a judge.

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

Judge Martin co-authored *Civil Rights Litigation: Cases and Perspectives* (Carolina Press 1995). He has written law review articles on a wide range of topics. Judge Martin's articles on juvenile justice have appeared 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.

### Iris Morgan

Ms. Iris Morgan is a Senior Management Analyst II for the Criminal Justice Information Services (CJIS) Program Area located within the Florida Department of Law Enforcement (FDLE). She currently coordinates the delivery of information services statewide, supervises the CJIS Help Desk, and is 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 Center (NCIC) audits of criminal justice agencies accessing FCIC and NCIC.

Ms. Morgan has two decades of 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, the National Fingerprint File Program, the Uniform Crime Reports Program, and the Criminal Justice Data Element Dictionary, as well as redesign of the Computerized Criminal History file.

### Lawrence F. Potts

Mr. Lawrence F. Potts is Director of the Boy Scouts of America's (BSA) Administrative Group, where he manages 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. He has also served as the Scout's Treasury Division director. Prior to joining the National Council, he had extensive experience in the casualty insurance industry, holding positions of Controller and Treasurer and serving on several boards of directors. He also served with the U.S. Armed Forces, attaining the rank of Captain.

Mr. Potts was an original member of the BSA Youth Protection Task Force, where he was instrumental in creating several tools for the prevention of child abuse in society and in scouting.

He was also an original member of the National Collaboration for Youth Sexual Abuse Task Force, an association of 16 not-for-profit youth-serving organizations seeking to prevent child sexual abuse. The task force pioneered efforts in educating and sharing information about sexual abuse among youth-serving agencies. Mr. Potts is the author of a paper on a model program's efforts to prevent child abuse.

Through BSA, Mr. Potts can communicate with more than 4.4 million youths and 1.1 million adults of mixed ethnic and racial backgrounds, and many others throughout society. Currently, he chairs the BSA Youth Protection Task Force, the Child Abuse Expert Advisory Panel, and the National Collaboration for Youth Sexual Abuse Task Force, and is a member of the National Child Abuse Coalition. He was a member of the U.S. Advisory Board on Child Abuse and Neglect from 1992-96.

As a Certified Public Accountant, Mr. Potts is a member of the American Institute of Certified Public Accountants and the Texas Institute. 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 at Austin, and is a member of Beta Alpha Psi and Phi Kappa Phi organizations.

### Stuart K. Pratt

Mr. Stuart K. Pratt is Vice President, Government Relations, for Associated Credit Bureaus Inc., an international trade association representing approximately 800 credit bureaus, 600 collection agencies, and 112 mortgage credit-reporting companies

across North America and Internationally.

Mr. Pratt is responsible for monitoring Federal and State legislative issues, managing industry lobbyists, and coordinating the industry's lobbying efforts when issues of concern arise on Capitol Hill or in a given State. In addition, he acts as a liaison between the credit-reporting industry and allied industries on Federal and State legislative issues. He also monitors trends in State legislation for long-range planning purposes, and has developed and implemented an ongoing State-level grassroots campaign.

The Greater Washington Society of Association Executives and the American Bankruptcy Institute are among Mr. Pratt's industry-related activities. He holds a bachelor's degree from Furman University in Greenville, South Carolina, and is currently pursuing his M.BA. at the University of Maryland.

### Jack Scheidegger

Since 1996, Mr. Jack Scheidegger has been Chief Executive Officer of Western Identification Network Inc., a coalition of western states that electronically share fingerprints and criminal history record information. Prior to his appointment, Mr. Scheidegger was Chief of the Bureau of Criminal Identification and Information for the California Department of Justice.

He previously served the department as Chief of its Bureau of Forensic Services, and as Director of its Bureau of Medi-Cal Fraud and Patient Abuse. Mr. Scheidegger also served as legislative advocate for the California Attorney General's Office.

Mr. Scheidegger has been a member of the SEARCH Board of Directors, Chair of SEARCH's Law and Policy Program Advisory Committee, and Chair of the Bureau of Justice Statistics/SEARCH National Task Force on Increasing the Utility of the Criminal History Record. He has also been a member of the California Peace Officers Association, the American Society of Crime Laboratory Directors, and the National Crime Information Center/FBI Western Regional Working Group (Control Terminal Officer).

Mr. Scheidegger holds a bachelor's degree in Public Administration from California State University, Sacramento, and a master's degree in Public Administration from the University of Southern California.

### Peter P. Swire

Mr. Peter P. Swire was the Clinton Administration's first Chief Privacy Counselor at the time of this conference, advising the White House on policies governing the use of personal information in government and industry. Mr. Swire, a privacy law specialist and law professor at Ohio State University (OSU), has written extensively on privacy issues and other matters of law. He was co-author of the book, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, which was published by Brookings Institution Press in 1998. Mr. Swire's research focus at OSU is on privacy, cyberbanking, and electronic commerce.

Mr. Swire also advises the U.S. Department of Commerce on issues relating to data flow between the European Union and the United States. He served as editor of the American Association of Law Schools' Section on Defamation and Privacy newsletter, and currently sits on *Electronic Banking Law and Commerce Report's* Editorial Advisory Board.

Previously, Mr. Swire served as Associate Professor at the University of Virginia School of Law, as an Associate at Powell, Goldstein, Frazer & Murphy in Washington, D.C., and as a judicial clerk to the Honorable Ralph K. Winter Jr., United States Court of Appeals for the Second Circuit.

Mr. Swire holds an A.B. from Princeton University and a J.D. from Yale Law School. He also studied at the Universite Libre de Bruxelles, Belgium, under a Rotary International Fellowship.

### 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 has written or edited 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 fields such 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 has also consulted on privacy for more than 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 has spoken at more than 500 national and international business and government meetings on privacy issues since the early 1960s, and appeared on all major U.S. television networks to discuss current privacy developments in business or government.

Between 1978 and 1998, he was 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 has

also worked with Opinion Research Corporation on a dozen proprietary privacy surveys for companies and industry associations.

In 1993, with SEARCH General Counsel Robert R. Belair, he founded the national newsletter and information service, *Privacy & American Business (P&AB),* to provide expert analysis and a balanced voice on business-privacy issues. *P&AB* conducts an annual national conference in Washington, D.C., on "Managing the Privacy Revolution," attended by 250 representatives of business, government, academic, and public interest groups. *P&AB* also conducts a Corporate Privacy Leadership Program and a Global Business Privacy Policies Project.

Dr. Westin holds a bachelor's degree from the University of Florida, an L.L.B. from Harvard Law School and a 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 N. Woulds

Dr. John Woulds is Director of Operations at the Office of the Data Protection Commissioner, the supervisory authority established in the United Kingdom under the 1998 *Data Protection Act*.

Dr. Woulds has been in the Office of the Data Protection Commissioner (previously the Data Protection Registrar) since March 1985. As director of operations, he is a member of the Commissioner's Management Board and is responsible for all operational aspects of the work of the Commissioner's Office. This includes notification, assessments casework, investigations, compliance casework, and policy advisory work in all sectors. Dr. Woulds also has management responsibility for the commissioner's role in freedom of information.

Prior to his appointment with the Data Protection Commissioner, Dr. Woulds 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.

Dr. Woulds is a Magistrate and a Fellow of the Royal Society of Arts.