1997

Electronic fingerprinting advances and issues

Carine F. Richards
San Jose State University

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_theses

Recommended Citation

Richards, Carine F., "Electronic fingerprinting advances and issues" (1997). *Master's Theses*. 1525.
DOI: <https://doi.org/10.31979/etd.u35x-5qf2>
https://scholarworks.sjsu.edu/etd_theses/1525

This Thesis is brought to you for free and open access by the Master's Theses and Graduate Research at SJSU ScholarWorks. It has been accepted for inclusion in Master's Theses by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

**ELECTRONIC FINGERPRINTING
ADVANCES AND ISSUES**

A Thesis

Presented to

**The Faculty of the School of Library
and Information Science
San Jose State University**

**In Partial Fulfillment
of the Requirements for the Degree
Master of Library Science**

by

Carine F. Richards

August 1997

UMI Number: 1386226

**Copyright 1997 by
Richards, Carine F.**

All rights reserved.

**UMI Microform 1386226
Copyright 1997, by UMI Company. All rights reserved.**

**This microform edition is protected against unauthorized
copying under Title 17, United States Code.**

UMI
**300 North Zeeb Road
Ann Arbor, MI 48103**

© 1997

Carine F. Richards

ALL RIGHTS RESERVED

APPROVED FOR THE SCHOOL OF
LIBRARY & INFORMATION SCIENCE

Dr. James Schmidt

James Schmidt

Dr. Ruth Hafter

Ruth Hafter

Dr. Linda Main

Linda Main

APPROVED FOR THE UNIVERSITY

M. Lou Livandorski

ABSTRACT

ELECTRONIC FINGERPRINTING ADVANCES AND ISSUES

by Carine F. Richards

This study investigates the general history of fingerprinting; the manual and automated processing of fingerprints; the evolution of electronic fingerprinting within law enforcement; and the expansion of the technology from law enforcement to other government agencies and to the private sector. Finally, the study discusses some issues generated by the use of Automated Fingerprint Identification Systems (AFIS) technology in the criminal justice setting and in welfare administration.

In the field of law enforcement, besides enhancing the processing of latent prints, AFIS technology makes it possible to exchange online fingerprint images and other pieces of criminal information, to increase the number of searches and identifications, to tie up criminal justice record systems, etc. However, AFIS systems are not foolproof systems. They reinforce privacy concerns by increasing the risk of unauthorized access and use of police computerized data.

When applied as a fraud deterrent in social services, their acceptance is not universal.

ACKNOWLEDGEMENTS

My deepest gratitude goes to the many people whose assistance made the realization of this work possible.

First, I am very grateful for the useful comments and the patience of the members of the thesis committee, Drs. James Schmidt, Ruth Hafter and Linda Main.

Sergeant Bruce Raye and Sergeant Aubrey Parrot (ret.), both from San Jose Police Department, Dr. Stephen K. Kwan, Professor in the College of Business of San Jose State University, Ms. Bobbi J. Cotter at the Office of Public and Congressional Affairs (FBI), and Mr. Bill Ledeen, Product Manager at Identix, provided invaluable information about manual and electronic fingerprinting methods in law enforcement.

A special word of thanks is due to Mr. Joseph L. Peterson, Professor of Criminal Justice at the University of Illinois at Chicago, for sharing the results of a survey he directed on automated fingerprint identification systems in 1995.

I would also like to express my gratitude to several organizations which sent me documentation about a child crime prevention program -- the Kids Identification Digital System (KIDS) project. They are the Applied Network Solutions, Inc.; Eastman Kodak Company; the Temecula Police Department; and the Temecula Valley School District. I hope their initiative will be very successful.

I wish to thank the Los Angeles County Department of Public Social Services and the Department of Social Services (Fraud Bureau) in Sacramento for information regarding the implementation of the Automated Fingerprint Image Reporting and Match (AFIRM) system in use in their welfare administration. Thanks as well to the FBI for the IAFIS Brochure they provided.

The following corporations sent me information about their products: Digital Biometrics, Inc.; Franklin Service Systems; Identicator, Corporation; Identix Incorporated; Infotec Development, Inc.; NEC Technologies, Inc.; Printrak International, Inc.; and TRW Systems Integration Group.

I owe warm thanks to the library staff of San Jose State University, especially the staff at the Government Publications Department and at the Reference Desk, for providing supportive services as well as constant encouragement throughout the

preparation of this thesis. The library staff of West Valley College in Saratoga was very helpful as well.

Thanks to Mr. Pascal Sletter of the European Commission for a very interesting interview about the ongoing efforts of the European Union to implement EURODAC, a central computerized system for the collection, exchange and comparison of fingerprints of applicants for asylum.

Finally, I dedicate this thesis to my family and friends whose infinite demonstrations of love, affection, and support were a constant source of strength and inspiration during this academic marathon.

LIST OF ABBREVIATIONS

AB	Assembly Bill
ACLU	American Civil Liberties Union
AFDC	Aid to Families with Dependent Children
AFIS	Automated Fingerprint Identification System
AFR	Automated Fingerprint Readers
AIS	Automatic Identification System
ALSM	Automated Latent System Model
ANSI	American National Standards Institute
ANSI	Applied Network Solutions, Inc.
ATF	Bureau of Alcohol, Tobacco, and Firearms
CAL-ID	California Automated Identification System
CCR	Computerized Criminal History
CFR	Code of Federal Regulations
CJIS	Criminal Justice Information Services
CLETS	California Law Enforcement Telecommunications System
CONFIRM	Countywide Networked Fingerprint Identification and Remote Match
CTA	Control Terminal Agency
CTO	Control Terminal Officer
DMV	Department of Motor Vehicles
DOJ	Department of Justice
EFT	Electronic Fund Transfer
FERPA	Family Educational Rights and Privacy Act

FBI	Federal Bureau of Investigation
GPO	Government Printing Office
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
III	Interstate Identification Index
IJIS	Integrated Justice Information System
Ident	Identification Division of the FBI
INLETS	International Law Enforcement Telecommunications System
INS	Immigration and Naturalization Service
IRS	Internal Revenue Service
ITN	Identification Tasking and Network Project
KIDS	Kids Identification Digital System
LAPD	Los Angeles Police Department
NAACP	National Association for the Advancement of Colored People
NBS	National Bureau of Standards
NCIC	National Crime Information Center
NCJRS	National Criminal Justice Reference Service
NEC	Nippon Electronic Corporation
NFF	National Fingerprint File
NISMART	National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children
NLETS	National Law Enforcement Telecommunications System
NOVARIS	Northern Virginia Regional Identification System
ORI	Originating Agency Identifier
OTA	Office of Technology Assessment

UCR	Uniform Crime Reporting Statistics
USC	United States Code
WIN	Western Identification Network

CONTENTS

ACKNOWLEDGEMENTS	v
------------------------	---

LIST OF ABBREVIATIONS	vii
-----------------------------	-----

Chapter

1. INTRODUCTION	1
-----------------------	---

Purposes and Interest of the Study

General Approach

Limitations of the Study

PART ONE

MANUAL FINGERPRINT SYSTEMS OF IDENTIFICATION

2. HISTORICAL EVOLUTION OF MANUAL FINGERPRINTING	12
--	----

General History

Early Developments of Manual Fingerprinting in the United States

3. GENERAL USES OF FINGERPRINTS	27
---------------------------------------	----

Uses of Fingerprints in the Fight Against Crimes

Uses of Fingerprints in Noncriminal Situations

4. ISSUES LINKED TO THE FINGERPRINTING METHOD	31
---	----

Being Fingerprinted

Misuses of Fingerprints

Drawbacks of the Manual Fingerprint Method in Police Work

PART TWO

ELECTRONIC FINGERPRINTING: ADVANCES

5. BRIEF HISTORY OF AFIS TECHNOLOGY WITHIN THE FBI	45
--	----

The Identification Division of the FBI

Forthcoming Programs

The Integrated Automated Fingerprint System

The NCIC 2000

General Presentation of the NCIC

The Files of the NCIC

The NCIC 2000

6. THE EXPANSION OF AFIS TECHNOLOGY OUTSIDE LAW
ENFORCEMENT 58

Applications of AFIS by Agencies of the Government

Applications of AFIS Technology in the Private Sector

7. ADVANTAGES OF AFIS OVER MANUAL SYSTEMS OF IDENTIFICATION
IN LAW ENFORCEMENT. 68

Size of Fingerprint Collections and Processing Time

Automated Processing of Fingerprints

Live-Scan Technology

Automated Data Extraction, Storage, Retrieval and Comparison

Enhancement of the Prints

Printing of Fingerprint Images

Electronic Transmission of Fingerprint Images and Database

Networking

Identification

PART THREE

ELECTRONIC FINGERPRINTING : SELECTED ISSUES

8. FINGERPRINTS AND CRIMINAL RECORDS 84

Criminal Records Used Within the Criminal Justice System

Criminal Records Used for Noncriminal Justice Purposes

Selected Issues

Mistaken Identities

The Quality of Criminal Records

Privacy Violations and Criminal History Records

9. THE USE OF AFIS TECHNOLOGY IN THE WELFARE SYSTEM 113

General

Issues

10. SUMMARY AND GENERAL CONCLUSIONS.	128
BIBLIOGRAPHY	135

CHAPTER 1

INTRODUCTION

This is a study of the origin, advances, and diffusion of automated fingerprint identification system (AFIS) technology in the United States. It is also an attempt at understanding the influence of a technology on the social structures where it is implemented. The study also looks into the effects upon individuals who are requested to submit to the electronic fingerprinting method.

AFIS technology is part of the phenomenal achievements in information technology which mark the last quarter of the twentieth century. These developments have a striking impact on the dynamic of society, not only by transcending time and space, but also by affecting the way people think, work and relate to the world.

Automation has invaded many spheres of modern life. For example, many elements of people's personal lives, such as their medical, financial, and professional records, are already stored in government and private databases. Electronic forms of control have been further enhanced by biometric technology and the apparition of complex automated identification systems. Specific physiological features gathered from the human body and considered, with a very high degree of statistical probability, to be unique to any given individual, are digitized, fed into computer systems, and compared with existing data in the computer memory. These features are as diverse as the structure of the DNA, the characteristics of the retina, the voice, the fingerprints, the shape of a hand, etc.

Automated identification systems are the contemporary answer to the need felt throughout the centuries to establish unambiguously the identity of individuals. Historical archives reveal some barbarian practices implemented to reach that end. For instance, during the Middle Age until the French Revolution, representatives of the public order in France lacked means of positively recognizing criminals. However, by marks on their shoulders, criminals could immediately be identified as recidivists. Re-established by Napoleon 1st, the "brand" definitely disappeared from France with the law of August 31, 1832. New identification methods came along in the nineteenth century and they enabled better distinguishing one person from the other. Among them, police started to photograph criminals and to record elements of their physical

appearance such as the size, the weight, and the measurements of their bony structure.

The real turning point in the use of scientific identification methods, however, occurred at the start of the twentieth century, when police of different countries singled out fingerprinting as the most reliable identification technique at their disposal.

Three characteristics of fingerprints explain the success of the method: their individuality, permanence, and their ability to be classified.

First, fingerprint patterns are unique to each finger of a person and to any individual, including monozygotic twins. Sir Francis Galton, who studied fingerprints in the late nineteenth century, called this characteristic of fingerprints "the principle of individuality." He was the first person to calculate that the probability of two individuals having the same fingerprint patterns would be one in 64 billion. The FBI estimates that this probability is one in ten billion.¹ Other statistical studies have been conducted on samples of the population to determine the extent of the principle of individuality. Cowger summarizes their results by stating that "the mathematical and empirical (experiential) data are more than adequate to provide a very sound basis for the use of friction skin prints as a means of positive, certain identification."²

Second, unlike other physical characteristics of the body, the general patterns of fingerprints do not change during the postnatal life of an individual, except in size and in rare situations. This is Galton's principle of permanence.

If fingerprints are erased or damaged because of a wound, chemicals, surgery, or because of activities like typing or working with clay, the original patterns will eventually return on the fingers. There are cases where a severe injury results in a permanent scar which obliterates or distorts the ridges. "As long as the area involved is not too extensive or too deeply involved, usually enough regenerative tissue remains to develop enough new tissue to make the pattern discernible."³ Furthermore, the scar itself can be used in the identification process.

¹ Jim Mallory, "Fingerprint Reader to Provide Positive Identification," *Computer Periodicals* (8 February 1994).

² James F. Cowger, *Friction Ridge Skin: Comparison and Identification of Fingerprints* (New York: Elsevier, 1983), 2.

³ Nash, *Individual Identification and the Law Enforcement Officer* (Springfield, IL: Charles C. Thomas Publisher, 1988), 27.

Third, the general patterns of fingerprints can be classified and organized in categories that can be systematically searched by fingerprint specialists. The need for a functional system to organize fingerprint patterns had already been recognized by Sir Francis Galton a century ago, when he wrote that fingerprints must be "so classified or 'lexiconized' that when a set of them is submitted to an expert, it would be possible for him to tell, by reference to a suitable dictionary, or its equivalent, whether a similar set had already been registered."⁴

The recognition of the value of these characteristics contributed to the development of dactyloscopy, that is, the method of identification based on fingerprints, and to its wide acceptance around the world in criminal justice matters as well as in noncriminal justice settings.

Automation increased the success of dactyloscopy. It did so to such an extent that AFIS technology is now spreading fast not only within the entire criminal justice system, but also in other agencies of the government and in the private sector. Large-scale diffusion of the technology throughout society is on the verge of bringing social changes of considerable importance and is therefore giving rise to a number of issues and questions. The following are especially important:

(1) AFIS technology is said to contribute to a safer society and to a society where criminality is more adequately fought. In the process, AFIS results in the establishment of a multitude of fingerprint databases giving access to personal information on the basis of which important decisions are made by criminal justice officials, employers, etc. Because the quality of fingerprint records has often proved to be unsatisfactory, is AFIS technology a first-rate method giving access to substandard pieces of information that can harm record subjects in many instances? More generally, what impacts will the implementation of AFIS technology have on law enforcement?

(2) The acceptance of AFIS technology is not universal.

Its application as a fraud deterrent in the welfare system is an example of an environment where digitalization and electronic storage of fingerprint data raise a vast

⁴ Cited in Thomas J. Deakin, *Police Professionalism: The Renaissance of American Law Enforcement* (Springfield, Illinois: Charles C. Thomas Publisher, 1988), 64.

range of issues. Connected in the collective consciousness with the search and capture of criminals, electronic fingerprinting is felt by some as a humiliating procedure which stigmatizes a vulnerable portion of the population. So, what impacts will the implementation of AFIS technology have on the welfare administration?

These are two questions this study will explore.

Purposes and Interest of the Study

The general purposes of this study are: (1) to place AFIS technology in its historical context; (2) to explore the development of AFIS technology in its original law enforcement setting in the United States; (3) to describe the trends of its development outside law enforcement; (4) to describe the strengths, weaknesses, and the main issues prompted by the multidirectional expansion of the technology.

A first interest of the study lies in its historical nature.

Part of the larger movement of the automation of society, AFIS technology is an important chapter of contemporary history. Through an exploration of the past and the present of AFIS technology, this study attempts to identify coming trends that may influence directly or indirectly the daily life of each of us.

A second interest of the study is its social nature.

The essence of any scientific or technological achievement must lie in the desire of its designers and users to improve the well-being of each individual while enhancing the collective social lifestyle. However, it often occurs that, rightly or wrongly, the implementation of a new technology is welcomed with reluctance. The implementation of AFIS technology in specific settings is no exception to the rule. This thesis notes the divergence of opinion among social groups with conflicting expectations and interests in the electronic fingerprinting method.

Finally, this study is also of interest in library and information science.

From the perspective of a librarian, fingerprint records are but one type of information subject to the classic treatment of data, that is, fingerprints are collected, classified, stored, and they can be disseminated. As this process is increasingly automated, some of the issues faced are similar to the ones met by other types of electronic information.

Because of the potentially profound impacts of electronic information management on society, information specialists have a double responsibility. First,

they must notice the issues generated by the continuous development and spreading of the automated information technology; second, they must expose these issues to the interested audiences.

General Approach

Two perspectives were fundamental in our approach:

(1) The view that a comprehensive approach is the most appropriate way to assess the status of AFIS technology.

Although an approach based on partial and specific perception of a phenomenon may be a more common method in social research, we elected, in agreement with the perspective of some authors such as C. Wright Mills, to take a global approach to AFIS technology. For Mills, "More data can lead to a fuller appreciation of complex topics. A favoured procedure along these lines is called 'triangulation'. . . . The general idea being promoted with the triangulation metaphor is that the best way to develop knowledge of a subject is to study it from a number of points of views."⁵

(2) The view that the information pertaining to AFIS technology is scattered in a wide variety of sources and that it needs to be brought together in a single piece of work.

This bibliographical type of study is referred to by Singleton et al. as an "available data research" which they oppose to the research strategies relying on data collected from experiments, surveys or field research. However, while available data research applies analytical techniques such as content analysis to explore the data extracted from the published material,⁶ measurements could not be used in our study due to the too wide variety of data collected from disparate sources.

With these two points in mind, the five main steps in our study have been as follows:

(1) We divided the study into four main topics: the general history of fingerprinting; the manual processing of fingerprints; their automated processing; and the identification of some major issues generated by the technology

⁵ Stephan Ackroyd and John A. Hughes, *Data Collection in Context* (New York : Longman, 1992), 171.

⁶ Royce Singleton et al., *Approaches to Social Research* (New York : Oxford University Press, 1988), 356.

(2) We then identified the relevant literature related to each of these topics and mainly published in the United States.

(a) Indexes and abstracts to books and periodicals, the National Union Catalog, Dissertation Abstracts International, and the Monthly Catalog of the United States Government Publications were used as first bibliographical tools. Automated resources available on Dialog, Lexis-Nexis, and Internet gave access to current aspects of AFIS technology. The National Criminal Justice Reference Service (NCJRS) also provided us with current reports on AFIS technology. Finally, other sources of information included business and government directories, serials, national and local newspapers, as well as national news magazines and periodicals.

(b) We requested information by mail from two sources.

First, we contacted several companies that design and sell AFIS systems or AFIS related products, like scanners or matching equipment. The companies that sent us trade brochures and other data describing the use and the applications of their devices are Digital Biometrics, Inc.; Franklin Service Systems; Identicator, Corporation; Infotec Development, Inc.; Identix Incorporated; NEC Technologies, Inc.; Printrak International, Inc.; and TRW Systems Integration Group. This information has been mainly used in Part Two of the study.

Second, we contacted organizations that use AFIS technology in the pursuit of specific goals. The Los Angeles County Department of Public Social Service, the Department of Social Services (Fraud Bureau) in Sacramento as well as organizations involved with the KIDS project (the Applied Network Solutions, Inc.; Eastman Kodak Company; the Temecula Police Department; the Temecula Valley School District) gracefully sent us documentation about their programs.

(3) A few interviews were conducted.

Sergeant Aubrey Parrot (ret.) from San Jose Police Department answered questions about the manual fingerprinting. Sergeant Bruce Raye, working at the time of the meetings at the Central Identification Unit of San Jose Police Department, was interviewed about AFIS technology and law enforcement in general. Finally, Dr. Stephen K. Kwan, Professor at the College of Business of San Jose State University was interviewed about the ConFIRM project.

(4) From the data accumulated, we prepared an overview of AFIS technology and identified key concepts and issues arising from the use of the technology in two major areas: law enforcement and the welfare administration.

(5) The final step was to present the outcome of the study in a descriptive way intended to give a clear picture of the current situation of AFIS technology as well as some insights regarding its future in American society.

Limitations of the Study

This study has been restricted in three ways.

First, our initial concern was with the development of AFIS technology within the United States. Very little reference is therefore made to the considerable work done in the field of AFIS technology in other countries.

The second limitation relates to the general scope of the study. As far as we can determine, no study of the scope of ours had been carried out until 1995. Existing studies on AFIS technology pertain to the analysis of certain aspects of the technology, such as specific applications of the method. The most comprehensive of such studies are probably those conducted at the Department of Criminal Justice of the University of Illinois at Chicago. They have as foci the identification and description of the AFIS systems used nationwide and worldwide in police work.⁷

The scope of our study is more comprehensive. It is meant to provide a global overview of the origin, development and expansion of AFIS technology from law enforcement to other spheres of application in the United States. A difficulty, however, is that the development of a technology and the analysis of its impacts can be studied from many points of view. In addition, AFIS technology itself has roots in or is intimately related to several disciplines such as computer science, image technology, sociology, law, economics, politics, telecommunications, etc. Each of them carries specific issues that could be the topic of specialized studies.

As a consequence, we have restricted the scope of our investigation by limiting the degree of detail in the analysis of the technology and by concentrating our

⁷ See David Klug, Joseph L. Peterson, and David A. Stoney. *Automated Fingerprint Identification Systems: Their Acquisition, Management, Performance, and Organizational Impact* (National Institute of Justice, 1992). See also Joseph L. Peterson, and Julie L. Moore, *The Status of AFIS Systems Worldwide: Issues of Organizations, Performance and Impact* (International Symposium on Fingerprint Detection, and Identification held in Ne' urim, Israel, June 1995).

attention on general issues inherent to the use of AFIS technology as well as to those aspects of the technology that directly affect individuals when they are requested to submit to electronic fingerprinting.

A third limitation relates to the bibliography. The scope of this study covers a large volume of bibliographical references from the late nineteenth century to the mid-1990s. The number of publications increased at the same rapid pace as the development of the technology. Therefore, the bibliography, although relevant, cannot be exhaustive and some of the data presented may already be outdated. Unavailability of some official statistical data is also a factor which limits the appreciation of the actual performance of AFIS systems.

Organization of the Thesis

The thesis is organized as follows.

Part I outlines the use of fingerprints at the dawn of human history and their systematic exploration from Modern Times until the end of the nineteenth century. It also includes a description of the manual processing of fingerprints for identification purposes by American police throughout the twentieth century; an approach to the uses of fingerprints for criminal and noncriminal justice purposes; and an enumeration of major issues pertaining to the manual method of fingerprinting.

Part II examines the general evolution of AFIS technology in the United States. It first describes the early steps in the development of the technology within the FBI and its forthcoming projects in that field. It then outlines the diffusion of AFIS systems outside law enforcement, and lists the advantages of the automated identification method over the manual method of identification.

Part III discusses selected social issues generated by the use of AFIS technology in law enforcement and the welfare administration. It also contains a summary of the study and the major conclusions.

PART ONE

MANUAL FINGERPRINT

SYSTEMS

OF

IDENTIFICATION

INTRODUCTION

The fingerprinting method used by the police has two distinct functions. "The first is record keeping where a complete set of fingerprints of an individual is used to determine the true identity of that individual. The second is criminal matters to implicate an individual as possibly responsible for the criminal activity."⁸ These functions illustrate the difference between inked and latent fingerprints.

Inked fingerprints (which are also referred to as *rolled fingerprints*) are used to establish or to verify the identity of a person for criminal and noncriminal justice purposes, as well as to determine whether that person has a criminal record. They are produced in a uniform way across the country. A special fingerprint ink is applied on the first joint of each finger of a person and the joint is rolled on a standard fingerprint card called a tenprint card. The impression of the fingers held flat together is subsequently taken. These two sets of fingerprints on the tenprint card constitute the fingerprint record of the person. When "major criminal prints" are taken, all the ridges of the hands are recorded. This includes the print of the ridges located at the very tip of the fingers, of the joints between the fingers, and of the sides of the fingers.⁹

Latent fingerprints (which are sometimes referred to as *evidence prints*) are the fingerprints accidentally left by criminals at the scene of their crime or on pieces of evidence. They are made by the perspiration or the oil found on the friction ridges, or by fingers that have been soiled with blood, dirt, etc. These prints have been called "latent" because they are difficult or even impossible to see. Some authors differentiate the *plastic fingerprints*, which are visible impressions of fingerprint patterns in crime scenes that can be easily photographed. A large range of artificial means including the use of powders, chemicals, radioactive material, laser beams, and electronic techniques has been developed to make latent prints visible. Once visible, they are lifted on a tape or photographed to be classified and filed. Latent prints have different characteristics than inked prints. For example, as criminals try to hide all the traces of their presence at the crime scene, latent prints are likely to appear as partial sections

⁸ James F. Cowger, *Friction Ridge Skin: Comparison and Identification of Fingerprints* (New York: Elsevier, 1983), 6.

⁹ *Ibid.*, 22.

of a full fingerprint and their quality is usually mediocre. "Genuine latent marks from crime scenes are invariably of very poor quality: spatial distortions [i.e., the distortions that change the geometry of the print] are exaggerated, fingers are dirty, images are smudged, the information content is scant and fragile, other patterns may be super-imposed (or sub-imposed), images may overlap other fingerprint marks or smudges, and may have deteriorated through the effects of weather."¹⁰

Before the advent of automation,¹¹ the identification of a person was done by manual comparison of latent fingerprints to the inked prints of known suspects, in the hope of having the fingerprints found at a crime scene "easily and quickly identified with any recorded print of the same finger."¹² If police had no suspect, they could still compare the incoming print to the ones held in their collection. However, as every new print could not possibly be compared with the multitude already on record, classification systems based on global characteristics of the patterns of fingerprints were created. Prints belonging to the same classification category were filed together and the incoming print was only compared to the ones of the same category. The identification process that followed was based "on the individual ridge characteristics found within the ridge structure" and was determined by the comparison of "the ridge characteristics and their position in relation to each other."¹³ If the comparison did not lead to any identification, the evidence print was stored in an unsolved latent file. On the other hand, when fingerprint specialists found a print with similar characteristics than the new one, they had the duty to prove the match.

No formal standard exists about the number of similar characteristics required to prove the match. It is determined individually by different courts or agencies.

¹⁰ Malcom K. Sparrow, "Measuring AFIS Matcher Accuracy," *The Police Chief* (April 1994): 148.

¹¹ Automation has not yet supplanted the traditional manual fingerprinting method of identification. However, in order to facilitate the reading of this paper, the texts pertaining to the manual method will be written mainly in the past tense.

¹² Harry Battley, *Single Finger Prints: A New and Practical Method of Classifying and Filing Single Finger Prints and Fragmentary Impressions* (New Haven: Yale University Press, 1948), 7.

¹³ Wendell W. Clements, *The Study of Latent Fingerprints: A Science* (Springfield, IL: Charles C. Thomas, Publisher, 1987), 48.

Already in 1941, Chapel wrote that courts had frequently accepted an identification based on less than 12 identical points and that most courts found 12 to 15 identical points to be enough.¹⁴

Although closely linked, classification and identification can be independent from each other. On the one hand, it is possible to identify fingerprints which cannot be classified. Clements supports this statement by noting that “an extensive scar may be present in the central area of the finger, destroying the pattern so that it cannot be classified with any degree of accuracy. But the ridge structure surrounding the damaged or destroyed area will contain a sufficient number of ridge characteristics to make a positive identification.”¹⁵ On the other hand, the author observes that a large number of people belong to the same general fingerprint classification category and can still be identified.

Organization of Part One

Chapter 2 provides a historical overview of the evolution of the manual method of fingerprinting. The first section outlines the steps which eventually led scientists to become aware of the value of fingerprints and to elaborate systems for their functional use. The second section focuses on the diffusion of the method in the United States.

Chapter 3 describes multiple uses of the fingerprinting method, both in criminal and noncriminal justice environments.

Chapter 4 outlines various issues generated by the fingerprinting method. Four specific issues are successively presented. The first section shows that the context in which the method is applied has an impact on its social acceptance or its rejection. The second and third sections illustrate cases of misuses and controversial uses of the method. The last section concentrates on drawbacks inherent to the manual method of fingerprinting.

¹⁴ Charles Edward Chapel, *Fingerprinting: A Manual of Identification* (New York: Coward McCann, Inc., 1941), 86.

¹⁵ Clements, *The Study of Latent Fingerprints: A Science*, 20.

CHAPTER 2

HISTORICAL EVOLUTION OF MANUAL FINGERPRINTING

General History

Reproductions of fingerprint patterns on a few prehistoric pieces of art from various places of the planet are the testimony to the early awareness some men experienced for the drawings imprinted on their fingertips. For example, researchers have found fingerprints from the eighth century B.C. on the walls of the city of Paphos in Cyprus. Neolithic ornaments and megaliths in Western Europe were decorated with such impressions.

Ancient civilizations were using fingerprints in some of their official dealings. For instance, they were used in China around 200 B.C. as a sign of the authenticity of official documents. Kuhne reports that "The Chinese employed the finger print system for the signing of contracts on the part of illiterate persons. In founding asylums every infant on its reception was recorded for possible identification, the design of its finger tips being the most important part of the record."¹⁶ During one of his expeditions in Central Asia, the Hungarian-British archaeologist and geographer Sir Aurel Stein (1862-1943) discovered Chinese loan contracts dated 782 A.D. in a sand-buried city of Turkestan. The sentence at the end of the contract is translated in the following way: "The two parties have found this just and clear and have affixed the impressions of their fingers distinctive mark."¹⁷ Fingerprints were also used in other parts of the world, like in Babylon for business transactions. A last example of the early uses of fingerprints dates back to the fourteenth century in Persia where "official government documents were impressed with fingerprints, and a government official observed that the fingerprints of no two persons were alike."¹⁸

¹⁶ Frederick Kuhne, *The Fingerprint Instructor* (New York: Munn and Co., Inc., 1935), IX.

¹⁷ Chapel, *Fingerprinting: A Manual of Identification*, 5.

¹⁸ Fletcher D. Thompson, "Golden Anniversary of FBI Identification Division," *FBI Law Enforcement Bulletin* (July 1974): 5.

The scientific study of fingerprints began in the second half of the seventeenth century¹⁹ with the work of three pioneers. Dr. Nehemiah Grew from London made in 1684 the first academic reference to fingerprints; Professor Marcello Malpighi from the University of Bologna made in 1686 the first scientific observation of fingerprints with a microscope; and Professor of Physiology John Evangelist Purkinje (1787-1869) from Czechoslovakia described nine standard types of fingerprint patterns in his medical thesis submitted in 1823 at the University of Breslau.

Outside the academic arena, the first person to use fingerprints in a practical way was Sir William James Herschel (1833-1917), a commissioner for the English government in Bengal who later became magistrate for the East Indian Company. Beginning in 1858, he required Indian merchants to imprint their fingerprints on official documents. He also used fingerprinting "as a method of checking the identities of Indian workers who all looked alike to him and who had been cheating the government by sending relatives and friends to collect salaries repeatedly in the same name. Herschel first collected all the fingerprints of the workers; when they arrived to receive their pay, they had to 'sign' for this money by pressing inked fingers to receipts."²⁰ Being the initiator of the system of fingerprinting for purposes of civil identification,²¹ he is credited "for giving fingerprints their first actual tryout in establishing individuality."²²

Years later, while looking at prehistoric pieces of pottery in Japan, Dr. Henry Faulds (1843-1930) saw ancient marks of fingers imprinted in the clay. The criminologist became interested in fingerprints and began to compare the fingerprint patterns of Japanese to the ones of English people. He described his comparative method the following way:

¹⁹ A more detailed overview of the milestones in fingerprinting is provided in: Ministry of the Solicitor General, Royal Canadian Mounted Police, *International Illustrated Vocabulary of English-French Fingerprint Technology with a Short Index in Six Languages*. 3d ed. (revised and enlarged), Jean L. F. Lambert, comp., Fingerprinting Centennial Edition 1891-1991, (Ottawa, Canada: Canada Communication Group-Publishing, 1991), XV-XVIII.

²⁰ Jay Robert Nash, *Encyclopedia of World Crime: Criminal Justice, Criminology, and Law Enforcement* (Wilmette, IL: CrimeBook, Inc., 1989), vol. II, 1526.

²¹ *Dictionary of Scientific Biography*, 1972, vol. VI, 323; *Who Was Who 1916-1928*, 491.

²² Kuhne, *The Fingerprint Instructor*, XI.

A common slate or smooth board of any kind, or a sheet of tin, spread over very thinly and evenly with printer's ink, is all that is required. The parts of which impressions are desired are pressed down steadily and softly, and then are transferred to slightly damp paper. . . . By using different colors of ink useful comparisons could be made of two patterns by superposition.²³

A controversy arose between Sir William Herschel and Dr. Henry Faulds regarding who was to be credited for the use of fingerprints in the field of criminal identification. In his article *On the Skin Furrows of the Hand* published in the October 28, 1880 issue of the British journal *Nature*, Faulds wrote that, when bloody fingerprints are left at the scene of a crime, "they may lead to the scientific identification of criminals." He further added that "there can be no doubt as to the advantage of having, besides their photographs, a nature-copy of the for-ever-unchangeable finger-furrows of important criminals." Sir William Herschel published an answer to Faulds in the November 25, 1880 issue of the same journal, claiming that he had been using fingerprints for twenty years in India before the publication of Faulds' article. He described the ways he used fingerprints in India for pensioners, registration offices and in jail. "On commitment to jail each prisoner had to sign with his finger. Any official visitor to the jail after that could instantly satisfy himself of the identity of the man whom the jailer produced by requiring him to make a signature on the spot and comparing it with that which the books showed."²⁴ The outcome of the controversy between the two men was that Herschel was credited for making the first practical and official use of fingerprinting, while Faulds was credited for writing the first article on the practical use of fingerprint to identify criminals.

It should be pointed out that both men seemed to have found difficulties in convincing authorities on some of their respective visions. Between 1886 and 1888, Dr. Henry Faulds tried unsuccessfully to convince Scotland Yard of the value of fingerprints for criminal identification purposes. But the British police at that time were totally devoted to the use of an anthropometric system of identification, the Bertillon system, and ignored Faulds' idea.²⁵ As for Herschel, in 1877 he proposed to the

²³ Henry Faulds, "On the Skin-furrows of the Hand," *Nature* (28 October 1880): 605.

²⁴ William James Herschel, "Skin Furrows of the Hand," *Nature* (25 November 1880): 76.

²⁵ Nash, *Encyclopedia of World Crime*, vol. II, 1138.

Inspector General of prisons of India the use of fingerprints as a way to identify prisoners, alleging that they would be “far more infallible than photography.”²⁶ The Inspector General, however, rejected the idea and Herschel did not carry it on.

In 1891, a cousin of Charles Darwin, the British scientist Sir Francis Galton (1822-1911) published a 23-page article in the British periodical *Philosophical Transactions* entitled *The Patterns in Thumb, and Finger Marks. On their Arrangement into Naturally Distinct Classes, the Permanence of the Papillary Ridges, that Mark Them, and the Resemblance of their Classes to Ordinary Genera*. This article was followed one year later by *Finger Prints*, the first book where fingerprints are proposed as a means of identification and where the scientist “considered virtually every aspect of friction skin including history, morphology, inheritance, individuality, permanence, methods of printings and potential usefulness.”²⁷

In this book, considered by Nash as the first scientific treatise on fingerprints and which ultimately led to the adoption of dactyloscopy by Scotland Yard, Galton did not just “considered” the permanence of ridge patterns, but, through a longitudinal study of six people, he proved its existence. The British anthropologist fingerprinted these individuals at two occasions, with an interval between prints going from nine to thirty-one years. These intervals covered the following periods of time: from childhood to boyhood, from boyhood to early manhood, from manhood to the age of sixty, and from age sixty-seven to the age of eighty. “He found a total of 388 points of agreement out of 389 points that were studied and mentioned having looked for more than 700 points of comparison with only one exception. The exception was of a ridge that had been split in a child but that had closed up a few years later.”²⁸

Sir Francis Galton created the first scientific system of classifying fingerprint patterns. His contribution to dactyloscopy is summarized by Cummins the following way:

²⁶ Cited by John Edgar Hoover, “The Role of Identification in Law Enforcement: An Historical Adventure,” (Part One), *FBI Law Enforcement Bulletin*, (March 1973): 11.

²⁷ Cowger, *Friction Ridge Skin: Comparison and Identification of Fingerprints*, 5.

²⁸ Nash, *Individual Identification and the Law Enforcement Officer*, 26.

He brought together and strengthened the evidence essential to the validation of fingerprints as means of personal identification, though none of the concepts was original with him; permanence of the fingerprint characteristics; uniqueness of an assemblage of ridge details; variability and classifiability of finger patterns. Furthermore, he reported on fundamental investigations; biological variations as manifested in fingerprints; inheritance of fingerprint traits; variation among racial and constitutional groups. . . . The book is a classic, an outstanding landmark in the progress of fingerprint science.²⁹

Another leading name in the history of the fingerprinting method was the Argentinean police officer Juan Vucetich (1858-1925). Born in the Dalmatian island of Lessina, he emigrated to Argentina in 1884 where he joined the police and became in 1889 Chief of the Anthropometric Bureau of Identification of Buenos Aires. In 1891, he created his own fingerprint classification system based on that of Sir Francis Galton and described it in his book *Dactiloscopia Comparada* ("Comparative Fingerprinting"). Adopted by almost all of the Spanish-speaking countries, it is considered to be the first practical classification system of fingerprints for law enforcement purposes.³⁰ Vucetich became in 1892 "the first expert to secure a conviction upon fingerprint as the sole clue."³¹ In La Plata, Argentina, Francesca Rojas accused a neighbor of killing her two sons. However, as the fingerprints found at the scene of the crime were hers, she was convicted for the murders.

The person whose work on the fingerprinting method was most spread in the English-speaking nations is Sir Edward Richard Henry (1850-1931). The system he created is the basis of the fingerprint classification method used by the FBI. When Sir Henry was Inspector-General of the police in Bengal, India, he developed his own fingerprint classification system, known as the Henry System, which he presented in his book *Classification and Uses of Fingerprints* published in 1900. Sir Henry split

²⁹ H. Cummins, cited by Donald J. Nash, *Individual Identification and the Law Enforcement Officer* (Springfield, IL: Charles C. Thomas Publisher, 1978), 23.

³⁰ Thomas J. Deakin, *Police Professionalism: The Renaissance of American Law Enforcement* (Springfield, IL: Charles C. Thomas Publisher, 1988), 64; Michael D. Lyman, *Criminal Investigation: The Art and the Science* (Englewood Cliffs, NJ: Regents/Prentice Hall, 1993), 131.

³¹ Henry T.F. Rhodes, *Alphonse Bertillon, Father of Scientific Detection* (New York: Abelard-Schuman, 1956), 149.

Galton's divisions into smaller ones, converted the fingerprint patterns into formulas mixing numbers and letters, and arranged them in an easily retrievable way.

A historical account of the development of manual fingerprinting would not be complete without a tribute to the work of the French criminologist Alphonse Bertillon (1853-1914). The anthropometric system of identification he conceived in 1880 was the most widespread method of criminal identification for about thirty years in Europe and in the United States. It competed for years with the Henry system before being given up. Before describing his system of identification based on "the application of the methods of anthropological anatomy to questions of judicial identification,"³² a special note should be made about Bertillon's contribution to the general development of law enforcement practice. "Among other things, Bertillon introduced the use of photography to preserve a crime scene; he developed a means for preserving footprints; and he advocated handwriting analysis as a crucial tool in investigation. These ideas were important steps in the development of police laboratories where the physical evidence of a crime could be subjected to scientific analysis."³³ Bertillon also devised the first scientific and "uniform standard of record-keeping for describing and identifying criminals."³⁴ His classification system was an answer to two problems in police identification work:

1. To put on file, in a set order, the particular characteristics of an individual, so that each time that individual is compared with his file the relation of the one to the other can be established.
2. To bring together the whole of the files thus established for all the subjects and classify them solely by means of their elements of identification, in order that it may be possible to find any one of them with the aid only of the elements taken from the person itself or the individual to be identified.³⁵

Bertillon's system of identification relies on three basic principles:

³² Alphonse Bertillon, *Signaletic Instructions: Including the Theory and Practice of Anthropometrical Identification* (New York: Werner Company, 1896), 1.

³³ David R. Johnson, in Terry W. Clinton, *Policing Society: An Occupational View* (New York: Wiley, 1985), 67.

³⁴ Bruce L. Berg, *Law Enforcement: An Introduction to Police in Society* (Boston: Allyn and Bacon, 1992), 284.

³⁵ Henri Souchon, in Philip John Stead, *Pioneers in Policing* (Montclair, New Jersey: Patterson Smith Publishing Corporation, 1977), 129.

(1) Some parts of the body do not change in size during the adult years.

(2) The measurement of body parts is easy to take.

(3) As Adolphe Quetelet, the famous Belgian statistician had already established in 1835, Bertillon knew that the dimensions of the parts of the body were unique to any individual. He determined that the probability of two people having the exact same anthropometric measurements was 286,435,456 to one.

The parts of the body measured in the Bertillon system were the following. First, there were measurements based on the entire body: the standing height, the outspread arm, and the sitting height. Second, there were measurements based on the length and width of the head, and the length and width of the right ear. Finally, there were measurements based on the length of the left foot, of the left middle finger, of the left little finger, and of the left forearm.³⁶ These measurements were converted into formulas, cataloged on Bertillon identification cards, and arranged according to this formula. Pictures of the criminals were also taken and were kept with the measurement cards and the records of previous convictions. The idea behind keeping the pictures with the measurement cards was "that no two people would have the same appearance and physical measurements."³⁷

A definite value of the Bertillon system was that a suspect could use an alias and still be recognized by the police due to his measurement card. Between 1880 and 1890, this system allowed the identification of 67,580 people by the police in Paris.³⁸

However, Bertillon's system was not perfect.

First, the structure of the bones does change with surgery, accidents, diseases, or afflictions like arthritis. Aging also affects the length of bony structures, modifying therefore the formula of a person and making his/her identification difficult or even impossible with the Bertillon cards. Consequently, the system was best suited for

³⁶ Bertillon, *Signaletic Instructions*, 15; Vivian Anderson Leonard, *The Police Records System* (Springfield, Illinois: Charles C. Thomas Publisher, 1970), 44.

³⁷ Don Whitehead, *The FBI Story: A Report to the People* (New York: Random House, 1956), 133.

³⁸ Souchon, in Philip John Stead, *Pioneers in Policing*, 139.

people between the ages of 20 and 65, when few changes could be observed in bony structures.³⁹

Another problem with Bertillonage was the considerable length of time required - about twenty minutes - to take the measurements of a person. This was not efficient in police departments where a lot of arrests were made.

A third problem was that errors in the measurements or in the recording of the measurements occurred. Two people could report different measures about one individual; or the same person taking the measurements of a particular individual on separate occasions could obtain different measures. The inaccuracy in measurements or in their recording compromised the identification of a person with the Bertillon cards.

A fourth problem was that the Bertillon system could not aid in determining the identity of a criminal who had not been in police custody previously.⁴⁰

These limitations made police officials more aware of the value of the fingerprinting method. Easier to use, faster, and more reliable than the anthropometric method, the records it produced also took less storage place than the Bertillon identification cards. Fingerprint identification systems therefore gradually replaced the Bertillonage method across the world, with Argentina leading the movement.⁴¹ In England, fingerprinting became the official police identification system in 1901 and Scotland Yard used it the same year. When the British police decided to reject the Bertillon system and to adopt the Henry system, "the results were quickly apparent, for the number of identifications which, under the anthropometric system had numbered 503 in 1901, quickly mounted up until at the end of 1902 they were 1,722 and in 1912 10,677."⁴²

To conclude, Deakin reports that Bertillon used the fingerprint method along with his own anthropometric system and, ironically, "in 1902, it fell to Bertillon to be the

³⁹ Chapel, *Fingerprinting: A Manual of Identification*, 18.

⁴⁰ Hoover, "The Role of Identification in Law Enforcement," (Part One), 10.

⁴¹ Nash, *Encyclopedia of World Crime*, 3322.

⁴² Obituary of Sir Henry in *The Times*, 21 February 1931, 7.

first to solve a murder case with fingerprints on the Continent, which led to the legend that Bertillon had discovered fingerprints!”⁴³

Early Developments of Manual Fingerprinting in the United States

The first authentic fingerprint pattern officially recorded in the United States is attributed to Gilbert Thompson of the U.S. Geological Survey when he used “his thumb impression to prevent the forgery of commissary orders during his supervision of a survey in New Mexico in 1882.”⁴⁴ That same year, Tabor, a San Franciscan photographer proposed to use the fingerprinting method “for the registration and identification of the large number of Chinese immigrants coming into our country.”⁴⁵

In 1883, Mark Twain published a few short stories in a book entitled *Life on the Mississippi*. In one of them, *A Thumb-Print and What Came Of It*, a murderer is identified by the bloody fingerprint he left on a document in the victim’s house. One can wonder in what way this story influenced the early development of fingerprinting in the United States. This unexpected and intriguing question is based on the fact that, when Twain published his book, “no thought of fingerprints as a means of human identification had been known to appear in American literature How much Twain’s story was based on acquired knowledge or upon a notion that may have persisted through the ages concerning the uniqueness of human fingerprints is vague.”⁴⁶ At any rate, it seems that, a few years later, Mark Twain received a copy of Galton’s 1892 treatise on fingerprints and that he based his detective novel *Pudd’nhead Wilson* on the findings of the English anthropologist.

⁴³ Deakin, *Police Professionalism*, 65.

⁴⁴ U.S. Department of Justice, Federal Bureau of Investigation, *Criminal Identification and the Functions of the Identification Division of the Federal Bureau of Investigation* (1 July 1937), by John Edgar Hoover, (np. 1937), 10.

⁴⁵ Nash, *Individual Identification and the Law Enforcement Officer*, 22.

⁴⁶ Hoover, “The Role of Identification in Law Enforcement: An Historical Adventure,” (Part One), 10-11.

In 1896, the International Association of Chiefs of Police (IACP) established the National Bureau of Criminal Identification in Chicago, Illinois with the purpose to compile and exchange criminal identification data among law enforcement agencies. Fingerprints started to be attached to criminal records around that time.

The first systematic use of fingerprints in the United States occurred in 1902 under the initiative of Dr. Henry Pelouze De Forest (1864-1948), "the American pioneer in the science of fingerprinting."⁴⁷ When he was appointed medical examiner in charge of the physical examination of the applicants for the civil service in New York City, De Forest realized that an athlete took the tests for a few candidates to the position. This impersonation clearly demonstrated the need to assess with absolute certainty the individual identity of the candidates. This led De Forest to compare the two rival systems co-existing then, that is, the Bertillon and the fingerprinting systems. He decided in favor of the second. "He installed the system in the examination of all civil service candidates, the first classified fingerprint record ever made officially in the United States being taken on Dec. 19, 1902. The subject, James Johnson, was a candidate for fireman, and in 1935, when Johnson's fingerprints were again taken and proved to be identical with the earlier record, the set became the record for the longest interval of dactylograms of an individual in the United States."⁴⁸

It has been mentioned earlier that the anthropometric system of identification was still used at the beginning of the twentieth century. However, besides the problems inherent in the method itself, an incident occurred which precipitated its fall. A Will West had been sentenced in 1903 to the Federal Penitentiary in Leavenworth, Kansas. By coincidence it happened that another prisoner also named Will West had been, since 1901, serving a life sentence in the same penitentiary.

The Bertillon measurements of both convicts were practically identical:⁴⁹

(1) Will West, the new inmate:

⁴⁷ John L. Sullivan, *Introduction to Police Science*, 3d ed (San Francisco: McGraw-Hill Book Company, 1977), 41.

⁴⁸ *National Cyclopedia of American Biography*, 1950, vol. 36, 41.

⁴⁹ Chapel, *Fingerprinting: A Manual of Identification*, 12; Rhodes, *Alphonse Bertillon, Father of Scientific Detection*, 155.

19.7, 15.8, 12.3, 28.2, 50.2, 1.78.5, 9.7, 91.3, 1.87.0, 6.6, 14.8.

(2) Will West, the inmate already in the penitentiary:

19.8, 15.9, 12.2, 27.5, 50.3, 1.77.5, 9.6, 91.3, 1.88.0, 6.6, 14.8.

Besides the remarkable similarity in their Bertillon measurements, both Will Wests looked very much alike. One feature, however, differentiated both men, their fingerprints.⁵⁰

Starting then, the fingerprinting method gradually replaced the Bertillonage. An area where fingerprinting immediately spread was the military. The Army began to fingerprint its personnel in 1905 and was followed by the Navy in 1907 and the Marine Corps in 1908.

The method also spread in the criminal justice system. Five examples illustrate this early development.

(1) In March 1903, New York State authorities decided to fingerprint their prisoners. On June 5, 1903, they officially adopted the fingerprint system in a few penitentiaries and "in 1913, fingerprinting was required by law for all inmates of the state prisons, reformatories and penitentiaries."⁵¹

(2) At the World's Fair in St. Louis, Missouri in 1904, Sergeant John K. Ferrier of Scotland Yard taught the Henry system of classification of fingerprints to St. Louis police officials who subsequently created the first police department fingerprint identification bureau in the United States.

(3) In 1904, "a sum of money 'not to exceed \$60' was appropriated by the Department of Justice . . . to establish a system of fingerprint identification in Leavenworth Prison."⁵² Leavenworth was "the first to offer facilities on more than a local basis when

⁵⁰ A study of official records of the two men seems to demonstrate that they were twin brothers. See Joe Nickell, "The Two 'Will Wests': A New Verdict," *Journal of Police Science and Administration* 8, no. 4 (1980).

⁵¹ Bill Heberton and Terry Thomas, *Criminal Records: State, Citizen and the Politics of Protection* (Brookfield, Vermont: Avebury, 1993), 27.

⁵² Eugene B. Block, *Fingerprinting: Magic Weapon Against Crime* (New York: David McKay Company, Inc., 1969), 25.

it gradually expanded the scope of its operations to include a free fingerprint exchange service among a growing list of contributing peace officers.”⁵³

(4) The California Bureau of Criminal Identification was established in 1905 in San Quentin prison “primarily to fingerprint inmates and to distribute copies of the fingerprints to police agencies for use in identifying inmates arrested after release from custody.”⁵⁴

(5) The first execution of a criminal whose conviction was solely based on the fingerprints found at a crime scene occurred in 1911 in Illinois. The criminal was Thomas Jennings.⁵⁵

The FBI officially adopted the fingerprinting method in 1908. On May 10, 1924, U.S. Attorney General Harlan Fiske Stone appointed John Edgar Hoover (1895-1972) as Director of the bureau at a time where law enforcement agencies were dealing with general organizational issues such as the need for a national system of police cooperation.⁵⁶ They were also facing specific problems regarding the management of fingerprints and criminal records. “Prior to 1924, there was no effective national repository and clearinghouse for fingerprint records, although there was a need for one due to the increasing number and mobility of criminals.”⁵⁷ Another issue was that many states were unable to perform positive fingerprint identifications for law enforcement purposes. A last problem of importance was that many people arrested in one jurisdiction could hide the criminal records they had in other jurisdictions.⁵⁸

⁵³ U.S. Department of Justice, Federal Bureau of Investigation, *The Identification Division of the FBI: A Brief Outline of the History, Services, and Operating Techniques of the World's Largest Repository of Fingerprints* (Washington, D.C.: GPO, 1991), 3.

⁵⁴ Donald L. Doernberg, and Donald H. Zeigler, “Due Process versus Data Processing: an Analysis of Computerized Criminal History Information Systems,” *New York University Law Review* 55, no. 6 (December 1980): 1116.

⁵⁵ Richard Lindberg, *To Serve and Collect* (New York: Praeger, 1991), 79-80.

⁵⁶ U.S. Department of Justice, Federal Bureau of Investigation, *Criminal Identification and the Functions of the Identification Division of the Federal Bureau of Investigation*, 11.

⁵⁷ U.S. Department of Justice, Federal Bureau of Investigation, *FBI: Facts and History* (Washington, D.C.: Government Printing Office, 1990), 5.

⁵⁸ U.S. Comptroller General, *The Federal Bureau of Investigation (FBI) Operates Two Computerized Criminal History Information Systems* (Washington, D.C.: GPO, 1979), 2.

On July 1, 1924, an Act of the Congress provided a partial remedy to the situation by establishing the Identification Division of the FBI - known then as the National Division of Identification and Information - as the nation clearinghouse for fingerprint cards and criminal identification records. The Identification Division of the FBI was established in accordance with the title 28 of the United States Code, Section 534 (28 U.S.C. 534) allowing the U.S. Attorney General:

(1) to acquire, collect, classify, and preserve identification, criminal identification, crime, and other records; (2) to acquire, collect, classify, and preserve any information which would assist in the identification of any deceased individual who has not been identified after the discovery of such deceased individual; (3) to acquire, collect, classify and preserve any information which would assist in the location of any missing person; and (4) to exchange such records and information with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions.

The "other institutions" include authorized railroad police departments and authorized police departments of private colleges or universities.

The first collection of the Identification Division of the FBI consisted of the combination and consolidation of the fingerprint collections of the International Association of Chiefs of Police and of the Federal Penitentiary in Leavenworth. It contained a total of 810,188 fingerprint records and about 200,000 Bertillon cards. The latter were quickly discarded because they were found less useful than the fingerprint records.

In March, 1932 the FBI started to exchange fingerprints with foreign countries. As a result, two years later "1,976 fingerprints were forwarded to foreign bureaus, and of these 6.5% were identified, while 15,387 fingerprints were received from foreign agencies and identifications were effected in 12.3% of these cases."⁵⁹ The FBI Latent Fingerprint Section was created one year later. "Utilizing the most experienced of its fingerprint identification specialists, the FBI Latent Fingerprint Section began to compile and classify on a single fingerprint basis the prints of notorious criminals and

⁵⁹ U.S. Department of Justice, Federal Bureau of Investigation, *The Civil Identification Section* (Washington, D.C.: n.p. 1935), 2.

suspects identified with major crimes.”⁶⁰ The Latent Fingerprint section also does research on unidentified bodies.

Created as a law enforcement agency, the FBI expanded its functions in 1933 when the Civil Service Commission - which now is the Office of Personnel Management - sent to the Identification Division more than 140,000 fingerprints of government employees and job applicants. This was the origin of the Civil Identification Section of the FBI, created on November 10, 1933. Since then, FBI fingerprint records are divided in two separate files. The first, the *Criminal File*, contains fingerprint records submitted to the FBI by local, state, and federal law enforcement agencies of people charged with violating Federal laws. This file provides “law enforcement agencies throughout the country with a means of locating wanted criminals. Posting a wanted notice with the FBI’s Identification Division ensures that an agency will be notified if a fingerprint received later should indicate the whereabouts of the wanted criminal.”⁶¹ The second file, called the *Civil File*, includes the fingerprint records of people applying for government and for some private employment. It also contains the fingerprints of aliens, military personnel, people requesting various permits or licenses, as well as the fingerprints of people who want to have them or the prints of their relatives on file, should the establishment of their identity be needed.

The size of the fingerprint collection of the FBI increased significantly before and during World War II. The submission to the FBI of the fingerprints of all 70,000 civilian employees of the War Department, and the forwarding of fingerprints, names, and other descriptive data on one million youths by the Civilian Conservation Corporation in 1937 are illustrations of this expansion.⁶² As a result, the collection became, according to Hoover, the only ready source of internal security information at the advent of World War II.

⁶⁰Hoover, “The Role of Identification in Law Enforcement: An Historical Adventure,” (Part One), 30.

⁶¹ *Encyclopedia Americana*, 1990, vol. 11, 216.

⁶² Marchand and Bogan, cited by Kenneth C. Laudon, *Dossier Society. Value Choices in the Design of National Information Systems* (New York: Columbia University Press, 1986), 37.

In 1935, under the instigation of Hoover, the FBI encouraged the population to have their fingerprints put on its record. This Program for Voluntary Fingerprinting was at first supported by different business and financial groups, as well as by the President of the United States and other politicians. It met a great deal of success among the population who could be fingerprinted in many public places including some libraries.⁶³ However, opponents to the idea soon appeared. Among them was the American Civil Liberties Union (ACLU) which published in 1938 a pamphlet entitled *Thumbs Down! The Fingerprint Menace to Civil Liberties*. In its introductory note, ACLU declares that “our position is that while fingerprinting may be entirely proper as a means of identification in occupations requiring licenses, it is wholly improper when accompanied by coercion or compulsion.” ACLU feared that a massive fingerprinting would lead the nation towards a regimentation of the population and that the problems that would derive from the fingerprinting method would outweigh its benefits. Among the potential “many evils” [sic], ACLU feared that fingerprint files would provide the basis for a labor blacklist and that such files would offer employers an easy means of control and intimidation of their employees.⁶⁴ The program for Voluntary Fingerprinting was not carried on but, since then, there have been other attempts to encourage the fingerprinting of the population.

The fingerprint collections in police departments continued to grow steadily all across the country, compelling law enforcement agencies to find better ways to manage them.

⁶³ Samuel Walket, *A Critical History of Police Reform: The Emergence of Professionalism* (Lexington, MA: Lexington Books, 1977), 157.

⁶⁴ American Civil Liberties Union, *Thumbs Down! The Fingerprint Menace to Civil Liberties*, (New York: Lexington Books, 1977), 18.

CHAPTER 3
GENERAL USES OF FINGERPRINTS
Uses of Fingerprints in the Fight Against Crimes

Fingerprints are instrumental in daily police practice and in the administration of justice. Their use lies in the determination and verification of identities. In criminal investigations, the analysis of latent prints and their comparison to the prints stored in police files can save people from suspicion or incriminate them. In the latter case, fingerprints are a vital element in conviction because they represent the irrefutable proof of presence at a crime scene. They are therefore used as an evidence against defendants in courts.

Fingerprint records can be exchanged between law enforcement agencies throughout the world in the search for particular criminals. They can also be collected for entire and specific groups of people.⁶⁵

In forensic medicine, research is currently being conducted to discover whether the *biochemical substance* composing latent prints can be used in identifications.⁶⁶

Fingerprints are also used in the prevention of crimes. For instance, law makers try to control violent crimes by legislating the registration of gun which usually includes the fingerprinting of the owners.

A last example of the use of fingerprints for criminal purpose is their application in the deterrence of impersonation or fraud. Decades ago, three pioneers in dactyloscopy (Sir William J. Herschel, Dr. Henry Pelouze De Forest, and Gilbert Thompson) had already used fingerprints with that purpose. There are more current examples. In the 1970s, in order to prevent the use of false checks, people in California were asked to submit their thumbprint on a device that permanently

⁶⁵ See for example: Sharon LaFraniere, and George Lardner, "U.S. Set to Photograph, Fingerprint All New Iraqi and Kuwaiti Visitors. Unusual Move Taken to Try to Counter Possible Terrorist Attacks," *Washington Post*, 11 January 1991, A23; and "U.S. to Fingerprint Visiting Iraqis, Kuwaitis," *San Jose Mercury News*, 11 January 1991, 9A.

⁶⁶ David Brown, "Arches, Loops and Whorls Make Your Mark on the World Unique," *Washington Post*, 3 July 1995, A3.

recorded the print on the checks.⁶⁷ During the same decade, “in order to curb fraudulent acquisition of cards by illegal immigrants and welfare cheaters,”⁶⁸ the Senate Finance Committee in Washington proposed to fingerprint six year old children who received a Social Security card, as well as older applicants for Social Security cards. Fingerprinting welfare recipients was also proposed to San Francisco officials, but was rejected by the city Social Services Commission in 1976.⁶⁹ Today, however, with the advent of automation, welfare recipients of San Francisco and of a few counties in the nation are being required to have their fingerprints taken before they can receive their allocation.

Uses of Fingerprints in Noncriminal Situations

Fingerprints are studied in a particular branch of anatomy that was coined “dermatoglyphics” by Harold Cummins and Charles Midlo in 1926. More exactly, the term covers the scientific exploration of the ridges on the skin of the fingers, the palms, the sole of the feet and the toes.

An important interest of the study of fingerprints in medical research lies in the investigation of the relationship between distinctive dermatoglyphic patterns and specific pathological conditions. The best known example of such a relationship is probably the presence of typical patterns on the finger tips of people suffering from chromosomal disorders like the Down’s syndrome. Other illustrations include the study of fingerprint patterns to detect pathologies of the limb, skin diseases, and mental disorders such as schizophrenia.⁷⁰

Fingerprints are also studied in anthropological research in the study of dermatoglyphic variations between groups of population.

Fingerprints can be used as a means to ensure security by allowing or refusing the access to restricted facilities or systems.

⁶⁷ Bill Hazlett, “Fingerprints: The Only Certain ID,” *Los Angeles Times*, 22 April 1973, II 3.

⁶⁸ “Fingerprints of Workers May Be Kept,” *Fingez Print And Identification Magazine* (May 1972): 23.

⁶⁹ “Welfare Board Says No on Fingerprints,” *San Francisco Chronicle*, 23 July 1976, 2.

⁷⁰ Danuta Z. Loesch, *Quantitative Dermoglyphics. Classification, Genetics and Pathology* (New York: Oxford University Press, 1983).

Another widespread use of fingerprints in noncriminal situations is in the background check for several employment, license and permit investigations and determination. The fingerprinting of school workers is a common procedure aiming at determining if an applicant has a criminal record. Executive Order 10450 regarding the Security Requirements for Government Employment also requests “a check of the fingerprint files of the Federal Bureau of Investigation” for “the appointment of each civilian officer or employee in any department or agency of the Government.”⁷¹ As a last example, the U.S. Code stipulates that:

Every member of a national securities exchange, broker, dealer, registered transfer agent, and registered clearing agency, shall require that each of its partners, directors, officers, and employees be fingerprinted and shall submit such fingerprints, or cause the same to be submitted, to the Attorney General of the United States for identification and appropriate processing.⁷²

In a different area, fingerprints can be very helpful in the investigation of the identity of people suffering from amnesia or of individuals whose identity cannot be determined for various reasons. For example, the mandatory fingerprinting of the armed forces personnel helps in the establishment of the identity of unrecognizable bodies or of those who have been kept prisoners for a long period of time.

Fingerprint-based identifications can take place after the occurrence of disasters such as fires, earthquakes, plane crashes, etc. A good illustration of the difficulty of the task in question is provided by the failure experienced by the FBI to identify 210 out of the 276 children who died on November 18, 1978 during the massacre in Jonestown, Guyana. In his book *The Children of Jonestown*, Kenneth Wooden noted that one of the reasons explaining the high number of unidentified children is that:

Guyana never required fingerprinting for anyone under sixteen years of age, and California, where the majority of the children were born, stopped recording footprints in the late 1950s. The practice was stopped, according to the California Bureau of Vital Statistics, because the ink used for the babies' prints came through the birth certificates.⁷³

⁷¹ Code of Federal Regulations, Title 3, 1949-1953 Compilation, Section 3. (a).

⁷² 15 U.S.C. 78q(f)(2).

⁷³ Kenneth Wooden, *The Children of Jonestown* (San Francisco: McGraw-Hill Book Company, 1981), 198.

A final illustration of the use of fingerprints in noncriminal situations is the voluntary fingerprinting of individuals who request to have a record of their prints recorded and stored in police agency. The fingerprinting of children is encouraged by the police and diverse organizations such as the Vanished Children's Alliance and the Kiwanis Club of Sunnyvale. The possibility of the disappearance or abduction of their children urges some parents to keep a copy of their children's fingerprints at home.

CHAPTER 4
ISSUES LINKED TO THE FINGERPRINTING METHOD
Being Fingerprinted

Because “fingerprinting is not a punishment, but a procedure, the purpose of which is to facilitate law enforcement,”⁷⁴ a suspect in custody can be fingerprinted by police officers without a warrant or without his consent.

Federal and state courts have recognized that the Fifth Amendment privilege against self-incrimination offers no protection against the compulsion to submit to fingerprinting or any other procedures, such as photographing, physical measurements, and writing or speaking for identification. It is elementary that a person in lawful custody may be required to submit to fingerprinting, as well as photographing, as a routine part of the identification process. The Fourth Amendment may even permit fingerprinting without probable cause for arrest. . . . The lawful arrest itself provides sufficient grounds for fingerprinting. The arrestee has no right to counsel when fingerprints are taken, and his refusal to provide prints is admissible as evidence of consciousness of guilt. Furthermore, an arrestee who refuses to give his name and address may be fingerprinted to facilitate his identification. . . . The procedure is minimally intrusive and may be considered essential and proper to facilitate the enforcement and execution of criminal laws.⁷⁵

There are, however, instances where dactyloscopy generated intense controversy.

A notable example is the massive fingerprinting of the Black men of Homestead, PA, in the late 1980s. The initiative was motivated by the failure of law enforcement to catch a man who had assaulted six women in the neighborhood. The psychological profile of the rapist established by the police showed that he might kill his next victim.⁷⁶ As a consequence, “police have requested that every Black male submit to fingerprinting and blood testing to match against evidence they have,

⁷⁴ United States v. Krapf, 285 F2d 647 (1961), cited in *Law Enforcement Reference Manual and Police Official Diary* (Trenton, NJ: Irving B. Zeichner editor, 1979), 126.

⁷⁵ William W. Parker, “Authority to Fingerprint Arrestee Is Clear - But What to Do When He Resists?” *The Police Chief* 59, November 1992, 10.

⁷⁶ “The Search for a Rapist,” *Newsweek*, 14 September 1987, 42.

evidence that also has definitely identified the suspect as a Black.”⁷⁷ The fingerprinting, which was to be applied to the men between the ages of 16 and 60, was voluntary. More than a hundred people agreed to undergo the procedure, but the rapist was finally caught through traditional police methods.

The police initiative was criticized by the Pittsburg branch of the ACLU which considered the practice as a violation of constitutional rights of black men. According to the Constitution’s equal protection clause, individuals cannot be singled out by the government because of a race or an ethnic origin. However, the President of the local chapter of the National Association for the Advancement of Colored People (NAACP) thought the procedure might well be necessary, but he also encouraged police to use other tactics in their investigation. This view was criticized in turn by the national office of the NAACP which declared that their position “has been and remains unalterably opposed to the fingerprinting procedure practiced by the Homestead (Pa.) police. . . . We regard it as police power run amok and is totally unacceptable in a democratic society where the rights of the individual are sacred.”⁷⁸ A third source of criticism came from some parents who questioned the voluntary nature of the fingerprinting of their sons and reported incidents of police harassment. Other parents expressed their concerns about what would happen to the prints in the future.⁷⁹

A similar case that has been evoked earlier involves another ethnic group that was subjected to fingerprinting in the agitated times of the war in the Gulf. In its fight against terrorism, the Department of Justice ordered INS officers to photograph and fingerprint every holder of an Iraqi or Kuwaiti passport. This procedure was qualified as anti-constitutional and was also considered as a violation of the privacy rights of Arab Americans.

When one leaves the field of law enforcement, the fingerprinting method can also become subject to controversy.

To start with, the constitutionality of being fingerprinted can be questioned.

⁷⁷ Lou Ransom, “Fingerprinting Only Black Males in Town Sparks Tension, Fear,” *Jet*, 21 September 1987, 12.

⁷⁸ “Homestead NAACP Chided on Fingerprint Suport [sic],” *Jet*, 28 September 1987, 7.

⁷⁹ Ransom, “Fingerprinting Only Black Males in Town Sparks Tension, Fear,” 12-13.

For example, in 1992 in California, "The state Supreme Court has refused to put into effect a lower-court ruling forbidding a city from requiring charitable solicitors to get fingerprinted. . . . The high court did not decide whether the fingerprint requirement was constitutional, an issue that remains unresolved. But by withdrawing the only appellate ruling against the practice, it removed a legal barrier to enforcement of any such local requirements in any city except Glendale, where the case originated."⁸⁰

Secondly, depending on the context where the fingerprinting takes place, the procedure can be perceived as a form of control by the government, an intrusion in someone's life, an invasion of privacy, or as a way to stigmatize a person and to reduce him/her to the rank of a criminal. This point will be expanded in Part Three of this study, in a chapter dedicated to the fingerprinting of welfare recipients and applicants.

Misuses of Fingerprints

The presence of a fingerprint at the scene of a crime is probably one of the strongest evidences of the guilt of a person and it is therefore crucial to his conviction. This observation leads to a double question. First, is it possible to forge a fingerprint? Second, are there any cases where fingerprints have been falsely reported present at the scene of a crime in order to incriminate an innocent person? The answer in both cases is positive.

To begin with, it is possible to forge fingerprints. Clements describes the way he duplicated the thumb print of one of his colleagues by using a liquid plastic.⁸¹ However, the author points out the fact that, if the goal of the forgery is the conviction of an innocent person, the mere forgery of a fingerprint is only the first step in the criminal scenario. The false print still needs to be placed in a crime scene and must be discovered by a latent fingerprint expert.

Three examples illustrate the second question. They demonstrate the confidence juries and members of the judicial system put in fingerprint evidence as they are brought at trials by law enforcement agents.

⁸⁰ "Court Won't Back Fingerprint Ruling," *San Jose Mercury News*, 13 June 1992, 3B.

⁸¹ Clements, *The Study of Latent Fingerprints: A Science*, 129-130.

The first case involves Count Alfred de Marigny in Nassau which had been accused in 1943 of the murder of his wealthy father-in-law, Sir Harry Oakes. The handling of the investigation in general and of the fingerprint evidence in particular has been characterized as “botched” by some authors. After many problems that will not be described here, the Count was finally acquitted of the charges against him when “experts convinced a jury that a fingerprint of the accused has [had] been deliberately ‘lifted’ from one place and implanted on another to produce damaging evidence against the defendant.”⁸²

The second example occurred in the late 1960s in the city of Buena Park in California. A catering truck driver arrested for a traffic violation had his fingerprints on record in a local police department. A police officer convinced of his culpability in a bank robbery copied his inked fingerprints from the police file and reported them as latent prints found in the bank.⁸³ Although thirteen witnesses testified that the truck driver was serving lunch at the time of the robbery, his print “evidence” led the judge to sentence him in 1968 to fifteen years in prison. “One small piece of evidence - a fingerprint - outweighed all the alibi testimony.”⁸⁴ The truck driver served 28 months before being released when the plot was discovered. The police officer was not charged in the case because he was covered by the expiration of the statutes of limitations. He was however expelled from the police for perjury and for the falsification of fingerprints in another case, and was sentenced to one year in prison.

The third example spread consternation and dismay within New York State Police and the public when two troopers “pleaded guilty to evidence-tampering in more than 20 criminal cases between 1988 and 1992.”⁸⁵ The scandal started with David L. Harding who worked for seven years as an excellent investigator in upstate New York. In 1991, after revealing his criminal actions during a job interview at the Central

⁸² Block, *Fingerprinting: Magic Weapon Against Crime*, 34.

⁸³ Clements, *The Study of Latent Fingerprints: A Science*, 127-128.

⁸⁴ Bob Baker and Paul Lieberman, “Faulty Ballistics in Deputy’s Arrest. Eagerness to ‘Make’ Gun Cited in LAPD Lab Error,” *Los Angeles Times*, 22 May 1989, II3.

⁸⁵ “Third State Trooper Arrested in Evidence-Tampering Case,” *New York Times*, 1 May 1993, 29.

Intelligence Agency,⁸⁶ he became the subject of an in-depth investigation. In the course of the trial that followed, he confessed to having lied in court in several cases where he testified as an expert. With regard to fingerprints, he lied among other things about the place where he found some of them, incriminating therefore innocent people. He was sentenced in December 1992 to four to twelve years in prison for evidence tampering in four criminal cases.

As a consequence of this case, the New York State Police decided to adopt the same procedures used by other police departments and the FBI in the handling of evidence and the verification of fingerprints. The new procedures include the following changes: "At least two investigators must sign all crime-scene reports and verify procedures used to obtain fingerprints. Investigators must photograph any fingerprints on an object before lifting them. Each of the 11 state police troops will be assigned a senior investigator to oversee criminal investigations, and two supervisors will review any fingerprints discovered at crime scenes."⁸⁷

Drawbacks of the Manual Fingerprint Method in Police Work

In theory, dactyloscopy is considered to be one of the best identification tools in police hands. However, and contrary to popular belief, many authors agree with Fincher when he writes that "the whole business of fingerprinting remains a chancy affair at best."⁸⁸ The truth of the matter is that the manual processing of fingerprint cards decreases by much the potential of the entire method.

The review of the literature shows that several factors are contributing to seriously hamper the expected benefits of manual dactyloscopy:

(1) Fingerprint patterns can be misclassified or classified differently by various experts for reasons such as:

- the ambiguity of some fingerprint patterns. According to Cowger, there is a part of subjectivity in the classification process. "While each class and subclass of pattern can be, and is, specifically defined for the system used, there is a continuum or

⁸⁶ "New York State Police Alter Evidence Procedures," *New York Times*, 9 March 1993, B6.

⁸⁷ Ibid.

⁸⁸ Jack Fincher, "Lifting 'Latents' is Now Very Much a High-tech Matter," *Smithsonian* (October 1989): 202.

flow from one pattern type to another that defies absolute delineation between types.”⁸⁹ This makes the fingerprinting method a science as well as an art, because the identification task relies in part on the expertise and in part on the judgment of fingerprint specialists.

- the increasing number of new subdivisions created to face the multiplication of fingerprint records. “The history of fingerprint technology development until very recently has been one of devising extended classification subcategories to enable the Henry system to accommodate increased numbers of prints.”⁹⁰ Cowger explains this the following way: “Because filing schemes began fairly simply and on a small scale, the rules and definitions were fairly broad. As the files grew, greater definition was necessary and the rules for classification grew more complex. These changes did not emanate from a single source and so, unfortunately, there are many variations in the interpretation of pattern types and subtypes even among those who, for instance, use the *Henry* system.”⁹¹

(2) A number of errors in the filing of fingerprint records prevented the identification process. The refiling was time consuming and labor intensive.

(3) While latent prints have always been expected to be of poor quality in criminal investigations, inked fingerprints were often of poor quality too. Depending on the pressure used at the time of the creation of the records, different distortions in the fingerprint patterns appeared on the cards making them smudged, overinked, or underinked.⁹²

- “Approximately eleven percent of the fingerprints submitted to the FBI are rejected because of poor quality and are returned to the contributing agency with a

⁸⁹ Cowger, *Friction Ridge Skin: Comparison and Identification of Fingerprints*, 36.

⁹⁰ U.S. Department of Justice, Bureau of Justice Statistics, *Automated Fingerprint Identification Systems: Technology and Policy Issues* (April 1987), by Thomas F. Wilson and Paul L. Woodard (Washington D.C.: GPO, 1987), 2.

⁹¹ Cowger, *Friction Ridge Skin: Comparison and Identification of Fingerprints*, 37.

⁹² Jim Mallory, “Electronic Fingerprint Technology,” *Law and Order* (May 1992): 116.

request for submission of better quality prints. In a large percentage of these cases, resubmissions are not received."⁹³

- The FBI rejects 18 percent of the inked cards it receives from local agencies.⁹⁴

- Up to 40 percent of the tenprint cards created in the conventional way are "of such poor quality that they are unstable."⁹⁵

In practical terms, this resulted in thousands of records that could not be used for identification purpose.

(4) The determination of the identity of suspects anxious to conceal their identity was a lengthy process that could exceed the time allowed by law. In Milwaukee County Sheriff's Department, for example, "The manual process could take up to a couple of days, which is a violation of the suspect's rights. In 1987, it became a federal law that a suspect held for more than four hours without booking had to be released."⁹⁶ This could end up in the release of a number of wanted criminals whose identity had not been established in time.

(5) As most of the fingerprint files consisted of the prints of the people arrested in a particular jurisdiction, a person arrested in one place but who had a prior record in another jurisdiction would not necessarily be identified with the conventional dactyloscopy.

(6) The exchange of fingerprint information between law enforcement agencies by mail slowed the identification process. At the FBI, "The average . . . fingerprint check time is 15 to 20 work days (mail delays can increase the average to 20 to 30

⁹³ U.S. Department of Justice, Bureau of Justice Statistics, *Data Quality of Criminal History Records* (Washington, D.C.: GPO, 1985), 26.

⁹⁴ Andrea Adelson, "Faster, More Accurate Fingerprint Matching," *New York Times*, 11 October 1992, 9.

⁹⁵ David G. Hall, "New Remote, Interactive Technology Enables Linkage of AFIS Systems," *The Police Chief* (October 1987): 62.

⁹⁶ "Milwaukee Installs Electronic System for Criminal Suspect Booking," *Government Imaging* (March-April 1994): 1.

days) and is too slow for many criminal justice purposes.”⁹⁷ The exchange of this information by fax was faster but it affected the quality of the prints.

(7) The collections of fingerprint cards took a lot of space in police departments. The FBI, which holds the biggest collection of fingerprints in the world, provides the best illustration for this point. “Imagine stacks of these [standard fingerprint] cards piled on top of one another, each as tall as the Empire State Building. One hundred and thirty-three such stacks would represent the approximate 193,000,000 cards on file in the Identification Division.”⁹⁸ In 1997, that number increased to reach “over 213,000,000 civil and criminal fingerprints of which approximately 127,000,000 are criminal.”⁹⁹

In addition to these general issues, others were specifically related to the processing of latent prints.

(1) “Although the potential usefulness of comparison of latent fingerprints as positive identifier has been known and accepted for a long time, its use on a practical level has been fairly limited. The obvious reason, of course, is that without a specific suspect in mind, it has been virtually impossible . . . to do a manual search of even all locally held ten-print cards.”¹⁰⁰

One of the very first problems faced by fingerprint specialists was indeed that the identification process was based on the knowledge of the identity of a suspect. When police had no suspect in mind, fingerprint experts performed cold searches, that is, searches “where no suspect or other identifying information other than crime scene prints are available to the police.”¹⁰¹ This guessing strategy has been judiciously referred to as “a needle in the haystack” strategy because the fingerprint specialists

⁹⁷ U.S. Congress, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options - Background Paper* (Washington, D.C.: GPO, 1991), 6.

⁹⁸ U.S. Department of Justice, Federal Bureau of Investigation, *The Identification Division of the FBI*, 9.

⁹⁹ “IAFIS: The Real Story,” [file on-line]; available from <http://www.fbi.gov/iafis/story.htm#results>; Internet; accessed 2 March 1997.

¹⁰⁰ Berg, *Law Enforcement: An Introduction to Police in Society*, 289.

¹⁰¹ Lyman, *Criminal Investigation*, 144.

had to compare the incoming latent print to the huge amount of prints in file. This task was nearly impossible to do and, therefore, most of the prints were never used in cold searches. They were "simply stored on the chance that they may be used in the future."¹⁰²

(2) The manual comparison of inked to latent fingerprint was tedious, extremely demanding and exhausting. "The work requires knowledge, patience, a trained eye and above all, tenacity. It is difficult, mentally and physically to study latent prints hour after hour, day after day, attempting to identify them to suspects."¹⁰³ The poor quality of latent prints made their classification very difficult, if at all possible. The individual level of competence of fingerprint specialists played consequently an important role in the identification process.

(3) The processing time of latent prints was extensive. In many cases, it could take months of search to find a match - if a match was ever found. The proliferation of fingerprint records worsened the situation. "As files sizes increase, such search becomes improbable, if not humanely possible."¹⁰⁴

The manual analysis of latent prints resulted therefore in an extremely low rate of identifications. A dazzling illustration is provided by the results of a study done during the 1970s in three major police departments in California. This study, which evaluated among other factors the frequency of identifications after the lifting of latent prints in 200 randomly selected residential burglary cases, revealed that, amazingly enough, identifications were made for only 1.5 percent of the cases in Long Beach, for 1.1 percent of the cases in Berkeley, and for 1.2 percent of the cases in Richmond.¹⁰⁵

Not surprisingly, the combination of the foregoing problems made the manual fingerprinting method insufficient and even inadequate in many cases to meet the

¹⁰² Peter W. Greenwood, Jan M. Chaiken, and Joan Petersilia, *The Criminal Investigation Process* (Lexington, MA: D.C. Heath and Company, 1977), 154.

¹⁰³ Clements, *The Study of Latent Fingerprints: A Science*, 79.

¹⁰⁴ U.S. Department of Justice, Bureau of Justice Statistics, *Automated Fingerprint Identification Systems: Technology and Policy Issues* (April 1987), 2.

¹⁰⁵ Peter W. Greenwood, Jan M. Chaiken, and Joan Petersilia, *The Criminal Investigation Process*, 154.

needs of the police in the field of identification. They often had to deal with the frustrating situation of having between their hands the proof of the culpability of a person that they were not able to identify because of insurmountable practical problems linked to the method in use. So, instead of being storehouses of valuable data, fingerprint collections were, to a large extent, a waste of precious resource. However, it was also obvious that the fingerprint files would keep growing. It was also understood that an increase in personnel or/and in financial resources in fingerprint records management would not necessarily increase the number of identification of criminals.¹⁰⁶ The law enforcement community was in great need for better investigative and fingerprint records management tools.

Fortunately, the research and development work in computer science and information technology was rapidly expanding, and promising technological devices became available. Their performance gave law enforcement officials the insight to conceive and design electronic fingerprint identification systems, which were an efficient and functional new approach to process the massive and ever increasing amount of fingerprint records.

¹⁰⁶ Ibid., 144.

PART TWO

ELECTRONIC FINGERPRINTING

ADVANCES

INTRODUCTION

An AFIS system can be defined as a "computerized system that stores fingerprint record cards in its database and can readily match latent prints found at crime scenes or identify suspects who have been arrested."¹⁰⁷ This definition is restrictive in the sense that it does not take into account the fact that AFIS systems not only store fingerprint record cards, but also the images coming from the direct scanning of fingers. Neither does it take into consideration other applications of automated dactyloscopy. Besides their application in criminal investigations, AFIS systems are used in various background checks, in the deterrence of welfare fraud, as security devices, etc. Finally, AFIS systems are not only used in the determination of the identity of suspects; they can also be applied to the identification of victims, and more generally to the identification of anyone whose fingerprints have been captured by the automated system. Bearing these points in mind, Suthard's broader definition of an AFIS is more accurate than Berg's: "An AFIS is a computer system designed to analyze, store, match and retrieve fingerprint images and the matching features extracted from the image."¹⁰⁸

AFIS technology brings important improvements in the way fingerprints are processed. Fingerprints are electronically scanned from tenprints cards or from latent prints or they are live-scanned, that is, scanned directly from the fingers of a person. Data are extracted from each fingerprint image, analyzed, and automatically converted into unique binary digital codes. This basic process varies from vendor to vendor, but two technologies stand out. Printrak International Inc. uses the minutiae as the basis for its fingerprint comparison method. Parameters such as the type of minutiae (that is, if they end, split, or merge), their location, and the direction of the ridges are taken into consideration. An image processor reads and analyzes the image and identifies a certain number of minutiae points from each finger. It then converts them into the binary formula which expresses the relationship among minutiae. On the other hand,

¹⁰⁷ Berg, *Law Enforcement: An Introduction to Police in Society*, 310.

¹⁰⁸ R.L. Suthard, "Implementing an Automated Fingerprint System in Virginia," *The Police Chief* 56, no. 6 (June 1989): 26.

the method used by Nippon Electronic Corporation (NEC) in its design of the California Automated Identification System (CAL-ID) is based on the fact that the poor quality of many inked prints prevents the good reading of the minutiae points and causes consequently a loss of accuracy in the search. Therefore, while "most other AFIS systems' method for comparison is to check the minutiae in the form of ridge ending and bifurcation points, . . . the NEC system of CAL-ID uses for data the number of ridges between minutiae points, which is immune to distortion. Points are compared as to how many ridges are in between them."¹⁰⁹

Digitized fingerprint images are then stored in the computer's memory where they can be searched and compared to the ones already in the database. Different types of searches can be performed: tenprint against tenprint; tenprint against latent; tenprint against tenprint and latent; latent against tenprint; latent against latent; latent against latent and tenprint; tenprint against unsolved latent; latent against unsolved tenprint.

The search and comparison process, which can be done from a remote or a central location, aims at finding a match. During the matching process, the AFIS system computes "a relative probability that two fingerprints are from the same finger (of a subject)."¹¹⁰ Matches have the double purpose to establish or to verify an identity. In the first case, the incoming print is matched with the entire database; in the second case, it is matched with only one record. At the end of the matching process, the AFIS system generates a rank-ordered list of possible "hits" that are displayed side-by-side with the incoming print for comparison. The Massachusetts AFIS, for example, reports up to ten best hits.¹¹¹ The Northern Virginia Regional Identification System generates

¹⁰⁹ J. Van Duyn, *Automated Crime Information Systems* (Blue Ridge Summit, PA.: TAB Professional and Reference Books, 1991), 36. A more detailed overview of five available automatic fingerprint identification systems is provided in Henry C. Lee and R.E. Gaensslen, *Advances in Fingerprint Technology* (New York: Elsevier, 1991), 176-182.

¹¹⁰ Van Duyn, *Automated Crime Information Systems*, 30.

¹¹¹ Berg, *Law Enforcement: An Introduction to Police in Society*, 290.

“a listing of individuals whose fingerprint minutiae match 75-percent or more the minutiae patterns of prints already in the system.”¹¹²

The final determination of an identity is made by fingerprint specialists and not by the AFIS system. The specialists testify in court and have the responsibility to prove the existence of a hit by demonstrating the similarities between a latent print and the hit they have isolated from the list generated by AFIS.

In more than twenty years of intensive research and development, AFIS technology has evolved and improved. When first implemented in police departments, these systems performed only basic identification tasks. With the evolution of computer science, however, the systems have become increasingly complex and powerful. Many of them are integrated with other criminal justice identification systems and law enforcement information systems, such as computerized criminal history systems and jail management systems. At the same time, AFIS are integrated with advanced technologies such as computer imaging, laser technology, and neural technology.¹¹³

Organization of Part Two

Chapter 5 describes the remarkable efforts made by the FBI to stimulate technological advances in the field of fingerprint processing. Although the very first AFIS - which was “a prototype system used to search fingerprints against a small, experimental database” - was developed during the 1960s by Pierre Thibault of the French National Police in Paris,¹¹⁴ credit for the expansion of AFIS technology in the

¹¹² William Folsom, “Automated Fingerprint Identification Systems,” *Law and Order* (July 1986): 27.

¹¹³ With this technology relying on the way the human brain works, a computer system “can learn to recognize patterns. Fingerprints are entered into the computer with a laser scanner and the neural network notes the patterns of whirls and ridges in detail. . . . When the system is asked to find a match for a new print, it produces 10 which are closest to it and a specialist examines those to find the correct match. Large numbers of sample prints are fed into the network to “train” it to recognize different patterns. If it errs, the correct answer is entered in and the computer will be more likely to get it right next time.” (Monica Horten, “Business Technology: Long Arm of Law Puts a Finger on High Tech Computers,” *Daily Telegraph*, 16 August 1993, 25).

¹¹⁴ Suthard, “Implementing an Automated Fingerprint System in Virginia,” 26.

United States is due to the FBI. Chapter 5 provides an overview of its past realizations and of its forthcoming projects.

Chapter 6 outlines various areas of application of AFIS technology outside the field of law enforcement. This includes the use of the technology by other agencies of the government as well as its use in the private sector.

Chapter 7 discusses the advantages of AFIS technology over manual systems of identification in law enforcement.

CHAPTER 5

BRIEF HISTORY OF AFIS TECHNOLOGY WITHIN THE FBI

The Identification Division of the FBI

The first step toward the automation of fingerprint records held in the Identification Division of the FBI occurred in 1934 with the installation of a punching system to process the cards.

In many of the subdivisions in the fingerprint files of the Identification Division, the number of fingerprint cards has grown to such an extent that searching them by hand has become unwieldy. In these subdivisions a system of searching by machine has been adopted. Under this system a punched card is made, which card is punched according to a formula representing the various fingerprint characteristics appearing on each fingerprint card. A selecting machine is then utilized which is very similar to the multiple card sorting machine which is found in many commercial houses today.¹¹⁵

Although helpful at first, it became increasingly clear over the years that the punching method was insufficient to meet the growing workload of the Division. A totally new technology was eventually designed through the joint efforts of the FBI and the National Bureau of Standards (NBS), in which computer hardware and software were conceived and designed to read, match, store and retrieve the data found on the fingertips.

1963 marks the beginning of intensive research in automatic fingerprinting.¹¹⁶ A few years of industrial experimentation were required to produce concrete results. In the late 1960s, the FBI signed a contract with Rockwell International Corporation (known then as the Autonetics Division of North American Aviation, Inc.) and with Calspan Corporation (called at that time the Cornell Aeronautics Laboratory, Inc.) to develop automated fingerprint readers (AFR) able to process minutiae data. In the

¹¹⁵ U.S. Department of Justice, Federal Bureau of Investigation, *Criminal Identification and the Functions of the Identification Division of the Federal Bureau of Investigation* (1 July 1937), by John Edgar Hoover, (np. 1937), 11.

¹¹⁶ For a more detailed chronology of the development and the implementation of a AFIS systems, see David Klug, Joseph L. Peterson, and David A. Stoney, *Automated Fingerprint Identification Systems: Their Acquisition, Management, Performance, and Organizational Impact* (National Institute of Justice, 1992), 19-23.

meantime, NBS developed software programs capable of classifying, searching, and matching the fingerprint data generated by the reader equipment.

A major problem with the AFR designed by the two companies was that they could only read fingerprint records of good quality. The FBI, which received a large number of fingerprint cards of poor quality, determined that developments in the technology designed by Calspan would better suit its needs. In September 1972, the company delivered to the FBI a prototype AFR able to read fingerprints of lower quality. The prototype was called FINDER, from the contraction of the words FINGERprint reaDER. FINDER could scan and read a fingerprint in half a second.

In 1974, the FBI signed a contract with Rockwell for the construction of five production model readers which were delivered to the FBI by August 1977.¹¹⁷ The expectations were high, as it is demonstrated in a text by Hoover:

It is hoped that the entire file of computerized criminal fingerprints stored at FBI Headquarters will one day have the capability of being selectively scanned for comparison with a single latent print found at the scene of a crime. It is also probable that electronic scanners may some day read and classify finger and palmprints directly from the surface of the human hand. With these exciting possibilities, an incriminating latent fingerprint could be, after appropriate classification, transmitted directly from a crime scene to the FBI Identification Division for matching or elimination against each fingerprint of all criminals on file. Correspondingly, with future equipment improvements, it is conceivable that a criminal suspect's identity may be instantly determined by simply placing his hand on an electronic scanner at police headquarters - or even one mounted in a patrol car!¹¹⁸

The project to automate the FBI criminal records and fingerprint files evolved in three phases.¹¹⁹ The purpose of the first phase of the FBI Automated Identification System (AIS-I), which started in 1972 and was implemented one year later, was to computerize the criminal history records of all the first offenders born after 1955 by creating a database with their names, some descriptors, and information such as the arrest charges and the disposition data. The second phase of the project (AIS-II)

¹¹⁷ U.S. Comptroller General, *The Federal Bureau of Investigation (FBI) Operates Two Computerized Criminal History Information Systems*, 7.

¹¹⁸ Hoover, "The Role of Identification in Law Enforcement," (Part Two), 24.

¹¹⁹ Neudorfer, "Fingerprint Automation: Progress in the FBI's Identification Division."

started in 1979 and provided for the automated name searching of incoming fingerprint cards against the database built during the first phase of the project. In 1983, AIS-II was connected with the National Crime Information Center's Interstate Identification Index (NCIC-III) and records started to be exchanged online in September of the following year between the FBI and the States that had joined III.¹²⁰ The third phase involved the automation of fingerprint searching. Implemented in 1989, it was designed to reduce the processing time for fingerprint records for both criminal justice and noncriminal justice purposes.

In addition to the automation of tenprint cards, the FBI also worked on the automation of latent prints and developed a Latent Descriptor Index which allowed a search of the files of the Identification Division by using latent fingerprint pattern types, case and physical description information.¹²¹ It also developed an Automated Latent System Model (ALSM) for the identification of latent prints. Based on artificial intelligence, ALSM targets repeat offenders and other persons described as "criminals in specific crime-type categories" by Neudorfer, and as "individuals known to be associated with special interest groups of major concern to the FBI" by Deakin.¹²² Information such as personal description, fingerprint data and the designation of the special interest groups are entered in the system and matched with the data already stored.

AFIS technology was also implemented by law enforcement agencies outside the FBI. In 1978, the San Jose Police Department served as a beta test site for a fingerprint identification system made by Printrak. In the same year, this company also installed the first AFIS fully operational outside FBI in the state of Minnesota. Printrak later installed AFIS systems in other law enforcement agencies including the Montgomery County Police Department, the Prince George's County Police

¹²⁰ A general description of the National Crime Information Center (NCIC) and of the Interstate Identification Index (III) is provided later in this chapter.

¹²¹ Neudorfer, "Fingerprint Automation: Progress in the FBI's Identification Division," 4.

¹²² Ibid., 5; Deakin, *Police Professionalism: The Renaissance of American Law Enforcement*, 297.

Department, MA, the Houston Police Department, and the California State Department of Justice.

Besides Printrak, two other companies were competing in the AFIS market, the Japanese company NEC and North American Morpho Systems. NEC sold its first AFIS system in the U.S. to the San Francisco Police Department in 1983 and then sold another system to the State of California. Morpho installed its first AFIS in Pierce County/Tacoma, WA in 1986.

The three companies Printrak, NEC, and Morpho are still leaders in the electronic fingerprinting field. Data in the Klug survey indicate that 47% of the agencies answering their questionnaire chose an AFIS designed by Printrak; 42% chose a system designed by NEC; and 11% chose one designed by Morpho.

Throughout the States, the tendency is for more law enforcement agencies to acquire fingerprint automated systems:

- "during the mid- to late 1980's more than 40 AFIS systems (data bases) were sold and installed by the three major vendors;"¹²³
- in 1990, the FBI reported that just "over half of the states and about 50 cities or counties agencies have operational automated fingerprint systems;"¹²⁴
- in 1991, Valentine stated that about thirty states have automated identification systems;¹²⁵
- in 1993, Slade wrote that "Thirty-nine states and the District of Columbia, along with some 350 towns, cities and counties now use AFIS technology."¹²⁶

Forthcoming Programs

The Integrated Automated Fingerprint Identification System

The FBI has its own custom designed AFIS, known as the Automated Identification System (AIS); but the FBI's system is obsolete and incompatible with the AFIS systems used by the States. . . . The Ident modernization plan is known as the Integrated Automated Fingerprint Identification System (IAFIS),

¹²³ Klug, *Automated Fingerprint Identification Systems*, 15.

¹²⁴ "WIN: AFIS Technology for Rural States," *FBI Law Enforcement Bulletin* (November 1990): 24.

¹²⁵ Paul W. Valentine, "1 Fingerprint Worth 1,000 Words on Md. Computer," *Washington Post*, 30 May 1991, C4.

¹²⁶ Margot Slade, "Fingerprint System Extends Arm of the Law," *New York Times*, 12 November 1993, B20.

and provides for the electronic transmission, storage, and processing of fingerprints.¹²⁷

The IAFIS is briefly described in the IAFIS brochure.¹²⁸ According to the brochure, IAFIS will provide five key services to law enforcement agencies:

- (1) the identification service based on tenprints cards sent to the FBI for both criminal and noncriminal purposes;
- (2) the identification service based on latent prints sent to the FBI;
- (3) subject search and criminal history services;
- (4) document and image services, including the electronic transmission of fingerprint images;
- (5) remote search services for identification purposes by authorized requesters who are not employed by the FBI.

Among the specific features the FBI wants to integrate in its \$787 million IAFIS system, Quindlen cites the following: a definite increased speed of processing of data along with the capability to scan fingerprint images and to display them on a computer screen; the capability to collect criminal history data, to perform searches for fingerprint and criminal history data, to add drawings, notations and marks to the images, to print out latent prints directly from a crime scene and the matches stored in the computer.¹²⁹

IAFIS, which should be fully operational in 1998, has three components.

(1) An advanced AFIS described by David Nemecek as the "data cruncher" of the whole system.¹³⁰ It will handle the fingerprint searching process of automated tenprints and latent fingerprints.

(2) An updated Interstate Identification Index (III) will provide the "implementation of the National Fingerprint File (NFF) concept; access to more

¹²⁷ U.S. Congress, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options*, 6.

¹²⁸ The "IAFIS brochure" is the U.S. Department of Justice, Federal Bureau of Investigation, *Integrated Automated Fingerprint Identification System (IAFIS)* (Washington, D.C.: GPO, 1994). The part of the brochure concerning the five IAFIS services is available on Internet at: <http://www.fbi.gov/iafis/iafisser.htm>; accessed 2 March 1997.

¹²⁹ Terrey Hatcher Quindlen, "FBI Shops for a Speedy Fingerprint System," *Government Computer News* (9 December 1991): 6.

¹³⁰ David Nemecek, deputy assistant director of the Criminal Justice Information Systems Division of the FBI, cited by Tim Minahan, "FBI Begins Effort to Overhaul Its Fingerprint ID System," *Government Computer News* (30 August 1993): 16.

criminal history data; the capability to transmit, store, and retrieve on-line electronic images of mug shots; and an upgrade of the technology base of III for supporting the overall workload.”¹³¹

(3) Finally, the Identification Tasking and Network project (or ITN), which will interact with the advanced AFIS and the III, is designed to “develop a system that will provide for the submission of electronic fingerprint images via NCIC or mailed fingerprint cards for identification purposes for fingerprint examiners.”¹³² ITN aims at the total elimination of the use of paper in the processing of fingerprint images. However, as all the police departments in the country are not yet automated, ITN will also support the paper transmission of the information.

The ITN project will reach high throughput levels. “When completed, ITN machines will support the processing of 30,000 to 100,000 electronic fingerprint images transmitted over the NCIC network daily”¹³³ and will give the FBI access to more than 200 million fingerprint records.¹³⁴

The National Crime Information Center (NCIC) 2000

General Presentation of the NCIC

The NCIC is authorized by title 28 of the United States Code, Section 534 (28 U.S.C. 534). It is managed by the FBI assisted by an Advisory Policy Board composed of 20 NCIC law enforcement officials elected from the states, and 6 members appointed by the Director of the FBI (2 from the judiciary, 2 from prosecuting agencies, and 2 from correctional institutions). An additional four members are designated by the International Association of Chiefs of Police, the National Sheriff’s Association, the National District Attorneys’ Conference and the National Probation and Parole Association.

¹³¹ Bruce J. Brotman and Rhonda K. Pavel, “Identification: A Move Toward the Future,” *FBI Law Enforcement Bulletin* 60 (July 1991): 5.

¹³² U.S. Department of Justice, Federal Bureau of Investigation, *Automated Information Systems Plan: Tactical Plan (Fiscal Year 1993-1995)*, Criminal Justice Information Services Division (Washington, D.C.: GPO, 1993), 2.

¹³³ Minahan, “FBI Begins Effort to Overhaul Its Fingerprint ID System,” 16.

¹³⁴ “PRC Snags FBI Fingerprint Contract,” *Government Imaging* 3, no. 5 (July 1994): 20.

The board members, who represent the four geographic regions of the United States, confer with state representatives, make recommendations, and formulate policies. The recommendations and new policies are then passed on to the Director of the FBI for his approval. Thus, in the final analysis, it is the director's decision as to NCIC's direction of operation, unless the U.S. Attorney General intercedes.¹³⁵

In every state, the District of Columbia, Puerto Rico, the Virgin Islands of the U.S., and Canada,¹³⁶ a law enforcement agency called the Control Terminal Agency (CTA) is responsible for the management of the state's criminal justice information system through which local user agencies access NCIC. Each of the 54 CTA designates a Control Terminal Officer (CTO) who is responsible for complying with NCIC policy and procedures issues.¹³⁷

The National Crime Information Center is a computerized index of criminal information and a law enforcement communication network that connects police agencies across the United States with the FBI. It is "the largest and best-known automated crime information system - as well as one of the most effective crime-fighting tools for the past 20 years in the United States."¹³⁸ It is also cited as the best example of law enforcement cooperation.¹³⁹

The original NCIC began operation on January 27, 1967 with a computer of a capability of only 128 Kbytes. It operated with 15 law enforcement agencies and one FBI field office "operating on a test schedule of 2 hours a day."¹⁴⁰ It was later extended in service to 24 hours each day, and included more than 60,000 law enforcement and

¹³⁵ Van Duyn, *Automated Crime Information Systems*, 3.

¹³⁶ Canada is the only foreign country allowed to access NCIC directly. The other countries must access the system through the Drug Enforcement Agency "which is the official liaison point with Interpol" (Hebenton, *Criminal Records: State, Citizen and the Politics of Protection*, 52).

¹³⁷ Don M. Johnson, "NCIC Training. Hit or Miss," *FBI Law Enforcement Bulletin* 60 (January 1991): 2.

¹³⁸ Van Duyn, *Automated Crime Information Systems*, 3.

¹³⁹ Johnson, "NCIC Training. Hit or Miss," 1.

¹⁴⁰ Deakin, *Police Professionalism: The Renaissance of American Law Enforcement*, 247.

criminal justice agencies. NCIC handles about 750,000 inquiries a day.¹⁴¹ All these law enforcement agencies are linked through sophisticated telecommunication networks, the main one being the National Law Enforcement Telecommunications System (NLETS). Other significant networks are the California Law Enforcement Telecommunications System (CLETS) and the International Law Enforcement Telecommunications System (INLETS).¹⁴² Heberton notes that NCIC "interfaces with a number of criminal justice information systems operated by other federal, state and local agencies. This includes the Identification Division, the National Law Enforcement Telecommunications System, the US Treasury Enforcement and Communication System, [and] the Department of Justice Telecommunications System."¹⁴³ The NCIC is the largest law enforcement telecommunications system in the world.¹⁴⁴

The Files of the NCIC

The number of files in the current NCIC system and their exact name cannot be determined from the available sources.¹⁴⁵ This is probably due to the fact that the information gathered by the NCIC is sensitive and is therefore not publicized outside the law enforcement community. Still, a report on the NCIC hot file system finds it rather surprising that:

Despite its importance, . . . , relatively little has been published concerning the hot file system [of the NCIC]. There have been occasional newspaper articles and television programs on the subject Remarkably, however, there has been no publication or broadcast that has attempted to present a broader view of the NCIC hot file system, describing in detail the types of information maintained in this federal-state cooperative system and the

¹⁴¹ Jon Zonderman, *Beyond the Crime Lab* (New York: Wiley Science editions, 1990), 158.

¹⁴² Van Duyn, *Automated Crime Information Systems*, 4.

¹⁴³ Heberton, *Criminal Records: State, Citizen and the Politics of Protection*, 52.

¹⁴⁴ Daniel Southerland, "Your Prints Will Come -- Any Second Now," *Washington Post*, 10 April 1993, F2.

¹⁴⁵ We want to thank Ms. Bobbi J. Cotter at the Office of Public and Congressional Affairs for a letter she sent on June 3, 1997 in which she writes that: "Presently there are 17 files in NCIC. They include: Article File; Alcohol, Tobacco and Firearms Violent Felon File; Boat File; Deported Felon File; Foreign Fugitive File; Missing Person File; Originating Agency Identifier File; Protection Order File; Securities File; Unidentified Person File; U.S. Secret Service Protective File; Vehicle File; Violent Gang and Terrorist Organizations Files; and the Wanted Person File."

procedures in place to attempt to keep the files accurate, complete and current, and discussing the legal and policy issues arising from the operation of the system and the use of the information obtained from it.¹⁴⁶

Some examples illustrate the discrepancies among published sources regarding the number of files in the NCIC system:

(1) The former Director of the FBI wrote that "Over 19 million records are located in our 12 automated files of criminal justice information."¹⁴⁷ Jon Zonderman reports that, by 1989, the NCIC maintained its records in 12 files.¹⁴⁸

(2) An undated police informational flier entitled "CLETS Communications Network" lists 13 files.

(3) Ekstrand (1993), Quindlen (1991), and Van Duyn (1991) report that the NCIC records are contained in 14 files.

As the list presented by Van Duyn presents the advantage of being descriptive, we use it as framework to outline the national criminal system. At the end of that list, however, we add an outline of the Interstate Identification .

The NCIC's files, as listed by Van Duyn in his book *Automated Crime Information Systems*, are the following:

(1) Wanted Persons

This file, the most used by patrol officers, contained 335,000 records in 1990.¹⁴⁹ The Wanted Persons File "includes identifying information on persons for whom federal warrants, or state warrants for felonies or serious misdemeanors, are outstanding, including parole and probation violators and juveniles who will be tried as adults."¹⁵⁰ In this database, police officers can find descriptive information of wanted persons, such as their names and known aliases, the year of their birth, the offense for which they were arrested, the number of companions at the time of arrest, and a cautious indicator.

(2) Missing and Unidentified Persons

¹⁴⁶ U.S. Department of Justice, Bureau of Justice Statistics, *Criminal Justice "Hot" Files* (Washington, D.C.: GPO, 1986), 2.

¹⁴⁷ William S. Sessions, "The FBI and the Challenges of the 21st Century," *FBI Law Enforcement Bulletin* 58, no. 1 (January 1989) : 2.

¹⁴⁸ Zonderman, *Beyond the Crime Lab*, 158.

¹⁴⁹ David F. Nemecek, "NCIC 2000: Technology Adds a New Weapon to Law Enforcement's Arsenal," *The Police Chief* (April 1990) : 30.

¹⁵⁰ U.S. Department of Justice, Bureau of Justice Statistics, *Criminal Justice "Hot" Files*, 11.

The Missing Persons file was added to the original five databases in October 1975, and the Unidentified Persons file in June 1983.

A. The Missing Persons file

The Missing Person file is composed of the following sections: the Missing Disabled Persons; the Endangered Missing Persons; the Involuntary Missing Persons (such as the victims of abduction or kidnapping); and the Missing Juvenile Persons, who are missing unemancipated persons. The Missing Juvenile Persons count for about seventy-five percent of all missing people reported on the NCIC.¹⁵¹ Deakin and the Department of Justice¹⁵² add a fifth section to this list, catastrophe victims. As of December 1, 1991, the file "contained 73 889 active missing person reports. A total of 42 048 (56.9%) were females and 31 841 (43.1%) were males."¹⁵³

B. The Unidentified Persons file

This file contains information about unidentified dead persons, like their approximate year of birth and of death, their sex, race, height, weight, eye and hair color, and their dental characteristics. In his article analyzing the Missing and Unidentified Persons file, Haglund states that "A high percentage of unidentified remains are decomposed, skeletonized, or otherwise compromised so as to render fingerprinting and recognition of many physical descriptors impossible. At present, 51% of unidentified persons are entered without fingerprint classification."¹⁵⁴

The file contained in December 3, 1991 a total of 2,189 records.

(3) Criminal History and Fingerprint Classification

(4) Stolen and Felony Vehicles¹⁵⁵

This database contains information on stolen vehicles or vehicle parts, and on felony vehicles; like the engine number, the vehicle or aircraft make and year, the vehicle identification number or aircraft license number.

(5) Recovered Vehicles

In this database, there is information such as the date of recovery, the vehicle identification number, and the value of the recovered vehicles.

(6) Stolen and Recovered Firearms

This database contains information like the type of stolen or recovered firearms, their serial number, the dates of theft and of recovery.

(7) Stolen and Recovered Heavy Equipment

(8) Stolen and Recovered Boats and Marine Equipment

¹⁵¹ William D. Haglund, "The National Crime Information Center (NCIC) Missing and Unidentified Persons System Revisited," *Journal of Forensic Sciences* 38, no. 2 (March 1993): 373.

¹⁵² Deakin, *Police Professionalism: The Renaissance of American Law Enforcement*, 249; U.S. Department of Justice, Bureau of Justice Statistics, *Criminal Justice "Hot" Files*, 12.

¹⁵³ Haglund, "The National Crime Information Center Missing and Unidentified Persons System Revisited," 372.

¹⁵⁴ *Ibid.*, 373.

¹⁵⁵ Felony vehicles are vehicles used in the perpetration of a crime.

This file contains information like the date of theft, the registration or document number of the boats and other marine equipment, their length and color.

(9) Stolen License Plates

This database contains information like the originating agency case number, the date of transaction, the date of theft.

(10) Stolen and Recovered Securities

"Stolen securities that can be entered into this NCIC database are serially numbered treasury and U.S. notes, bonds, and bills, municipal and corporate bonds, federal reserve notes, common and preferred stocks, and silver certificates."¹⁵⁶ This database has information such as the case number, the date of issuance and of theft, and the registration number of the security.

(11) Stolen and Recovered Identifiable Articles

This database contains information like the originating agency case number, the value of the articles, the date of transaction, of theft, and of recovery of the articles.

(12) Canadian Warrants

(13) U.S. Secret Service Protective File

This "highly confidential database" protected by a "sophisticated cipher encryption system" was added to NCIC on April 27, 1983. It is the smallest file of the NCIC, with only 61 records in 1986.¹⁵⁷ According to Jon Zonderman, there were "28 names in November 1988 and a high of 85 in 1985."¹⁵⁸ It contains comprehensive histories of people which are considered of danger to American high officials and visiting Heads of States and "it is argued that this file allows tracking of these individuals."¹⁵⁹

(14) Originating Agency Identifier (ORI) File

"The Originating Agency Identifier (ORI), a nine-character code assigned by the FBI to each user agency, is the primary control for accessing NCIC. The ORI controls user agency access to NCIC by identifying each agency to the system and determining the levels of access to NCIC files and types of functions allowed, such as inquiries and requests for records."¹⁶⁰

The ORI file contains information such as the name, address, and phone number of nearly every NCIC law enforcement and criminal justice agency, as well as on certain foreign criminal justice agencies, like Scotland Yard.

(15) The Interstate Identification Index (III, or Triple I)

¹⁵⁶ Van Duyn, *Automated Crime Information Systems*, 14.

¹⁵⁷ Deakin, *Police Professionalism: The Renaissance of American Law Enforcement*, 250.

¹⁵⁸ Zonderman, *Beyond the Crime Lab*, 167.

¹⁵⁹ Heberton, *Criminal Records: State, Citizen and the Politics of Protection*, 51.

¹⁶⁰ U.S. General Accounting Office, *National Crime Information Center. Legislation Needed to Deter Misuse of Criminal Justice Information*, By Ekstrand, Laurie E., Testimony Before the Subcommittee on Information, Justice, Agriculture, and Transportation, Committee on Government Operations, and the Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, House of Representatives, 1993 [on-line]; available from <http://www.cpsr.org/cpsr/privacy/misc-privacy/gao-ncic-abuses-report-1993.txt>; Internet; accessed 22 March 1996.

The Interstate Identification Index is "an existing but unfinished federal database . . . which is a master index of the criminal names stored in state databases."¹⁶¹ It was born out of the desire to eliminate the duplication of criminal history record information in state depositories and in the FBI Computerized Criminal History File. The hope also was that III would "improve the fingerprint identification assistance already provided to those States that request it, and would coordinate an exchange of criminal records throughout the country."¹⁶²

The index contained 10,102,212 records in August 1986 and 20,277,016 records in October 1994. These records are based on the fingerprint cards created at the time of arrest. One card is sent to the state repository where the arrest occurred, while a second card is sent to the FBI Automated Identification System. "If no prior record is on file, the FBI assigns an FBI number and a new record is established in the Identification Division computer. A corresponding index record is also created in the NCIC III identifying the State of origin that will provide the record upon request."¹⁶³ The information received from an III query include the name of the individuals being investigated, along with their criminal history records in state databases, their aliases, place of birth, social security number, scars, fingerprint classification, height, and weight.

The states' participation in the III is optional, and, as of the Fall of 1994, only 29 states had chosen to participate in the Index.

The NCIC 2000

After about twenty years in operation, upgrade of the capabilities of the NCIC became a pressing problem. In 1986, the FBI started its plans to design what is now known as NCIC 2000.

With the NCIC 2000, patrol cars will be equipped with a single-finger mobile scanner and a computer terminal linked to the FBI. The index finger of a suspect will be live-scanned; then the fingerprints will be recorded by the device. The electronic

¹⁶¹ Mitch Betts, "Gun Law Mandates Criminal Database in Five Years," *Computerworld* (6 December 1993): 24.

¹⁶² L. Glasheen, L. "Crime and Politics," *Security Management* 26, no. 1 (January 1982): 67.

¹⁶³ Emmet A. Rathbun, "Interstate Identification Index," *FBI Law Enforcement Bulletin* 54, no. 1 (January 1985): 14.

image of the print will be compressed to one-sixtieth of its original size¹⁶⁴ and sent electronically to the NCIC where it will be matched with the prints stored in the Wanted Person File. Within seconds of the request, information regarding the suspect's criminal history, probation or parole status, his/her aliases, signature, tattoos, etc. will be transmitted back to the police car.

These enhancements to the original NCIC will have a significant impact on law enforcement activity and performance. The probability of positively identifying suspects will be increased and will result in fewer false arrests. Other benefits include the improvement of the capabilities of existing files; the intelligence name-searching; the access to other law enforcement databases; and the access to uniform crime reporting statistics (UCR). Furthermore, NCIC 2000 will also:

support more than 13 million requests per day from some 72,000 users; double the NCIC's current transaction rate to enable the system to handle 82 queries per second and give responses in one to five seconds; provide on-line fingerprint matching capability to perform single-print positive ID against a file of more than 225,000 prints; ensure system reliability of .9995 availability for critical functions.¹⁶⁵

Finally, as the requests to the NCIC will be exchanged from computer to computer, the safety of police officers will be increased. Previously, officers had to "radio an NCIC request to someone with a terminal and they are [were] dependent on that person to accurately translate the oral request into a typed query." In addition, as the messages transmitted will be written on a computer screen, suspects will no longer be able to overhear warning messages about them.¹⁶⁶

¹⁶⁴ Bulkeley, "Police Turn To Databases to Link Crimes," B5.

¹⁶⁵ "Harris Corporation Wins \$47 Million Contract to Upgrade FBI's National Crime Information Center, " *PR Newswire* (19 March 1993).

¹⁶⁶ Terrey H. Quindlen, "Harris Will Overhaul FBI's NCIC," *Government Computer News* (29 March 1993): 1.

CHAPTER 6

THE EXPANSION OF AFIS TECHNOLOGY OUTSIDE LAW ENFORCEMENT

Applications of AFIS by Agencies of the Government

Originally mainly developed for applications in law enforcement, AFIS systems were subsequently recognized as having potentialities for use in other areas where positive identification of individuals was equally important. AFIS technology started to spread when a large variety of AFIS systems became faster, smaller, more flexible, customized, easier to use and more affordable than the ones previously engineered.

Aerospace and defense companies have been working in the field of fingerprinting for years. They have taken advantage of their "experience in integrating large and complex systems" and in developing imaging systems to design and manufacture their own AFIS systems.¹⁶⁷ Other companies created more recently design full AFIS systems or partial equipment that interface with AFIS systems. Such companies sell products not only to police agencies but also to the criminal justice system in general, to other government agencies, and to a wide variety of private purchasers such as corporations, plants, banks, laboratories, hospitals, etc. Non-law enforcement customers attracted to AFIS technology may produce a shift in the AFIS market. The former head of the Identification Division of the FBI, Conrad S. Banner, was prophetic when he stated that "Fingerprint's biggest use will be in the business world."¹⁶⁸

With this remarkable abundance of new customers interested in electronic fingerprinting, the AFIS market is now a lucrative business. The tendency of AFIS technology to expand is reflected in descriptions such as "the burgeoning market for automatic fingerprint verification"¹⁶⁹ or "this exploding market."¹⁷⁰ According to

¹⁶⁷ Scott, "Defense Skills Applied to Biometric ID," 54.

¹⁶⁸ Quoted by Robert A. Bennet, "Refining the Art of Fingerprinting," *New York Times*, 11 November 1987, D10.

¹⁶⁹ "Truly Digital," *The Economist*, 21 May 1994, 94.

¹⁷⁰ William B. Scott, "Defense Skills Applied to Biometric ID," *Aviation Week and Space Technology* 144, (17 October 1994): 54.

Sparrow, the sale of AFIS represents "a billion dollar per year business worldwide."¹⁷¹ The making of live-scan devices in particular is expected to be extremely profitable. That "emerging business . . . could explode to \$750 million in sales in five years from present sales of under \$20 million."¹⁷²

Several government agencies are using AFIS technology to meet their identification needs. Imaging systems designed by Identix, for example, are used at the Internal Revenue Services; the Immigration and Naturalization Service; the Drug Enforcement Agency; the Illinois Department of Children and Family Services; NASA; and the Pentagon. Printrak counts among its customers the social services of a few counties in California. Finally, NEC, through the Western Identification Network, has contracts with agencies such as the Internal Revenue Service; the U.S. Secret Service; and the U.S. Postal Service.

AFIS technology is used by government agencies in a wide variety of applications, such as:

(1) controlling access to government buildings or facilities. AFIS systems compare an incoming print to the prints stored in their memory. Once identified and authenticated, the access is authorized. The same procedure exists when employees or visitors are checking out the place. The use of AFIS systems in these situations helps in the detection of people using a false identity. It also helps in the control and tracking of who is coming in and going out a facility and at what time. AFIS systems can therefore act as a way to check the attendance at work.

(2) controlling the access to data stored in government computer databases.

(3) fighting and deterring fraud in social service departments.

(4) controlling fiscal fraud. The Internal Revenue Service (IRS) decided in 1994 to fingerprint the "professional tax preparers who file electronically. . . . Under the new regulations, originators of electronic returns will have to get their fingerprints taken at a local policy [*sic*] department and submit them to the IRS. The IRS will then return the

¹⁷¹ Malcom K. Sparrow, "Measuring AFIS Matcher Accuracy," *The Police Chief* (April 1994): 147.

¹⁷² Adelson, "Faster, More Accurate Fingerprint Matching," 9.

prints through the FBI, which will compare them with the criminal fingerprint database."¹⁷³

(5) establishing the identity of applicants at the time of the issuance of driving licenses by the Department of Motor Vehicles.

(6) helping Immigration and Naturalization Service (INS) to monitor illegal immigration.

The use of an electronic method to control border is attractive.

The number of legal and illegal aliens presently in the United States, already significant, is growing steadily. The INS currently maintains over 41 million individual alien files ("A file"), and processes over 1 million alien violators a year. In addition, approximately 500 million people are inspected by the INS annually at air, land and sea ports of entry.¹⁷⁴

INS tested and compared the use of different electronic identification systems based on the scanning of the hands, the retina, and fingerprints to speed the entry of the air travelers. The fingerprinting method was not selected because of its law enforcement connotations.¹⁷⁵

The INS and the Border Patrol want to develop electronic fingerprint systems that would contain the records of "known criminals and others of interest to the INS."¹⁷⁶ The OTA states that the Border Patrol envisions checking "aliens apprehended at illegal border crossing points" by performing a first fingerprint check on a small database containing only the fingerprint records of illegal aliens who are serious repeat offenders. If the search results in a hit, a second fingerprint search would be done against state and federal databases.¹⁷⁷

¹⁷³ Kennedy Maize, "IRS Tightens Rules On Electronic Filing," *Newsbytes, Washington - News*, 21 September 1994.

¹⁷⁴ Walter T. Hempel, "INS Offers Investigative Aid," *The Police Chief* (June 1994): 36.

¹⁷⁵ James I. Davis, *Statement Before the San Francisco Social Services Commission Regarding the AFIRM System*, 16 May 1993 [mailing list on-line]; available from cpsr-activists at CSLI.Stanford.EDU; Internet; accessed 29 March 1995.

¹⁷⁶ Steve Johnson, "Someday, Computers May Recognize Your Face," *San Jose Mercury News*, 2 June 1993, 13A.

¹⁷⁷ U.S. Congress, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options*, 21.

AFIS technology has also been used in the framework of special missions in different points of the border between the United States and Mexico, in places like El Paso, Texas in Operation Hold-the-Line and in San Diego, California in Operation Gatekeeper. In the latter which began in 1994, INS used

a new fingerprint computer that employs technology developed by Identix Inc. of Sunnyvale. Using a Windows program, a laser scanner and a mouse, agents are able to immediately see how many times each illegal entrant has been caught trying the same thing before. . . . Eventually, the system will be linked to computers that contain files on 'criminal aliens' - illegal immigrants who have been arrested for crimes in the United States.¹⁷⁸

Another example of the struggle against illegal immigration is the pilot project called the "INS Law Enforcement Support Center" which "will be an investigative resource for law enforcement, linking state and local law enforcement officers with the INS alien data files. The proposed center will operate 24 hours a day, seven days a week, using the National Law Enforcement Telecommunications Systems (NLETS) as a communication link to 65,000 criminal justice agencies."¹⁷⁹

INS files contain valuable pieces of information about aliens, such as their fingerprints, their picture, some biographical information, etc.

A final example of the struggle against illegal immigration is the pilot project called California Identification and was launched in September 1994. This project "enables INS to input fingerprints and background information on criminal alien deportees into the database used by law enforcement agencies statewide. A 'flag' on the alien's file alerts local authorities that they have encountered a prior deportee and instructs them to contact INS. These criminal aliens are then subject to arrest and Federal prosecution or deportation."¹⁸⁰

¹⁷⁸ Ken McLaughlin, "Border Patrol Goes High-Tech," *San Jose Mercury News*, 24 October 1994, 1A.

¹⁷⁹ Walter T. Hempel, "INS Offers Investigative Aid," *The Police Chief* (June 1994): 36.

¹⁸⁰ "Attorney General Announces New Initiatives to Remove Criminal Aliens; Los Angeles County Jail Site of Landmark Pilot Project," *PR Newswire* 22 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 28 May 1995.

(7) There is a large-scale application of AFIS technology to avoid abuses of asylum procedures by multiple applications in the European Union. The text of a convention for the establishment of a central computerized system for the collection, exchange and comparison of fingerprints of asylum applicants, called EURODAC, is currently being discussed in the framework of the European Union. The purpose of EURODAC will be to assist in determining the Member State responsible for examining applications for asylum lodged in one of the Member States of the European Union, pursuant to the Dublin Convention, signed on 15 June 1990 by the Member States. EURODAC will be implemented within the coming years.¹⁸¹

Possible future uses of AFIS technology by other government agencies include application in the control of voter registration and prevention of voting fraud, and in the issuance of passports. Passports may some day contain the digitized fingerprints of their holders. Individuals asking for more than one passport or assuming a false identity would be detected by the system.

Applications of AFIS Technology in the Private Sector

More and more aspects of our daily life are being touched by AFIS technology because the method can be applied to wherever the establishment or the verification of the identity of individuals is required.

How can AFIS technology be used in the private sector?

First, it can be used in the prevention of unauthorized access to data or to control the entry to restricted areas or facilities.

Second, AFIS systems can provide the proof of the identity of a person before allowing a financial transaction. For instance, the Electronic Funds Transfer Association proposed in 1993 to add "customer fingerprints, watermarks or holograms to ATM cards."¹⁸²

Visa International "has looked at fingerprint technology to reduce fraud by assuring positive identification of credit users. A digitized description of a consumer's fingerprint could be imbedded in the card's magnetic strip. When the consumer makes a purchase, the finger could be inserted in a slot in a machine at the register, with the credit card inserted at the same time. The

¹⁸¹ Text approved by Mr. Pascal Steller of the European Commission, Secrétariat Général, Task Force Justice et Affaires Intérieures, Frontières Extérieures, Immigration, Asile.

¹⁸² "Banks Seek Ways to Thwart Bogus-ATM Scheme," *San Jose Mercury News*, 21 May 1993, 3C.

machine would tell the clerk whether the fingerprint matched the information in the card, confirming the customer's identity."¹⁸³

Third, AFIS systems can act as anti-theft devices if they are installed, instead of keys, on cars or to gain access to private houses.

Fourth, AFIS technology is widely used in the background screening for different professions, licenses and permits.

Fifth, The healthcare field can use AFIS technology in many ways.

Fingerprint databases can help in the identification of patients in hospitals, in the detection of medical insurance fraud, and in the access control to medical records. It has also been suggested that fingerprint live-scan technology be used in the identification of unconscious individuals and in the immediate access to their medical history.

A trade brochure published by NEC reports that, in Hamilton County, the director of Cincinnati Health Department sees a potential application of electronic fingerprinting in the maintenance of children's immunization records.

AFIS technology can also be applied in pharmacies in the verification of the identity of both doctors and their patients who fill a prescription.

Finally, digitized fingerprints stored in badges containing also encrypted medical information were used for each of the 7,000 athletes who participated in the Special Olympics World Games in Connecticut in June, 1995. In case of an emergency, the scanning of the badge held around the athletes' neck provided paramedics with immediate access to the medical record of the athlete in need.¹⁸⁴

Sixth, AFIS technology can also help in the establishment of national identity programs.

¹⁸³ Robert A. Bennet, "Refining the Art of Fingerprinting," *New York Times*, 11 November 1987, D10.

¹⁸⁴ «Pitney Bowes Showcases Advanced Technology at 1995 Special Olympics World Games; Veritas™ System Speeds Access to Critical Medical Information on Athletes,» *Business Wire* 29 June 1995 [wire services on-line]; available from [http:// www.infoseek.com](http://www.infoseek.com); Internet; accessed 5 July 1995; and «(PBI) ADVISOR/New Technology Bows at Special Olympics; Pitney Bowes' High Tech Veritas System Provides Instant and Secure Access to Medical Records of Special Olympians,» *Business Wire* 30 June 1995 [wire services on-line]; available from [http:// www.infoseek.com](http://www.infoseek.com); Internet; accessed 5 July 1995.

To illustrate, a contract was signed between Comparator Systems Corporation and a foreign country (not cited) on March 6, 1995.

This contract represents the first biometrically-protected national identification card in the world, and established Comparator as the first biometrics company to be chosen for such widespread use. . . . Comparator units are planned to be placed at police stations and border crossing throughout the country, permitting officials to verify the identity of any citizen by comparing the fingerprints of the individual against his/her national identification card and/or the central database.¹⁸⁵

Seventh, fingerprints can also be digitized on magnetic cards together with other identifying data of the card holder. The so-called "smart cards" can be used for multiple purposes, such as banking transactions, financial services, etc.

The LaserCard produced by Drexler Technology Corporation is a concrete illustration of a card which can store a large amount of information such as texts, X-rays, pictures, digital voice recording, signatures, hand geometry scans and, of course, digitized fingerprints. It is used "as a medical records card by British Telecom in the U.K. and IBM in Hong Kong, as an automobile maintenance records card for Honda, as a medical image storage card in the U.S.A., as a VISX vision/eye surgery control card in five countries, and as a cargo manifest card for the U.S. Army."¹⁸⁶

Eighth, AFIS technology can be applied to the promotion and improvement of child protection.

The issue at stake is important because children are often the victims of neglect, assault, or other abuses. A lot of them just disappear.

The 1990 National Incidence Studies of Missing, Abducted, Runaway and Thrownaway Children in America, (NISMA), conducted for the U.S. Department of Justice, estimated that in 1988 nearly 1.4 million children were reported missing or displaced. At the same time, parents' initiatives such as annual photographs, recording dental statistics, and fingerprinting of children,

¹⁸⁵ "Comparator Systems Corp. Chosen For Use in National Identification Card Project," *Business Wire*, 6 March 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 11 March 1995.

¹⁸⁶ "ADVISORY/LaserCard to Be Demonstrated at Card Technology/Card Security Conference," *Business Wire* 11 April 1995 [wire service on-line]; available from <http://www.infoseek.com>; Internet; accessed 16 April 1995.

show increased interest in taking responsibility for child security and protection.¹⁸⁷

Activists in child abuse prevention and child protection are fighting for the enactment of laws to better protect children. Fingerprint automation is part of the measures proposed to reach their goal. A first illustration is provided by California Assembly Bill No. 2053 aiming at giving parents access to the criminal record of the baby-sitter they hire. "AB 2053, which passed the Senate and the Assembly, would give all parents access to Trustline, a statewide nanny registry that checks names and fingerprints of potential care givers against criminal files and the Justice Department's Child Abuse Index."¹⁸⁸ Another example is the National Child Protection Act signed by Bill Clinton in 1993 which establishes a national database available to child care centers for people indicted and convicted of various offenses such as child abuse, sex offenses and arson.¹⁸⁹ It also establishes "procedures for national criminal background checks for child care providers via fingerprint submissions."¹⁹⁰

Novel applications of AFIS technology in the field of child crime prevention have been pioneered by Diane G. Apa and Drena Rogers. In 1993, Diane G. Apa, founded the National Fingerprint Program for Child Identification in Kirksville, Missouri. The database she created collects, classifies and computerizes children's fingerprints. It also helps parents and law enforcement in their search for missing children¹⁹¹ or in other child victimization issues.

Drena Rogers conceived the Kids Identification Digital System (KIDS) Project. Tested in Temecula, a small community located in Southern California, the project reflects the efforts by parents and their children, law enforcement agencies (the

¹⁸⁷ "SafeCard Launches Child Registration and Search Service; Comprehensive Initiative Addresses Major National Problem," *PR Newswire* 11 April 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 16 April 1995.

¹⁸⁸ "Saving Other Children. AB 2053, If Wilson Signs It, Would Screen Care Givers," *San Jose Mercury News*, 29 September 1993, 6B.

¹⁸⁹ Laws Alone Won't Stop Child Abuse, *San Jose Mercury News*, 29 December 1993, 6B.

¹⁹⁰ U.S. Department of Justice, Federal Bureau of Investigation, *CJIS: Criminal Justice Information Services. A Newsletter for the Criminal Justice Community*, 10.

¹⁹¹ "Computerized Child Fingerprint Repository," *Law and Order* (March 1992): 111.

Riverside County Sheriff's Department and the Temecula Police Department), the Temecula Valley Unified School District and two companies (Eastman Kodak and ANSI, the Applied Network Solutions, Inc.) in their fight against child abduction.

In this project, a database containing digitized identifying information about children from kindergarten through the eighth grade has been created. The pieces of information include the following: the picture of the children, their fingerprints, height, weight, hair color, medical problems, scars, school papers, their art work and the picture of the children's parents or guardians.

The data are stored on CD-ROMs, each one containing the information of about 500 children. "The entire program is software and hardware protected with passwords so only those with proper access will be able to get the data."¹⁹² Other important advantages of the program are that the data can be updated and that PicturePlus, the software used in Project KIDS, offers the capability "to take a digital image and load it into software that makes a person look older."¹⁹³

During the early phase of the project, the Temecula Valley Unified School District board was concerned about the confidentiality of the information they were gathering. So, if police need the information, they must contact the school and ask for it. Second, "In response to privacy concerns, the sheriff's department and the schools agreed early on that the disks themselves would not be released to the authorities."¹⁹⁴ The CD-ROMs are therefore kept by the school or at the district office. However, if a child is reporting missing, the entire set of identifying data is accessible to the police within minutes. The information can be sent electronically to other police departments, and leaflets can be immediately laser-printed and distributed in the community.

Participation in Project KIDS is voluntary and parents sign a release form establishing their desire to participate or not in the project. The form is scanned and

¹⁹² "Digital Imaging Discourages Child Abduction," *Law and Order* (June 1994): 32.

¹⁹³ Ibid.

¹⁹⁴ Ellis Booker, "Digital Photo Bank Aids Missing-Kid Search," *Computerworld*, 28 February 1994.

included in the database. The participation rate was higher than predicted, reaching 97 percent of the parents.

CHAPTER 7
ADVANTAGES OF AFIS OVER MANUAL SYSTEMS
OF IDENTIFICATION IN LAW ENFORCEMENT
Size of Fingerprint Collections and Processing Time

The number of fingerprints gathered for criminal and noncriminal justice purposes is so substantial that it is considered "unmanageable in many states. These workloads have increased to the point that many states have become unable to perform technical fingerprint searches in all criminal cases and only a few states are able to do fingerprint searches for noncriminal applications for employment and licensing purposes."¹⁹⁵ At the federal level, the Identification Division of the FBI bends under the weight of its four floor collection of fingerprint cards. During the National Conference on Improving the Quality of Criminal History Records held in January 1992, the Chief-Legal Counsel of the FBI Identification Division used the month of March 1991 as an example to illustrate the routine activity of the Division. During that month, the Division received about 770,000 fingerprint cards. This represents a daily average of 36,000 cards. In the IAFIS brochure published three years later (1995), the FBI foresaw that this volume would increase with the development of automation.

One of the most vital contributions of AFIS technology to the management of fingerprint cards is its capability to process fingerprint collections of all sizes. A 1995 survey by Professor Peterson indicates that "The design size [of ten print data bases] for all agencies ranged from 60,000 to 9,000,000 ten print cards, with a mean of 902,000 and median of 500,000 records. . . . In terms of actual size of the ten print data bases, the mean is about 739,000 and median is 400,000. Compared with the 1990 survey, this represents an increase of more than 30% in the average ten print data base."¹⁹⁶

¹⁹⁵ U.S. Department of Justice, Bureau of Justice Statistics, *Automated Fingerprint Identification Systems: Technology and Policy Issues* (April 1987), 18.

¹⁹⁶ Joseph L. Peterson and Julie L. Moore, *The Status of AFIS Systems Worldwide: Issues of Organizations, performance and Impact* (revised September 1995). Presented at the International Symposium on Fingerprint Detection, and Identification, (Ne'urim, Israel, June 1995), 11.

The importance of AFIS systems lies not only in the amount of data they can process but also in their speed. Some criminal cases have been solved thanks to AFIS technology, while lengthy manual searches were often tried in vain. In 1985, for example, Richard Ramirez, also known as the California's Night Stalker, was identified in three minutes by the Los Angeles AFIS. Police estimated that it would have taken a fingerprint specialist 67 years to make the same identification manually.

The search time of AFIS systems varies according to the system used and the type of search being done (tenprint to tenprint; unsolved latent against latent; etc.). To illustrate:

- Wilson and Woodard report that average searching time "for a ten-print search (rolled print to rolled print comparison) in a file of under 500,000 is a matter of minutes. For a latent search, the search time averages about one-half hour."¹⁹⁷
- The Massachusetts AFIS can sort 250,000 tenprint cards in three minutes.¹⁹⁸
- CAL-ID does about 650 matches checked per second.¹⁹⁹
- The FBI is working on a computer that "would be able to scan 250,000 prints from a master file of criminals within about 20 seconds;"²⁰⁰
- With its new Series 2000, Printrak announces in a trade brochure that "for the first time, agencies have the tools to perform fingerprint matches in real time."
- The survey by Professor Peterson indicates that the latent print to tenprint database search time is: 15 to 60 minutes for 36% of police agencies that answered the survey; 10 to 15 minutes for 19% of them; 0 to 5 minutes in 18% of them; one hour or more for 15% of the sample; and 5 to 10 minutes for 13% of the sample.²⁰¹

Rapid processing of large amounts of fingerprint cards has valuable consequences in the practice of law enforcement.

¹⁹⁷ U.S. Department of Justice, Bureau of Justice Statistics, *Automated Fingerprint Identification Systems: Technology and Policy Issues* (April 1987), 18.

¹⁹⁸ Berg, *Law Enforcement: An Introduction to Police in Society*, 290.

¹⁹⁹ Van Duyn, *Automated Crime Information Systems*, 36.

²⁰⁰ Michael Tackett, "FBI's Vaunted Fingerprint Files a 'National Resource On Decline,'" *Chicago Tribune*, 23 May 1993, 3C.

²⁰¹ Peterson, *The Status of AFIS Systems Worldwide*, 17.

First, it saves considerable time in fingerprint processing and in identification work. It also helps diminish the backlogs in the cataloguing of fingerprint cards in police departments. At the FBI, "The fingerprint backlog at the end of FY 1995 was over 1,000,000 cards and it continues to grow."²⁰² The implementation of IAFIS will provide a solution to this issue.

Another advantage of AFIS systems is that they make it possible to do daily latent checks, and to periodically re-check latent prints that have not been identified. Two examples illustrate how successful this process can be. First, in 1991, Becklund reported that CAL-ID was doing 280 latent searches a day and that the system turned up 30,000 matches; second, the AFIS used at the Dallas Police helps identify over 1,000 latent prints per year.

Finally, rapid identifications based on a positive identifier increase the safety of police officers who can learn within minutes the identity of a suspect. They can therefore make a better decision about the suspect on the basis of sound data. In addition, the possibility of an improper arrest is reduced, as well as the release of wanted suspects whose identity was not revealed in time.

Automated Processing of Fingerprints

Live-Scan Technology

"Live-scan is an inkless intelligent terminal that records prints by optically scanning a person's fingers and hands."²⁰³ Developed in the 1980s, the technique is used in the direct scanning of the fingers, as well as in the scanning of tenprint and latent cards. The procedure can be performed directly in a crime scene, in a police car, or in any place where a portable scanner can be carried.

The scanned print is displayed on a high resolution screen and its quality can be immediately controlled and improved for each finger separately during the fingerprinting-taking process. This was impossible with the manual method of fingerprinting. If the print quality of one finger was not satisfactory, the entire tenprint card had to be redone.

²⁰² "IAFIS: The Real Story," 2.

²⁰³ "Handwriting on the Wall: Fingerprint Technology Buying Surges in 1995," *Business Wire* 30 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 6 June 1995.

Control of the quality of scanned prints can be achieved in two ways.

First, instructions are displayed on a screen for the operator. The Fingerprint Quality Control Software used for the Identicator Direct Finger Reader System, for instance, displays instructions ensuring the correct placement of the finger on the scanner as well as indications that the image is of bad quality or that the platen surface is dirty.

Second, the quality of the print can also be automatically controlled by the computer itself. For example, the Identix Quality Assurance software is designed to allow police departments to define preset standards before accepting a print. If the standards are not met, the fingerprint is rescanned or the image annotated. In another component of the system, the TouchPrint 600 Live-Scan System, Identix reports using a method that prevents image fogging from moist fingers. A final illustration is the AFIS compatible Direct Finger Reader DFR-90 and DFR-95 built by Identicator Technology which, according to the documentation sent by the company, adjusts to accommodate various skin conditions and finger pressures to provide optimum image quality.

These features have a direct impact on the ability of AFIS systems to process a record, that is, to read and analyze it, and to search through the database for a match. The quality of the prints has a direct effect on the accuracy of a search, which, in fingerprint terminology, is "a measure of the ability of the system to locate a print that is in the data base."²⁰⁴ The accuracy rate of tenprint fingerprint searches increased from 75 percent for manual systems to 97-98 percent for AFIS systems.²⁰⁵

Automated Data Extraction, Storage, Retrieval, and Comparison

When the quality of the image being scanned is accepted, AFIS systems automatically extract the data they need. They then convert or digitize these data, compress them, and store them on optical or on magnetic disks. Once stored, the images can be electronically retrieved on a computer screen. At this point, AFIS

²⁰⁴ U.S. Department of Justice, Bureau of Justice Statistics, *Automated Fingerprint Identification Systems*, by Thomas F. Wilson and Paul L. Woodard, 12. For an analytical study of the concept of accuracy as it pertains to AFIS technology, See Sparrow, "Measuring AFIS Matcher Accuracy," 147-151.

²⁰⁵ U.S. Congress, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options*, 6.

technology provides a solution to three problems in the manual fingerprinting method. First, it decreases the general processing time of fingerprint cards as well as their retrieval time. Second, it solves the problem of prints that used to be misfiled or out-of-file. Finally, it diminishes the storage place needed in the filing of fingerprint records. A vivid example for this last point is provided by the Identification Division of the FBI. Its collection, held in cabinets taking up to 300,000 square feet in Washington, D.C.,²⁰⁶ is expected to be reduced to a 46,500 square foot computer center in West Virginia.²⁰⁷

At the end of the matching process, the incoming print and a print detected by the system are displayed side-by-side for comparison. Technology allows the prints to be rotated on the screen or enlarged so that identifications are performed on a very discriminative basis. Schmitt reports the case of an AFIS that magnifies each image to 25 times. A double cursor, one for each fingerprint, moves in parallel and “can be used to simultaneously highlight corresponding minutiae on the two images. The fingerprint operator examines the similarities and determines if a ‘hit’ has been made.”²⁰⁸

Enhancement of the Prints

The quality of the prints can be improved at two moments.

Whereas live-scan technology improves the quality of the prints when fingerprints are scanned, electronic enhancement techniques improve it after they are taken. The quality of distorted inked or latent prints is enhanced in several ways. Missing sections of the prints can be touched up and edges of the fingerprint ridges can be enhanced. Image enhancement techniques can also correct “breaks in the skeletal pattern, cuts or breaks in the ridges caused by scars or burns.”²⁰⁹ They allow the reconstruction of a print by using methods such as the wavelet analysis. “The procedure first divides an image into its basic constituents. It then pulls out and saves

²⁰⁶ Tackett, “FBI’s Vaunted Fingerprint Files a ‘National Resource On Decline,’” 3C.

²⁰⁷ U.S. Congress, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options*, 33.

²⁰⁸ Judith Blair Schmitt, “Computerized ID Systems,” *The Police Chief* (February 1992): 35.

²⁰⁹ U.S. Congress, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options*, 5.

the constituents that define the image and ignore those that don't contribute information essential to the reconstruction of the image."²¹⁰

A major benefit of enhancement techniques is that they reduce the number of cards rejected because of poor quality. In addition, by allowing automated systems to search for matches with the best data the computer can generate, they increase the probability of finding matches. Finally, the reproduction of very clear prints improves the perception of very fine details and helps fingerprint specialists find irrefutable proofs of hits in courts of law.

The enhancement of a fingerprint was accepted in a court. The *FBI Law Enforcement Bulletin* describes Commonwealth of Virginia v. Knight (CR-90-1353-02-F) as "the first documented case of a *Frye* hearing."²¹¹ An unidentifiable fingerprint found on a pillowcase at the scene of a crime underwent an image enhancement procedure which made it identifiable within four hours. Although defense attorneys criticized the scientific validity of this process, "the court ruled the enhanced print admissible, stating that the process did not alter the actual pattern of the print; it only made it more visible."²¹²

Printing of Fingerprint Images

Electronic scanning produces fingerprint cards of very high quality. Laser-printed cards, in particular, thanks to their high level of resolution, can be easily processed by AFIS systems. Their diffusion will probably result in an increase in the number of arrests by police "because the improved quality of central fingerprint files will better facilitate computerized fingerprint matching."²¹³ Furthermore, as predicted, some police departments experience a decrease in the rejection rate of cards from the

²¹⁰ Elizabeth Pennisi, "Mathematics Aids Fingerprint Detection," *Science News* 142, no. 21(21 November 1992): 350.

²¹¹ The *Frye* Test determines whether a scientific technique has achieved sufficient recognition in the scientific community to become admissible as evidence before a jury. (*Frye v. United States* 293 F. 1013 (DC Cir.) [1923]).

²¹² "Conviction Through Enhanced Fingerprint Identification," *FBI Law Enforcement Bulletin* (December 1992): 16-17.

²¹³ David G. Hall, "New Remote, Interactive Technology Enables Linkage of AFIS Systems," *The Police Chief* (October 1987): 61-62.

FBI to almost zero.²¹⁴ Finally, with AFIS technology, it is now possible to print fingerprint records in various formats. Multiple copies can be made rapidly without losing the original quality of the print.

Electronic Transmission of Fingerprint Images and Database Networking

The advent of technology also brought improvements in the exchange of fingerprint information between law enforcement agencies.

Computer image technology allows for fingerprint images to be electronically transmitted from one system to another, decreasing the speed of that exchange to a few seconds or minutes. With the advances in image compression techniques, instant transmission of information is now possible.²¹⁵

Very complex and sophisticated fingerprint database networks have been established at the local, state, interstate, and federal levels of law enforcement. The most sophisticated state AFIS in the United States is the California Automated Identification System (or CAL-ID), which is run by the California Department of Justice. CAL-ID is "an automated fingerprint matching and identification system that is a nationwide and worldwide model for such high-tech system."²¹⁶ It is the first statewide automated identification network and was planned to provide police departments throughout the state "with remote terminals for conducting computerized fingerprint searches and for retrieval of fingerprint images for hard-copy printout or screen display."²¹⁷ Another highly sophisticated statewide AFIS is the one used by the Texas Department of Public Safety. According to a pamphlet published by NEC, its manufacturer, the system supports fingerprint identification for all 254 counties and includes 59 remote terminals.

²¹⁴ Pilant, "Image Processing Technology," 45.

²¹⁵ "Printrak Gives Law Enforcement Agencies On-Site Identification Capability for the War Against Crime," *Business Wire*, 9 March 1994 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 14 March 1994.

²¹⁶ Van Duyn, *Automated Crime Information Systems*, 30. Van Duyn describes with some details CAL-ID's two identification databases, its multilevel network and its three subsystems (Van Duyn, *Ibid.*, 34-43).

²¹⁷ Hall, "New Remote, Interactive Technology Enables Linkage of AFIS Systems," 61.

The first interstate automated fingerprint identification system in the United States is the Northern Virginia Regional Identification System (NOVARIS) which began operation in April 1984. It originally linked six Northern Virginia jurisdictions (the counties of Fairfax, Arlington, and Prince William; and the cities of Alexandria, Falls Church, and Fairfax). On February 14, 1985, it was linked to the automated systems of two other states, respectively to DCAFIS, the AFIS of the Washington, D.C. Metropolitan Police Department; and to RAFIS, the AFIS of Montgomery and Prince George's Counties in Maryland.

A second example of an interstate network system is the Western Identification Network, Inc. (WIN) which became operational in 1989 and might soon include all the Western states. According to a police informational flyer dated January 1993, (1) WIN's Central Site Members are Idaho, Montana, Nevada, Oregon, Portland, Utah and Wyoming; (2) WIN's Interface Members are Alaska, California and Washington; and (3) the Federal Members of the network are the U.S. Secret Service, the U.S. Postal Inspection Service, and the U.S. Immigration and Naturalization Service. Remote subsystems and booking terminals are installed throughout these states. WIN is able to process "24,240 arrest cards and 4,500 crime scene latent prints per month against a database of 1.3 million criminal fingerprint records."²¹⁸ These numbers are slightly different than the ones reported one year later by Van Duyn who writes that WIN is able to process 18,000 arrest cards and 3,400 latent prints per month against 1.4 million fingerprint records.²¹⁹ The out-of-state hit rate produced by WIN proves the value of the concept of interstate networking. NEC reports that the general out-of-state hit rate of the network exceeds thirty percent, while Van Duyn observes that the concept was particularly successful for Wyoming. Indeed, "42 out of the state's 70 tenprint hits were from neighboring states - a 60% out-of-state hit rate."²²⁰

Finally, the concept of nationwide networking between law enforcement agencies is illustrated by the NCIC 2000 which has been outlined earlier.

²¹⁸ "WIN: AFIS Technology for Rural States," *FBI Law Enforcement Bulletin* (November 1990): 25.

²¹⁹ Van Duyn, *Automated Crime Information Systems*, 123.

²²⁰ *Ibid.*

Fingerprint database networking through all the levels of law enforcement greatly increases the probability in making identifications. Investigators are no longer limited to their own jurisdiction, but they can submit requests for identification in law enforcement agencies located all around the nation. This ability to share and exchange online fingerprint information at a high speed and at long distance encourages a closer cooperation between law enforcement agencies.

Identification

Frequently, suspects are unwilling to identify themselves to the police or they give a false identity. Police reports can also contain wrong pieces of information about the identity of a person because of clerical errors. In consequence, the identification of suspects can be a major preoccupation.

A turning point to this issue came with the advent of AFIS technology. As AFIS-based identifications rely on the unique characteristics found on the fingertips of a person, if the suspect is in the database being searched, his positive identity will be established regardless of his silence or of his false declarations.

The advantages of this are clear; they are discussed in more detail in Part Three.

AFIS technology helps in the detection of aliases and in the establishment of accurate and reliable databases based on positive identifiers. AFIS also reduces missed identities and of wrong arrests.

The determination of the identity of criminals who leave latent prints on the scene of a crime is also a crucial issue.

It has been known that, for decades, one of the major reasons for which latent prints were underutilized was that their process was based on the knowledge of a suspect. Not surprisingly, the introduction of AFIS technology totally modified this approach by offering the extraordinary possibility to conduct large-scale cold searches of latent prints. The capability of AFIS systems to solve these “otherwise unsolvable crimes” is cited by the largest number of police agencies as their principal impact on the department since their implementation.²²¹

A few numbers illustrate the regained value of latent prints:

²²¹ Klug, *Automated Fingerprint Identification Systems*, 52.

- At the Washington, D.C. Police Department, before the implementation of AFIS, "only four cases on cold searches were made. The department is now making 100 cases per month on cold searches."²²²

- Within the five years following its implementation, the AFIS used by Milwaukee, Wisconsin, Police Department reached 37 percent identification on unknown latent prints.²²³

- When CAL-ID went online, "officials ran prints from 400 unresolved Northern California homicides and matched prints with suspects in 75 of these cases, leading to 39 arrests."²²⁴

Old cases can now be solved thanks to AFIS technology.

The investigation of the murder of Thora Marie Rose, a 45 year old waitress, which occurred in Los Angeles on October 3, 1963, is particularly enlightening of the benefits of electronic systems. The fingerprint specialist delegated to the crime scene was able to record 36 fingerprints of the murderer. Unfortunately, despite the manual review of over 30,000 sets of prints in Sacramento, no match could be found. In December 1990, the fingerprints of the criminal were run in an AFIS containing more than one million prints and were matched with the ones of Vernon Robinson. Charged with first-degree murder, he was sentenced to life in prison.²²⁵

This case - maybe the oldest solved by AFIS technology - illustrates the way high technology becomes a new tool for justice. It can help police find the key to unsolved crimes, sometimes before they reach the statute of limitations.²²⁶ This is an immense task in itself if one considers that there were about 40,000 unsolved

²²² Carol D. Buraker, and William K. Stover, "Automated Fingerprint Identification: Regional Application of Technology," *FBI Law Enforcement Bulletin* (August 1984): 5.

²²³ Schmitt, "Computerized ID Systems," 35.

²²⁴ Becklund, "Crime Computer is a Help, but Can't Do It All," A31.

²²⁵ Ibid.; "Print Match After 30 Years Puts Finger on Murder Suspect," *San Jose Mercury News*, 12 September 1993.

²²⁶ Raymond Fjetland and Charles Robbins, "The AFIS Advantage: A Milestone in Fingerprint Identification Technology," *The Police Chief* (June 1989): 22.

homicides between 1985 and 1993 - of which only 7,000 were recorded in the FBI database for unsolved murders.²²⁷

Finally, the new value of latent prints affects the dynamics of police work.

Fjetland and Robbins examined this issue and observed that more identifications increase the workload in police departments. The study by Klug et al. confirms this observation.²²⁸ Second, the authors point out that the role of identification officers is more important than before, and that, because the probability to identify a criminal has increased by much, these officers feel a better motivation in doing their job. Lastly, they observe that there is more training in crime scene preservation.²²⁹

²²⁷ Bulkeley, "Police Turn To Databases to Link Crimes," B5.

²²⁸ Klug, et al., *Automated Fingerprint Identification Systems*, 51.

²²⁹ Fjetland, "The AFIS Advantage: A Milestone in Fingerprint Identification Technology," 22.

PART THREE

ELECTRONIC FINGERPRINTING

SELECTED ISSUES

INTRODUCTION

The advent of AFIS technology has introduced unprecedented and revolutionary changes in the global handling of fingerprints. It brought remarkable improvements in the field of fingerprint-based identification and it is contributing to the restructuring of criminal justice records management. As a result of its success, intensive industrial research aimed at further enhancing its capabilities is ongoing and there is now a consistent trend towards the continuous diffusion of the technology not only in additional police departments, but also, besides law enforcement, in several agencies of the government and in the private sector.

The qualities of modern AFIS systems are: powerful, effective, reliable, extremely fast, user-friendly, etc. For all these merits, however, the implementation and/or the adoption of electronic fingerprinting systems by police raise a number of questions and issues. For example, the choice of an AFIS system should result from a careful analysis of factors such as its compatibility with other systems, its cost, flexibility, reliability, and the security it provides against various threats. However, Dr. Malcom K. Sparrow from Harvard University thinks that "Very few [police] departments have the in-house technical knowledge to compare the accuracy and reliability of different systems. They remain hostage to a variety of misleading performance measures devised by vendors."²³⁰ As a consequence, compatibility between AFIS systems of neighboring jurisdictions is often the main criterion of selection of a vendor.

Compatibility between computers is, as a matter of fact, "essential for efficiency and effective use of resources in the field of law enforcement."²³¹ This comment, written in the context of the computerization of data in the general field of international cooperation in criminal justice and in criminal investigations is also relevant to the narrower field of AFIS technology in the U.S. When AFIS technology was first implemented, there was a lack of compatibility between the systems designed by miscellaneous manufacturers. In response to the impossibility of communication between systems of different makes, agencies of the government worked to establish

²³⁰ Malcom K. Sparrow, «Information Systems: A Help or Hindrance in the Evolution of Policing?» *The Police Chief* 58, no. 4 (April 1991): 32-34.

several image transmission standards. They developed for instance in December 1986 the ANSI/NBS-ICST 1-1986 *American National Standard for Information Systems - Fingerprint Identification - Data Format for Information Interchange* which was later revised to become the ANSI/NIST-CSL 1-1993 *Data Format for the Interchange of Fingerprint Information Standard*. This last standard "defines the content, format and units of measurement for the exchange of information that may be used in the fingerprint identification of a subject. The information consists of a variety of mandatory and optional items, including related record data, digitized fingerprint information and compressed or uncompressed fingerprint images."²³² The evolution of AFIS technology made the issue of compatibility between systems less of an issue than it had been. "Data exchange between systems will be achieved by concentrating on the exchange of grey-scale images . . . rather than through exchange of the subsequently extracted minutiae data."²³³ New types of standards have therefore been adopted. Among them is the FBI Wavelet/Scalar Quantization (WSQ) Fingerprint Image Compression Standard (IAFIS-IC-0110) which is an algorithm for the transmission, storage and compression of grey-scale fingerprint images.

Another determinant factor in the acquisition of an AFIS is its cost. Greguras and Sykes examined the possible application of AFIS technology as a means to secure identifications in electronic fund transfer (EFT) systems. Considering the heavy cost of AFIS technology in 1980, they wrote that "This expense can only be justified for protecting bank vaults, important military computing systems, or other highly valued assets, and is simply not cost justified in an EFT setting."²³⁴ However, the cost of the technology has decreased in twenty years and AFIS technology is now applied to some EFT transactions.

²³¹ John C. Johnson, International Co-operation and Mutual Assistance: The Use of Computer Technology; in Richard Scherpenzeel, *Computerization of Criminal Justice Information Systems* (The Hague: Helsinki Institute for Crime Prevention and Control, 1992), 197.

²³² «New Fingerprint Standard Approved», *Government Imaging* (July 1994): 14.

²³³ Sparrow, «Information Systems,» 34.

²³⁴ Fred M. Greguras and David J. Sykes, Authentication in EFT: The Legal Standard and the Operational Reality, *The Computer Law Journal*, vol. 2, 1980, 76 and 78.

The same situation happened in law enforcement. Because of their high cost, AFIS systems were mainly implemented at federal agencies, state identification bureaus and large police departments. However, with time, factors such as the increasing need for better identification tools and the availability of the technology at a more affordable cost led police departments of smaller size to find innovative ways to fund their AFIS system. Apart from using government funds or leasing the machine, some departments spend the money confiscated in drug busts to make the purchase.²³⁵ Network sharing of fingerprint data also helps small departments to alleviate the significant expense. The savings resulting from a joint purchase can be substantial. For example, in the case of the Northern Virginia Regional Identification System which was "the first locally funded, regional, automated fingerprint identification system in the United States,"²³⁶ the collective savings for the three automated systems linked in one network was estimated at \$4.5 million.²³⁷

Even if the cost of an AFIS system is substantial, most of the authors recognize that the advantages of AFIS are worth the investment. Fjetland and Robbins are particularly convinced of this point when they write that "Although the AFIS is a big-ticket item, it represents a one-time expense that increases the productivity of both the police and sheriff's identification departments - which would otherwise be impossible without hiring more staff. The cost effectiveness of the AFIS becomes apparent when compared with the cost of increasing the identification staffs to the level necessary to equal the current productivity rate."²³⁸ It should however be pointed out that, contrary to the statement of the two authors, the purchase of an AFIS system is not "a one-time expense." Additional costs include operational expense such as the training of AFIS operators, the hardware and software maintenance costs, the cost related to the time invested in the conversion of manual to electronic data, etc.

²³⁵ Mallory, «Electronic Fingerprinting Technology,» 117.

²³⁶ Folsom, «Automated Fingerprint Identification Systems,» 27.

²³⁷ Buraker, «Automated Fingerprint Identification,» 5.

²³⁸ Fjetland, «The AFIS Advantage: A Milestone in Fingerprint Identification Technology,» 22.

A last illustration of some issues faced by management during the implementation and/or the adoption of an AFIS system is manpower. Some police departments experience either a lack of personnel to enter fingerprint information into a new AFIS system, or a lack of personnel to process old cases. Becklund and Rohrlach argue that many unsolved murders in Los Angeles will not be solved by AFIS technology because LAPD does not have the manpower to remove the unsolved cases from the Department's archives, to find usable prints and to feed them into the AFIS system. It is therefore obliged to turn down the requests of past murders' relatives who wish to have the prints found at crimes scenes run into the automated system. As a consequence, LAPD is developing policies as to which unsolved cases are to be put in priority in the AFIS.²³⁹

In addition to administrative and technical problems, some issues, more profound, are likely to affect record subjects, that is, the individuals whose fingerprints have been digitized and stored in an AFIS system. At the heart of the debate is the fact that fingerprint records can be linked to networks of personal information which, for a large part, reflect decisions made by individuals in various social situations, like getting a driving license, working for the government or for high-security companies, committing a criminal act, requesting some help from the government, etc. Segments of people's life are therefore stored in several government or private databases and their fingerprint records become a pointer to the information they contain. This is the origin of serious concerns for groups for which the implications of submitting to AFIS technology has the potential of becoming prejudicial. Part Three, which presents an overview of important issues, focuses on two such groups: the individuals with a criminal record and the individuals on welfare.

Organization of Part Three

Chapter 8 describes instances where AFIS technology highlights and magnifies issues that were present and known long before the automation of criminal records begun within the criminal justice system. It establishes the relationship between fingerprint records and criminal history records and discusses major consequences

²³⁹ Laurie Becklund and Ted Rohrlach, «Crime Computer Is a Help, but Can't Do It All,» *Los Angeles Times*, 5 January 1991, A31.

deriving from the use of criminal records for criminal and noncriminal justice purposes. Finally, it examines the possible impacts AFIS technology has on social issues.

Chapter 9 describes an instance where AFIS technology raises new questions, new challenges because it is used in a prototypical way in a situation where it is perceived as intrusive, authoritative or as a form of control by the government. Specifically, it focuses on issues generated by AFIS technology in the framework of its application to the welfare system.

Chapter 10 presents a summary of the study and its general conclusions.

CHAPTER 8

FINGERPRINTS AND CRIMINAL HISTORY RECORD INFORMATION

Criminal History Records Used Within the Criminal Justice System

Fingerprint searches are used by police to perform two functions – to verify or confirm the identity of a person;²⁴⁰ and to determine whether the person has a criminal history record.

Criminal history record information is the “information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detention, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.”²⁴¹

Identification record information constitutes another of several types of criminal justice data, and it is defined as the “fingerprint classifications and other physical descriptive data concerning an individual to the extent that it does not include any indication or suggestion that the individual has at any time been suspected of or charged with criminal offense.”²⁴²

Criminal history records are important in more than one respect. In addition to reflecting a propensity to criminality, they also show that the person is willing to risk the consequences of criminality. Finally, they may also be indicative of a possible future misconduct.²⁴³

²⁴⁰ A brief description of the way the manual processing of fingerprints works in identification bureaus of criminal record repositories can be found in U.S. Department of Justice, Bureau of Justice Statistics, *Automated Fingerprint Identification Systems: Technology and Issues*, April 1987, by Thomas F. Wilson and Paul L. Woodard (Washington, D.C.: GPO, 1987). A detailed description of the automated fingerprints process at the FBI is the object of the chapter entitled “Organizational Components of the FBI Identification Division,” in U.S. Department of Justice, Federal Bureau of Investigation, *The Identification of the FBI. A Brief Outline of the History, Services and Operating Techniques of the World’s Largest Repository of Fingerprints* (Washington, D.C.: GPO, 1991).

²⁴¹ 28 C.F.R. §20.3 (b).

²⁴² SEARCH Group, *Standards for the Security and Privacy of Criminal History Record Information*, (Sacramento, CA, 1988), 8.

²⁴³ U.S. Department of Justice, Office of Legal Policy, *Report to the Attorney General: the Admission of Criminal Histories at Trial*, August 14, 1986, 11-12.

From the criminal justice perspective, criminal history record information is “the informational thread that weaves together the functions performed by law enforcement, prosecutors, defense, courts, corrections, probation and parole.”²⁴⁴

At the federal level, fingerprint records and criminal history record information form the Department of Justice criminal history record information system, which is defined as the “Identification Division and the Computerized Criminal History File system operated by the Federal Bureau of Investigation.”²⁴⁵ Further in the law, in 28 C.F.R. §20, “Appendix to part 20,” Subpart C-§20.31, the relationship between fingerprints and criminal history records is well-established. “Each state having a record in the Computerized Criminal History (CCH) file [of the FBI] must have a fingerprint card on file in the FBI Identification Division to support the CCH record concerning the individual.”

The importance of the relationship between fingerprints and criminal history records at the state level is stressed in a report submitted by a National Task Force whose goal was to propose a model for the improvement of the reporting of disposition of criminal history record information to state central repositories:

The forwarding of fingerprints to the repository is a critical step in creating a record of the arrest or case cycle in the criminal history database, since it provides (1) a means of legally-sufficient positive identification of the offender and (2) a means of assuring that the new case will be associated with any prior arrests and prosecutions of the offender in a complete criminal history record. For these reasons, every state criminal history record except one is currently fingerprint-based; that is, case cycle are included on the criminal history record only if based upon fingerprint identification.²⁴⁶

Once the identity of an individual is established and his or her name is linked to a criminal history record, officials from each component of the criminal justice system can make recommendations and decisions about the record subject on the basis of the information held in the record.

²⁴⁴ Search Group, Inc., *The American Criminal History Record* (Sacramento, CA, 1976), 1.

²⁴⁵ 28 C.F.R. §20.3 (j).

²⁴⁶ U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Report of the National Task Force on Criminal History Record Disposition Reporting* (Washington, D.C.: GPO, 1992), Appendix 5-2.

During their investigations - described as “a search for information that will help police officers to make a decision on a suspect, arrestee and the person they would wish to see prosecuted before the courts,”²⁴⁷ - police gather, use and, more importantly, they rely on the information they receive from local, state or federal police resources to make decisions about the record subject. For instance, they learn if there is a warrant issued against a suspect and they can therefore infer whether the suspect in question is likely to be armed and dangerous, whether he/she should be interrogated, arrested, released, etc. In other words, thanks to the information contained in the records they consult, police officers can foresee the reactions of a suspect and act accordingly.

In the judicial system, prosecutors use criminal history record information along with other criminal justice information to decide whether charges should be brought against a defendant as well as to determine the appropriate charges. They are also used in negotiating plea-bargaining and in recommending pre-trial release conditions, bail and sentencing. Judges use criminal justice records in setting bail and in determining sentences. Based on the examination of a defendant's prior conviction record, bail can be denied, pre-trial release conditions and sentences can be more severe.

In the correction system, correction officers use criminal justice history records in the determination of the level of security and of supervision to be administered to the prisoners. Probation officers and parole board members rely in part on them in their recommendations and decisions about the incarceration or the eligibility for parole. Finally, criminal records are also used in court cases preparation, jury selection and witness verification.

Criminal Records Used For Noncriminal Justice Purposes

The expression “noncriminal justice requests” refers to the background checks conducted for noncriminal agencies of the government, for private employers, financial and insurance companies, schools, etc. to control or verify the integrity of applicants to several licenses, jobs, and permits.

A study conducted by the Bureau of Justice Statistics indicates that more than half of all requests to some state repositories for criminal record information is made

²⁴⁷ Heberton, *Criminal Records: State, Citizen and the Politics of Protection*, 67.

by noncriminal justice agencies. The same study reports the findings of a national survey published in 1989 revealing that the State criminal record repositories are handling about 2,000,000 noncriminal justice access requests a year.²⁴⁸ The increase in background checks fuels the ongoing debate regarding the right by the noncriminal justice community to access criminal records in order to make noncriminal justice decisions. Electronic fingerprinting technology seems to worsen the discussion:

As fingerprint matching becomes a more powerful tool of criminal identification and as matching from large files becomes faster and easier, there will be increasing pressure to expand the search capability of law enforcement agencies. For example, government employees, military personnel, and juveniles are routinely fingerprinted for reasons having nothing to do with crime. Controversy is likely to develop over whether fingerprints that were collected for noncriminal purposes should be included in files that can be searched by law enforcement agencies.²⁴⁹

This issue, because of the complexity of its ramifications, could be the topic of another paper.

At the FBI, the number of requests for noncriminal justice purposes is higher than the number of requests for criminal justice purposes. In 1970, only 13,000 sets of fingerprints out of a total of 29,000 sent one day to the Federal agency came from law enforcement agencies. "The remaining 16,000 sets were sent in by banks, insurance companies, government employers (municipal, county, state, and federal), licensing agencies, and the like. In return, these agencies received from the FBI any information it had in its files on the 29,000 persons whose prints came in that day."²⁵⁰ A more recent report indicates that "Noncriminal justice fingerprint checks account for about half of all Ident fingerprint activity."²⁵¹

²⁴⁸ U.S. Department of Justice, Bureau of Justice Statistics, *Report on the National Task Force on Criminal History Record Disposition Reporting*, Appendix 2-4.

²⁴⁹ Michael D. Lyman, *Criminal Investigation: The Art and the Science* (Englewood Cliffs, NJ: Regents/Prentice Hall, 1993), 144.

²⁵⁰ Aryeh Neier, *Dossier: The Secret Files They Keep on You* (New York: Stein and Day, Publishers, 1974), 94.

²⁵¹ Congress of the United States, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options. Background Paper* (Washington, D.C.: GPO, 1991), 19.

During the 1980s, there was a slight increase in the total number of fingerprint checks from State and Federal agencies. The number increased from 3.7 million in 1981 to about 4.1 million in 1990. The increase of federal requests went “from 2.1 million (about 8,400 per day) in fiscal year 1980 to 2.3 million (about 9,200 per day) in fiscal years 1989 and 1990. Most of them were for employment and security purposes. Federal agency officials expect no significant baseline growth during the 1990s, since the Federal civilian workforce is unlikely to grow, and the Federal defense workforce may actually shrink.”²⁵²

Among the federal agencies using the services of the Identification Division of the FBI, are the Census Bureau, the Federal Aviation Administration (FAA), the Secret Service, the Department of Defense (DOD), the Office of Personnel Management (OPM) and the Central Intelligence Agency (CIA). The main users of the Division are the Defense Investigative Service (DIS), the Office of Personnel Management (OPM) and the Immigration and Naturalization Service (INS) which “collectively account for about 90 percent of all Federal noncriminal justice fingerprint checks” in their respective background search on people seeking DOD clearances, on Federal civilian employees, and on the people who want to become U.S. residents, naturalized citizens or who are seeking asylum.²⁵³

The increase in the number of noncriminal requests is explained in part by the enactment of state and federal laws requiring background checks for a growing number of professions and licenses.²⁵⁴ This trend was accompanied by a dramatic parallel increase in the number of requests for expungements and reviews of records.²⁵⁵ One can assume that these requests are a reflection of what Marchand calls the “social costs” or the “record discriminations” of having a criminal record.

²⁵² Ibid.

²⁵³ Ibid., 19-20.

²⁵⁴ Examples of such state statutes enacted in California, Illinois, Connecticut, Iowa, and the States of Virginia and Washington are described in the U.S. Department of Justice, Bureau of Justice Statistics, *Public Access to Criminal History Record Information*, by Robert R. Belair, Criminal Justice Information (Washington, D.C.: GPO, 1988), 25-27.

Central to Marchand's opinion is "the controversy over the use of criminal justice records to deny individuals the benefits and services of our society."²⁵⁶ First, when they have a criminal history record, people can be denied various licenses, such as permits to carry a firearm, or licenses to practice a certain number of professions. People can be prevented from participating in educational programs and from being part of the armed forces. Individuals with an arrest or a conviction record can also be denied financial benefits such as credit, loans or some insurance. Furthermore, arrest or conviction records could be used, around 1980, as a basis for "nondesirability" in some public housing in New York City. Another author wrote in the early 1970s that a criminal record held by one person could also affect the desirability status of other members of a family.²⁵⁷

A last case of record discrimination concerns employment determination. Background checks providing information on arrests and convictions of applicants are particularly important for employment involving trust or money, like high security jobs, jobs with children, or in financial institutions. The obvious rationale lies in the nature of criminal records which are seen as pointers to possible future misbehaviors that can negatively affect a company. Furthermore, "employers worry over hiring convicted criminals not only because they might steal from them, but because of possible lawsuits from clients victimized by these criminals. An area of liability becoming more prominent in lawsuits is negligent hiring."²⁵⁸

To sum up, the significance of criminal history records is a function of the judicial and social consequences they may have for an individual. Fingerprint record

²⁵⁵ U.S. Department of Justice, Bureau of Justice Statistics, *National Conference on Improving the Quality of Criminal History Records: Proceedings of a BJS/Search Conference* (Washington, D.C.: GPO, 1992), 31.

²⁵⁶ Donald A. Marchand, *The Politics of Privacy, Computers and Criminal Justice Records: Controlling the Social Costs of Technological Change* (Arlington, VA: Information Resources Press, 1980), 96.

²⁵⁷ Neier, *Dossier: The Secret Files They Keep on You*, 106-107.

²⁵⁸ Tony Lesce, *The Privacy Poachers: How the Government and Big Corporations Gather, Use and Sell Information About You* (Port Townsend, WA: Lompanics Unlimited, 1992), 18.

searches, considered as a key to open these records, are therefore trigger mechanisms that can affect millions of people, criminals or not, in their daily life.²⁵⁹

Selected Issues

Extensively used for criminal and noncriminal justice purposes, the importance of criminal records cannot be overstressed because of the serious impacts they have for the record subjects and, to a larger extent, to society in general. One would presume that their routine consultation by police, their recognition as valuable identification tools, and their common acceptance by the public are all factors guaranteeing that they constitute a foolproof system of information on the basis of which informed decisions are made about the record subjects. Yet, certain weaknesses of the criminal record system undermine public confidence in this system of reference. Some of these weaknesses, which will be briefly overviewed, include: (1) the occurrence of cases of mistaken identities; (2) questions about the quality of criminal records; and (3) concerns about the improper use of criminal records. Underlying their description, the question is: What is the effect, if any, of AFIS technology on these issues?

Mistaken Identities

The check of a criminal record and all the consequences deriving from that control must pertain to the person under investigation. However, evidence points to the fact that cases of mistaken identities do occur.

Two kinds of mistaken identities can be identified. *False negative* situations refer to searches where an existing criminal record is not found - maybe because the record subject used an alias or because he/she used someone else's name. On the other hand, in *false positive* situations, the correct name of a record subject is found but it does not refer to the right person. This happens for example when two people have the same name. False positive situations can be caused by "the careless use of

²⁵⁹ For detailed statistical information regarding the number of people having a criminal record, see U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Survey of Criminal History Information Systems, 1993, With Supplementary Information on Presale Firearm Checks, 1994* (Washington, D.C.: GPO, 1995).

a database,²⁶⁰ i.e., by name-only searches or by searches conducted on the basis of other identifiers, such as social security numbers, that are not entirely reliable.

It is important to stress that identifiers can be divided in three categories according to the probability they provide in asserting identities. The less reliable identifiers are the *informative identifiers*. They have “only marginal and confirmative value in establishing the identity of the individual in question.”²⁶¹ The best chance to establish a positive identity is provided either by the presence of several *conditional identifiers* or by the presence of two *absolute identifiers* which “constitute a high probability that the person sought has been identified. A match of two of the absolute identifiers, for example, fingerprints and eyeball pattern, would constitute virtual certainty that the match is unquestionable.”²⁶²

Attempts to find a remedy to the occurrence of cases of mistaken identities have led to various legal initiatives requiring the use of reliable identifiers. For instance, “the model bill of the National Conference of Commissioners on Uniform State Laws (NCCUSL) requires public requesters to submit either fingerprints or at least two pieces of identifying information required by the repository.”²⁶³

Another example is the third edition of “Standards for the Security and the Privacy of Criminal History Record Information” published by Group Search in 1988. The Standard 10.1 about the Positive Identification of Record Subjects reads as follows: “Except as permitted in Standard 10.2, criminal justice information, except criminal intelligence and investigative information, shall be available only on the basis of positive identification of an individual by means of fingerprints or other equally reliable means.”²⁶⁴

²⁶⁰ Michael W. Klein, “A Case of Mistaken Identity,” *Newsweek*, 19 December 1994, 20.

²⁶¹ Robert J. Rieder, *Law Enforcement Information Systems* (Springfield, IL: Charles C. Thomas Publishers, 1972), 91-92.

²⁶² *Ibid.*

²⁶³ U.S. Department of Justice, Bureau of Justice Statistics, *Public Access to Criminal History Record Information*, by Robert R. Belair, 51.

²⁶⁴ SEARCH Group, Inc., *Standards for the Security and Privacy of Criminal History Record Information*, 20.

AFIS and Mistaken Identities

With the advent of AFIS technology, the general field of fingerprint-based identification acquired a new dimension. A review of the relevant literature suggests that the adoption of AFIS technology in law enforcement departments is usually followed by a higher degree of precision, accuracy, reliability and speed in the positive identification of the individuals being checked. A correct identity based on fingerprints is guaranteed, and common problems - such as the refusal of suspects to communicate their identity to the police or the use of official documents (like driving licenses) that are "easily and often faked"²⁶⁵ - do not interfere anymore with the identification process. It is therefore not surprising that the factual improvement in fingerprint-based identifications is the determinant factor in the acquisition of an AFIS system. More precisely, the main reasons for police authorities to purchase an AFIS system are, by order of importance, their desire: (1) to improve ten-print identification; (2) to improve latent print identification and the identification process in general; and (3) to keep up with the latest technological advancements.²⁶⁶

What are the drawbacks and the positive impacts of AFIS technology on the issue of mistaken identities?

One limitation with the electronic fingerprinting is that it is possible for AFIS systems not to detect a print stored in the computer. This can happen because of factors "including errors in data entry, classification, filing, and comparison, as well as errors in the search algorithm and scoring system."²⁶⁷ Another factor is that the long list of suspects generated in some cases by AFIS systems can discourage the investigators and can prompt to the establishment of particular policies that can affect the end-result of a search. "For example, the department might specify that only the top three matches be included in an investigation of suspects."²⁶⁸ Finally, the entire

²⁶⁵ Gordon Witkin and Ted Gest, "Gun Control's Limits," *U.S. News and World Report*, 6 December 1993, 26.

²⁶⁶ Peterson, *The Status of AFIS Systems Worldwide*, 6.

²⁶⁷ U.S. Department of Justice. Bureau of Justice Statistics. *Automated Fingerprint Identification Systems*, 12

²⁶⁸ Edward Ratlege and Joan E. Jacoby, *Handbook on Artificial Intelligence and Expert Systems in Law Enforcement* (New York: Greenwood Press, 1989), 25.

fingerprint-based process relies and depends on the AFIS matcher accuracy and on the quality of the images fed in the system - both factors being, to a certain extent, interdependent.

Malcom Sparrow observes that AFIS systems matching accuracy is difficult to measure and he lists a series of conceptual and measurement errors that prevent its assessment. By way of illustration, he notes that AFIS users tend to calculate the "overall number of hits, expressed as a percentage of the number of searches undertaken. Thus, they do not distinguish searches that are unsuccessful because of matcher inaccuracy from those that are unsuccessful because there was no matching file print in the data base."²⁶⁹ He also points out the fact that, when comparing a new print to the ones stored in an AFIS system, fingerprint matchers should be able to handle unavoidable spatial and topographical distortions existing between the two sets of prints. Sparrow refers to distortions occurring either to the geometry of the print (such as the digitalization of a print that has been rotated by a few degrees) or to the ridges of the fingerprints (such as the appearance or disappearance of scars, burns, dry-skin cracks, etc.).

As for the question of the quality of the print, despite increasingly sophisticated methods conceived to obtain prints of the best quality, technical problems can still be present. Latent prints are often partial or unclear, and can therefore "result in an incorrect match when run through a computer."²⁷⁰ Traditional rolled tenprint cards, also notorious for their poor quality, are not always easily decrypted by AFIS systems. The problem here is that data of mediocre quality can hamper the identification process. It can increase the risks of misidentification and this may lead to improper arrests, and therefore to the violation of people's civil rights. It should be reminded, however, that final responsibility in the determination with the positive identity of a person does not lie with the electronic system but on fingerprint specialists.

On the positive side, a beneficial effect of AFIS technology is that it makes it easy to determine the real identity of suspects. The San Francisco Police Department,

²⁶⁹ Malcom K. Sparrow, "Measuring AFIS Matcher Accuracy," *The Police Chief*, April 1994, 147.

for instance, estimates that 17 percent of the people they arrest lie about their names and other identifying information they provide, but they are now identified by the automated system.²⁷¹ A particular aspect of this question is that electronic fingerprinting is tremendously valuable in linking the various files pertaining to one person in a single file. Van Duyn gives the example of a suspect who, "after being identified by WIN AFIS, was linked to 20 additional cases."²⁷²

The number of aliases detected by AFIS systems is rather impressive. For instance, "as of August, 1987, the Massachusetts AFIS had positively identified 737 criminal suspects who were using aliases."²⁷³ Another illustration involves the joint purchase of an AFIS system by Pierce County, Washington, Sheriff's Department and Tacoma Police Department. When they converted their collections of tenprint cards into the electronic format, "the system found 30% of the cards were duplicated; aliases were noted and criminal histories of many offenders were consolidated."²⁷⁴

Records are also duplicated at the FBI. The 176,930,370 fingerprint cards that formed its collection in 1986 "represented over 56 million people because many criminals had multiple arrests and even civilians might be represented more than once."²⁷⁵ Records duplication is a common phenomenon throughout the criminal justice system not only because people use different names but also because each component of the system creates its own file about a criminal. The need to repeatedly type the same pieces of information increases the risk of data entry mistakes.

²⁷⁰ Jonathan B. Moses, "Fingerprint Advances Help Solve Crime," *Wall Street Journal*, 23 September 1992, B20.

²⁷¹ Department of Justice, Bureau of Justice Statistics, *Automated Fingerprint Identification Systems: Technology and Issues*, 12.

²⁷² Van Duyn, *Automated Crime Information System*, 123.

²⁷³ Bruce L. Berg, *Law Enforcement: An Introduction in Police in Society* (Boston: Allyn and Bacon, 1992), 289.

²⁷⁴ Raymond Fjetland and Charles Robbins, "The AFIS Technology: A Milestone in Fingerprint Identification Technology," *The Police Chief* (June 1989): 20.

²⁷⁵ Thomas J. Deakin, *Police Professionalism: The Renaissance of American Law Enforcement* (Springfield, IL: Charles C. Thomas Publisher, 1988), 240-241.

AFIS technology can eliminate this redundancy because it participates to the trend towards the automation of the booking process in which fingerprints, pictures, and texts (including official forms and personal documents taken from the arrestee) are digitized in the computer of a booking station and stored in a police department computer system. From there, the information can be transmitted via modem through the entire criminal justice system. Federal agencies such as "The Drug Enforcement Administration (DEA), U.S. Marshals Service, Immigration and Naturalization Service, FBI, Bureau of Prisons and others have each been considering alternatives for automating parts of the booking process"²⁷⁶ by using image processing technology. Such an approach to the booking procedure is gaining further success and is spreading at State and local law enforcement agencies as well.

It should be finally mentioned that, when the NCIC 2000 is fully operational, it will be possible to quickly proceed to the identification of fugitives or wanted persons who can currently avoid being recognized during police controls. The electronic transmission of their fingerprints, photographs and criminal files will enable law enforcement officers to positively identify them in record-time, to differentiate people with similar names and physical appearance and to know whether the people before them are wanted by police authority.

The automated detection of previous cases of mistaken identities, the correction of these mistakes, and the expected reduction in the number of new cases of mistaken identities are all factors contributing to the general improvement of criminal history record systems and should reduce the number of innocent people harmed because of such errors.

The Quality of Criminal Justice Records

Impressive technological advances mark the ongoing computerization of criminal justice data. Summarized in the framework of the First United Nations Workshop on Computerization of Criminal Justice Information held in Havana, Cuba on September 7, 1990, the benefits of this automation include:

- (1) an increase in the overall efficiency in criminal justice performance thanks to the usual effects of automation, such as a decrease in the general

²⁷⁶ U.S. Department of Justice, Federal Bureau of Investigation, Department of Justice's Joint Automated Booking Station Project, *CJIS, Criminal Justice Information Services. A Newsletter for the Criminal Justice Community*, vol. 1 no 1, Fall 1994, 7.

processing time of various tasks, a better use of the resources and the reduction of human errors;

- (2) an assistance in the decision-making process to all criminal justice authorities, from the law enforcement officer to the probation and parole officer, thanks to the fast availability of accurate criminal justice records;
- (3) the improvement in inter-agency cooperation at the national and international level through the easy compilation and exchange of records;
- (4) the improvement in the availability of statistical information, which, in turn, provides criminal justice policy-makers with sound pieces of information to better control the entire criminal justice system;
- (5) an improved efficiency in the administration and routine tasks of criminal justice agencies;
- (6) the adoption of standards which facilitate the exchange of information through the criminal justice system.²⁷⁷

A key element in this global vision is the same as in any other area of computer technology: the quality of the data input in automated systems.

Ideally, computerized data should be "accurate, consistent, authorized, valid, complete, unambiguous, and processed according to specifications in a timely manner."²⁷⁸ However, long before its automation, the criminal record system had been criticized as lacking of accuracy and reliability and it is well substantiated in the literature that, despite the many efforts to improve their quality, a large number of computerized criminal records are still incomplete or inaccurate. They are nevertheless disseminated and used inside and outside the criminal justice system.

An important study conducted by Laudon provides evidence of the lack of quality in criminal files in the period between 1979 and 1982. Only 45.9 percent of files of the NCIC and 25.7 percent of the records held by the Identification Division of the FBI were complete, accurate and unambiguous.²⁷⁹ As for the state level, the percentage of files of good quality ranged from 12.2 percent and 18.9 percent for two states to 49.4 percent in a third state.²⁸⁰

²⁷⁷ Richard Scherpenzeel, ed. *Computerization of Criminal Justice Information Systems* (The Hague, Netherlands, 1992), vol. 1, 21-23 and 50-52.

²⁷⁸ Daniel T. Brooks and Suzan H. Nycum, *Computer Crime: Prevention, Detection, Prosecution* (New York: Law & Business, Inc., 1983), 9.

²⁷⁹ Kenneth C. Laudon, *Dossier Society: Value Choices in the Design of National Information Systems* (New York: Columbia University Press, 1986), 139.

²⁸⁰ *Ibid.*, 142.

Other examples of reports or accounts on the quality of criminal records include the following.

Nationwide audit programs have been established by the NCIC “for the purpose of assessing data quality within the [NCIC] system and monitoring policy compliance by the state Control Terminal Agencies and the originating agencies.”²⁸¹ One of them, conducted in 1986, showed that, while the quality of the records was quite high in some states (Arizona, New Jersey, Oregon, and Wisconsin), it was poor in other ones (South Carolina and Alabama). Their quality was especially inferior in Alabama, where 13 percent of the recorded information about wanted persons was invalid and 8 percent of the information was inaccurate. Furthermore, 17 percent of the records had been cleared just before the audit. Among the factors affecting the quality of the data,

perhaps the most serious is the failure of law enforcement agencies to remove invalid records, particularly wanted person entries when the warrants have been withdrawn or served and stolen vehicles entries when the vehicles have been recovered. . . . Other problem areas included failure of entering agencies to institute procedures for cross checks and third-party review of record data before entering it into the system, failure of some agencies to provide hit confirmations as required by NCIC rules, failure to properly validate records and inadequate audit and training staffs at the state level.²⁸²

The DOJ concludes its review of the audit by stating that “Although the overall quality of NCIC entries may be quite high, it appears likely that the files do contain an unknown but possibly large number of serious errors which present the possibility of improper arrests and seizures of property.”²⁸³

Non official sources also document the issue of the quality of the criminal records. Morris, for example, states that “At best ‘rap sheets’ are only indicators of past police contact and can not be relied upon for their accuracy. Because ‘raps’ are outdated by several days the moment they arrive in a department, ‘rap’ users should treat them as historical reference materials only.”²⁸⁴ Another author assesses that “At

²⁸¹ U.S. Department of Justice, Bureau of Justice Statistics, *Criminal Justice information Policy, Criminal Justice «Hot» Files* (Washington, D.C.: GPO, 1986), 28.

²⁸² *Ibid.*, 31.

²⁸³ *Ibid.*, 32.

least 12,000 invalid or inaccurate reports on suspects wanted for arrest are transmitted each day to Federal, state, and local law-enforcement agencies, according to projections by the Federal Bureau of Investigation.”²⁸⁵ Although the article reports only incorrect information “including faulty warrants, wrong heights, weight and date of birth,” a large number of studies conducted on the subject conclude that one of the major problems in the quality of criminal records is the poor disposition reporting. In this respect, a 1991 Office of Technology Assessment report says: “The FBI continues to have problems with missing dispositions, either because they are not reported by the States or because the FBI lags in entering the reported dispositions into the criminal history records. A significant percentage of reportable dispositions (roughly 30 to 50 percent) are never provided to the FBI. Ident currently has a backlog of about 2.5 million unprocessed dispositions.”²⁸⁶

At the FBI, the long and costly process of converting manual files to the electronic format is still in progress and should be complete by the end of the 1990s. As of mid-1991, only 54 percent of the criminal records held in the Identification Division were completely automated. Another 33.5 percent of the criminal records, representing 8.7 million criminals, were partially automated. Only the name, the fingerprint minutiae, and the physical description of the individuals were computerized.²⁸⁷ Consequently, during the 1992 National Conference on Criminal History Records, the Chief-Legal Counsel of the FBI Identification Division warned the audience that it was almost impossible to analyze the criminal file of the federal agency for true disposition figures because only half of the records were automated. As the examination of every manual record was not possible, “most of the FBI surveys

²⁸⁴ Jack Morris, *Police Intelligence Files: An Introduction to the Use of Confidential Police Files* (Orangevale, California: Palmer Enterprises, 1983), II-4.

²⁸⁵ David Burnham, “F.B.I. Says 12,000 Faulty Reports On suspects Are Issued Each Day,” *New York Times*, 25 August 1986, 1.

²⁸⁶ Congress of the United States, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program*, 1991, 12-13.

²⁸⁷ Denis G. Kurre, “FBI Felon Identification System,” *Congressional Digest* 70, (June-July 1991): 168.

are necessarily limited to the automated records.”²⁸⁸ Nevertheless, speaking at the same conference, the General Counsel of SEARCH stressed that 40 to 60 percent of the criminal history records were incomplete.

A criminal history record system of excellent quality is imperative, not only to insure the smooth running of the criminal justice system, but also to protect people’s rights. Programs have been developed and measures have been taken in order to bring a solution to the issue. For example, the FBI has been working for years at reviewing and correcting its criminal record system, at reducing its fingerprint card backlog, and at bringing its backlog of arrest and disposition records up-to-date. The Bureau also tries to decrease the release of records of poor quality by implementing policies such as the “one-year rule.” According to that rule, the FBI “cannot give out to non-law-enforcement agencies . . . any criminal history information more than one year old without noting a final disposition. The information that is on-line to law enforcement through NCIC, however, has no such rule.”²⁸⁹

Similar programs have also been established at the state level. One of them, established in the 1990 Comprehensive Crime Control Act requires from the states receiving Edward Byrne Memorial State and Local Law Enforcement Assistance Formula Grant to allocate five percent of the grant for the improvement in their disposition reporting, automation and reporting of criminal history records to the FBI. Also, as mentioned above, audits are being held in order to “assess the completeness and accuracy of the criminal history record databases maintained by state central repositories.”²⁹⁰

Finally, the intention for the entire criminal justice community to work together to solve the issue can be seen in initiatives like the creation in 1990 of a Task Force on Disposition Reporting. For the first time, “senior and nationally recognized judges,

²⁸⁸ U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *National Conference on Improving the Quality of Criminal History Records: Proceedings of a BJS/SEARCH Conference* (Washington, D.C.: GPO, 1992), 53.

²⁸⁹ Jon Zonderman, *Beyond the Crime Lab*, 165.

²⁹⁰ U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Assessing Completeness and Accuracy of Criminal History Record Systems: Audit Guide*, (January 1992), (Washington, D.C.: GPO, 1992), 1.

court administrators, criminal history repository directors, a director of a pretrial services agency, a prosecutor and law enforcement officials [worked together] to review disposition reporting problems and to make recommendations for improving disposition reporting of criminal history record information to state central repositories."²⁹¹ The consequences of inaccurate or incomplete data can be dramatic or dreadful not only for the person who is judged on the basis of these pieces of information and who has his/her civil and constitutional rights jeopardized, but also to those, such as police officers who base the decisions they make on these data. The implications are so important that "A number of people have sued police for arresting them using out-of-date, incomplete, or false data, and police officers have even sued NCIC administrators for putting them at risk in civil suits. Courts often have ruled in favor of people arrested falsely, and many data-integrity cases are settled out of court; either result often takes months or years and has a high financial and emotional cost."²⁹² This is not, however, a clear-cut issue - witness some debates at some courts of justice.²⁹³

AFIS and the Quality of Criminal Records

Considering the number of studies criticizing the quality of criminal records, it seems appropriate to suggest that the electronic fingerprinting method is a powerful technology providing fast and accurate access to criminal information that is, to a certain extent, of questionable quality but on the basis of which important decisions are nevertheless being made. While this observation may appear to some as an overstatement, it is still a reminder that highly sophisticated systems do not guarantee reliable databases. A natural question therefore arises as to whether the quality of the records stored in AFIS systems is optimal.

²⁹¹ U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Report of the National Task Force on Criminal History Record Disposition Reporting. Findings. Recommendations*, (June 1992), (Washington, D.C.: GPO, 1992), 1.

²⁹² Ibid.

²⁹³ Linda Greenhouse, "Court Weighs Ramifications of Digital Age Considers Legal Role of Computer Errors," *New York Times*, 8 December 1994, A21.

First, it may be assumed that mistakes in manual record systems are simply transferred and stored in AFIS systems. This is a problem inherent in the building of any new record system on old data. Second, as observed above, there is always the question as to whether the quality of the prints digitized in AFIS systems is good enough to enable their proper automated processing, use and management. Third, the quality of the data stored AFIS systems can be affected by the same factors than any other computerized data. For example, human mistakes, such as the misspelling of a name, can still occur. Other classical sources of lost or altered computerized data include damages in the hardware caused by the action of physical agents (dust, moisture, etc.) and by natural hazards (earthquakes, floods, etc.); unexpected mistakes in programming; deliberate acts of malevolence on the software (the introduction of viruses, for example); the lost of data during their transmission to another computer; mistakes in the way the data have been gathered or input; the intentional insertion, removal or change of data by unauthorized people or for unauthorized purposes.

A question to examine now is whether - or to what extent - AFIS technology can affect the quality of criminal records. The range and the depth of the problems involved cannot be extensively discussed in this paper. However, elements can be highlighted.

First of all, it is clear that AFIS technology has not been designed primarily to improve the quality of criminal records. Nevertheless, AFIS technology can have an indirect influence on the quality of data by serving as a new incentive for intensifying the ongoing process of improvement of the existing criminal justice systems. It can be argued, indeed, that the wider use of AFIS technology can result in a proportional increase in the number of known cases of incomplete, inaccurate or ambiguous criminal records. Increase in pressure exerted on criminal justice authorities by both concerned citizens and agencies of the government can be expected. Such pressure reflects not only the ever-increasing awareness of the potential damages on people's lives arising out of the use of computerized data, but also the desire to achieve criminal justice record systems characterized by integrity and reliability, on the basis of which fully and accurately informed decisions respecting people's rights can be made. It has been noted that the action of private individuals anxious to have their records

reviewed, corrected, sealed or expunged, combined with financial incentives and legislative support of a government anxious to develop reliable databases have already led to improvements in criminal record systems, but more work needs to be done. AFIS can contribute to the completion of this task for the following reasons.

First, AFIS technology can impel the establishment of new priorities, revised standards or different procedures for better control of the quality of criminal justice records because it is a fairly recent technology still in an early stage of diffusion. In practice, this becomes very complex because of : (1) the complexity of the structure of the U.S. criminal justice system and of its numerous information systems; (2) the extreme difficulty in establishing effective standards and regulations related to information policies to be applied at all the levels and jurisdictions of the criminal justice system; and (3) the crucial problem of the exchange of information within and between the segments of the criminal justice system. It is however vital to re-assess existing policies in the light of the possibilities offered by AFIS technology, to clarify what is further needed, and to translate the identified needs into operational terms to better control the data stored in criminal record systems.

A second reason lies in the extreme degree of sophistication and the range of capabilities of AFIS systems among which are: their capability to integrate different types of data (text, pictures) and technologies, to connect various AFIS systems to each other, and to link different criminal justice record systems. AFIS systems can therefore connect the wealth of data spread in the different components of the criminal justice system, and make it integrated and coherent.

Integrated justice information systems (IJIS) offer a vision of overall coherence and of apparent simplicity. They are also a critical necessity. Their importance is highlighted in tragic instances in which the flow of information between various segments of the criminal justice system is hampered. In California, for example, it has been found that "The inability of the state to process fingerprint cards of day care applicants is just part of a larger problem California has in tracking its criminals. Parole information on felons is kept in Department of Corrections computers, criminal history in state Department of Justice computers. The two systems cannot communicate. The seriousness of that surfaced during the investigation of the kidnapping and killing of

Polly Klaas.²⁹⁴ Bentfield notes that the inability to share information across different justice and public safety jurisdictions is a problem that has long existed in criminal justice systems.²⁹⁵ It is therefore not surprising that IJIS are gaining increasing acceptance throughout the criminal justice community.²⁹⁶ At the present time, however, IJIS that encompass or that rely on biometric image technology still need further development. In this respect, the national sales and marketing manager of automated identification systems for TRW's Integrated Engineering Division declared that "the fingerprint can be the single thread of identification throughout the entire criminal justice system - from the time an individual is taken into custody, through the pretrial and court administration process, jail management, and release. . . . All the technology is there to make an integrated, cohesive system, but nobody's put it together in a continuum for law enforcement."²⁹⁷

With regard to the issue of the quality of criminal records, it can be projected that IJIS that encompass or that rely on AFIS technology will provide substantial benefits based on concepts that have been evoked earlier in this paper. For example, data based on positive identifiers and scattered in several databases can be automatically linked to each other, reviewed and compared with more accuracy than before, and finally consolidated in a correct record. With identical records shared by the all the components of the criminal justice systems, the updating of criminal files should be faster, easier, more comprehensive, and more precise than before. Seen in this light, the diffusion of AFIS technology is likely to cause pressure for more coherent and reliable criminal justice record systems.

It should be finally pointed out that concrete initiatives involving fingerprints have already been proposed to stimulate the control of the quality of criminal records.

²⁹⁴ Linda Goldston, «State Lags in Checking Day Care Workers,» *San Jose Mercury News*, 22 December 1993, 1A.

²⁹⁵ Ken Bentfield, «A Quiet, Deadly Weapon Against Crime: The Integrated Criminal Justice Information System,» *Government Imaging* (August 1995): 14.

²⁹⁶ *Ibid.*, 16.

²⁹⁷ Clark David, quoted by William B. Scott, "Defense Skills Applied to Biometric ID," *Aviation Week and Space Technology* (17 October 1994): 54.

For example, it has been suggested that the FBI develop and implement at the State and local levels of the criminal justice system a "fingerprint identification and criminal history record audit program"²⁹⁸ that would be similar to the audits of the States and local hot files record systems already conducted periodically by the FBI.

To sum up, with respect to the quality of criminal records, it is very unlikely that AFIS be the ultimate solution. It is rather an opportunity to enhance measures already in place and to create new measures better suited to the problem.

Privacy Violations and Criminal History Records

Computerization is a modern life reality and spares no sector of activity.

Federal agencies have more than 20,000 mainframes and minicomputers and 200,000 microcomputers installed, employ 100,000 data-processing (DP) people and spend more than \$15 billion annually on computerization. . . . The 50 states have more than 1,000 mainframes and minicomputers and 20,000 microcomputers installed, employ 15,000 DP people, and spend over four billion dollars annually. . . . The 2,000 governments of cities over 10,000 in population have 2,000 mainframes and minicomputers and 20,000 microcomputers, employ 20,000 DP people, and spend \$4 billion annually for computerization.²⁹⁹

A particular aspect of computerization is the creation of databases containing personal information about individuals.³⁰⁰ At the end of the 1980s, the federal government had stored more than four billion personal files, that is, 15 to 20 files on each and every citizen.³⁰¹ The risk that employees having access to these data misuse them and interfere with private lives resulted in the enactment of several federal and state laws. Some of them pertain only to information gathered by the government, while others aim at protecting people's right to privacy in specific

²⁹⁸ U.S. Congress, Office of Technological Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options* (Washington, D.C.: GPO, 1991), 15.

²⁹⁹ Kenneth L. Kraemer, in Charles Dunlop and Rob Kling, *Computerization and Controversy. Value Conflicts and Social Choices* (San Diego: Academic Press, Inc., 1991), 169-170.

³⁰⁰ The Federal Privacy Act of 1974 defines the term "record" as «any item, collection, or grouping of information about an individual that is maintained by an agency including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.»

³⁰¹ Daniel L. Slotnick et al., *Computers and Applications: an Introduction to Data Processing*, 2nd ed. (Lexington, MA: D.C. Heath and Company, 1989), 562.

situations of the social life. Among the important federal laws are the *Freedom of Information Act* of 1970; the *Fair Credit Reporting Act* of 1970; the *Family Educational Rights and Privacy Act* (FERPA) of 1974; the *Privacy Act* of 1974; the *Right to Financial Privacy Act* of 1978; the *Electronic Fund Transfer Act* of 1978; the *Computer Fraud and Abuse Act* of 1986; the *Cable Communications Policy Act* of 1984; the *Electronic Communications Privacy Act* of 1986; the *Video Privacy Protection Act* of 1988; and the *Computer Matching and Privacy Protection Act* of 1988.

However, despite the legislation in force and despite the efforts of pressure groups, the truth is that privacy breaches in personal files do occur. Regarding this reality, Michael D. Scott documents four major types of privacy violations: the *electronic intrusion* in someone else's computer; the *interception* of data from another computer system; the unauthorized *aggregation of data* on individuals; and the *misuse of information* which, as it is described by Scott, refers to the principle that information gathered for one purpose cannot be used for another purpose.³⁰² Admittedly, security measures to protect criminal files do not prevent privacy violators from accessing, intercepting and misusing them. "The availability of arrest records to those without official access to the system is so notorious that it has been noted and taken into account as a fact in litigation, despite the supposedly private nature of such data."³⁰³

This section depicts particular cases of privacy violations involving law enforcement agents who removed data from criminal record files in an unauthorized way and for unauthorized purposes.³⁰⁴

The magnitude of the problem is difficult to estimate. In the course of a study about confidential information being illegally used, evidence indicated that "there existed an extensive network of information brokers capable of obtaining confidential

³⁰² Michael D. Scott, in Dennis Campbell and Joy Fisher, eds., *Data Transmission and Privacy* (Boston: Martinus Nijhoff Publishers, 1994), 501-504.

³⁰³ R. Paul Davis, "Records of Arrest and Conviction: A Comparative Study of Institutional Abuse," *Creighton Law Review*, 1980, 869.

³⁰⁴ Cases of unauthorized access to police systems by non law enforcement officials are also described in the literature. See for example, Martin Wasik, *Crime and the Computer* (Oxford: Clarendon Press, 1991), 45.

information by bribing government officials or private company employees who had legitimate access to the information."³⁰⁵

In a testimony before the Subcommittee on Information, Justice, Agriculture, and Transportation (Committee on Government Operations), and before the Subcommittee on Civil and Constitutional Rights (Committee on the Judiciary, House of Representatives), Laurie E. Ekstrand presented the results of a survey conducted in 1993 regarding the misuse of criminal justice information within the NCIC. She received information on sixty two examples of abuses of the system by NCIC officials. Thirty three were related to the misuse of NCIC for personal purposes, sixteen concerned the misuse of the system for profit, seven occurred for political gains, and six were the result of an apparent misunderstanding of NCIC policy.³⁰⁶

Press accounts also report misuses of criminal justice databases. For example, "Newly disclosed records show that in the last three years, dozens of the [Los Angeles] Police Department's employees have been found to be using its computers to check the background of baby sitters, house sitters and other for personal reasons."³⁰⁷ Other reasons are linked to the capacities inherent to automated systems. "Critics charge that because of the system's speed, police use it for mass or random record checks, such as keying random license plate numbers into their cruiser terminals or entering the names of everyone on a homeless shelter's sign-in list."³⁰⁸

Whereas literature reports cases of unauthorized use and disclosure of criminal data, it does not report, to our knowledge, instances in which law enforcement officers knowingly and malevolently falsified criminal data. The possibility nevertheless exists.³⁰⁹ Also, police officers have been accused of creating false records. "Laudon

³⁰⁵ U.S. Congress, *Sale of Criminal Records*, 8-9.

³⁰⁶ U.S. General Accounting Office, *National Crime Information Center. Legislation Needed to Deter Misuse of Criminal Justice Information*, by Ekstrand, Laurie E.

³⁰⁷ "Police Computers Used for Improper Tasks," *New York Times*, 1 November 1992, 38L.

³⁰⁸ Zonderman, *Beyond the Crime Lab*, 158.

³⁰⁹ For examples of such scenario, See Andre Bacard, *The Computer Privacy Handbook* (Berkeley, CA: Peachpit Press, 1995), 5. For the record, the distortion of data in an AFIS

charges that access to criminal history records is so easily achieved that he found several cases in which police undercover personnel created false records within the system as part of the undercover agent's cover, since it was assumed that the records system would be accessed by organized crime as a check on these agents."³¹⁰

There is a marked lack of uniformity in police authority response to the issue of improper use of police computer systems.

In Los Angeles Police Department, for instance, where more than 45 employees have been disciplined between 1989 and 1992 for improper use of the computer system, "Most received only oral reprimands or suspensions of two or three days."³¹¹ To the contrary, officials at the federal level take the question very seriously. During a hearing before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, David F. Nemecek, Inspector-Deputy Assistant Director at the FBI Criminal Justice Information Services Division, declared that the NCIC managers wanted "to inform, unequivocally, that taking information from NCIC and using it for any purpose other than that for which it was intended is criminal behavior with severe penalties for violators."³¹² He insisted on the measures taken for years to protect the integrity of the NCIC data. The NCIC Advisory Police Board, he says,

has acted in an aggressive, self-policing role, setting stringent policies regarding computer access, record quality, and dissemination of information. . . . A massive training program has been developed requiring every criminal justice employee having access to NCIC information to receive basic training in system policies. Heavy emphasis is placed on the concept that NCIC is a criminal justice system and information is restricted to those with authorized access. Stringent automated logging procedures exist, allowing NCIC and States to reconstruct and trace every transaction made on the system.³¹³

system and in a computerized criminal justice file is the plot of modern detective stories such as *Cruel and Unusual* by Patricia Cornwell (Thorndike, ME: G.K. Hall, 1993).

³¹⁰ Susan H. Gray, "Electronic Data Bases and Privacy: Policy for the 1990s," *Science, Technology & Human Values* 14, no. 3, (Summer 1989), 250.

³¹¹ "Police Computers Used for Improper Tasks," 38L.

³¹² U.S. Congress, *Sale of Criminal Records: Hearing before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary House of Representatives*, 102d Congress, 2d sess., 30 July 1992, 7.

³¹³ U.S. Congress, *Sale of Criminal Records*, 3.

It should however be pointed out that the views expressed by Nemecek do not match the ones expressed by Ekstrand. She found that criminal prosecution was administered in only seven out of 49 cases of misuse of the NCIC system. Five other cases were still pending at the time of the testimony and the outcome of the final eight cases was unknown.

Besides being accessed for personal purposes, criminal history records can also be used for profit. In his opening statement of the hearing mentioned above, Chairman Don Edwards said that in 1991, "numerous individuals were arrested nationwide on charges of illegally obtaining and selling information from Federal computer files. Some of those involved, according to press accounts, included employees of a police department with access to FBI computer records, and other were current or former employees of the Social Security Administration."³¹⁴ In an article presented as part of this hearing, Michael Isikoff reported the case of a terminal operator at the Fulton County, Ga Sheriff's office who sold records to a private investigator for \$240 apiece and the case of a Virginia State Police officer who "was indicted on charges of selling NCIC records to two Prince George's County private investigators, who allegedly charged clients \$200 for each criminal record check."³¹⁵ A number of private companies are also specialized in the sale of confidential information including credit and criminal histories. Their clients use the information for purposes as diverse as "locating people or making decisions on hiring, firing, suing or lending."³¹⁶

To make things worse, it also happens that criminal records are sold in a detrimental way to record subjects. For example, as these fraudulent and unethical database searches are usually made on the basis of a limited number of identifiers, they can easily result in mistaken identities, with the negative consequences mentioned earlier. It also occurs that records dealers sell arrest records without

³¹⁴ U.S. Congress, *Sale of Criminal Records*, 1.

³¹⁵ Michael Isikoff, "Theft of U.S. Data Seen as a Growing Threat to Privacy," *Washington Post*, 28 December 1991.

³¹⁶ Mitch Betts, "Personal Data More Public Than You Think," *Computerworld*, 9 March 1992, 14.

mentioning the dropping of the charges or the acquittal of the record subjects. This can result in other instances of record based discriminations.

A last issue regarding the misuse of criminal records relates to the ulterior use of the information obtained from police files. Once outside the original database, police loose control over the information and concern has been expressed about further negative uses of the data. In fact, it is plausible to assume that they can be used "for a range of other improper purposes, including blackmail, or even by drug dealers seeking to check out their customers."³¹⁷

AFIS and Privacy Violations

Significant dangers to privacy are inherent in the introduction of any computer-based storage and retrieval systems giving access to records containing personal information. With respect to AFIS technology, controversy arises because its larger diffusion throughout the U.S. criminal justice system, the multiplication of requests for criminal information for both criminal and noncriminal purposes, in conjunction with the availability of this information to a growing number of government employees greatly increase the possibilities of misuse of criminal data. The problem goes far beyond the issues generated by the electronic fingerprinting method to touch the broader field of personal privacy in the computer age which has been analyzed in great detail in many publications since the early 1970s.

AFIS technology can be considered in this discussion in two ways. On the one hand, it has been pointed out in Part Two of this paper that the electronic fingerprinting method can be conceived in some of its general applications as a way to enhance the protection against various types of unauthorized access to automated systems; on the other hand, with regard to the issue of personal privacy in the criminal justice setting, AFIS can be seen as an enhanced information technology that can possibly put some aspects of personal privacy in further danger.

In the first case considered, AFIS is used as a biometric authentication technique. "Authentication is performed by requiring the individual to allow a measurement to be taken, and comparing the result of the test against a previously

³¹⁷ Isikoff, «Theft of U.S. Data Seen as a Growing Threat to Privacy,» A4.

recorded profile for that individual.”³¹⁸ In the present study, the measurement being taken refers to that of fingerprints. However, it should be kept in mind that biometric authentication measures also encompass the measurement and comparison of other characteristics proper to any individual, such as the retinal patterns, the voice print, and handwritten signatures.

An important question is whether AFIS systems offer the perfect security in preventing various types of intrusion in computer systems and, consequently, whether they are a good protection against the unauthorized use or disclosure of the confidential information they process. The answer is no. Of course, they are conceived on the basis of the intrinsic characteristics of fingerprint which, in modern day life, are expressed in sentences like : “When it comes to industrial espionage, spies can disguise their identity, alter ID cards, and crack passwords, but they cannot change their fingerprints.”³¹⁹ In another clear example Identifier Technology points out in one of its promotional catalog sheets that “unlike cards, keys, badges, or password, fingerprints cannot be lost, stolen, exchanged, forgotten, or compromised.” While this may be true, it has been felt for years that the protection of the security in computerized systems should not rely only on one security technique, even if it is as reliable as fingerprint matching. Therefore, the access to AFIS and to other computerized systems generally presupposes the use of the combination of two or three of the following identification methods: (1) something that only the user knows, like a password, a social security number or a personal identification number; (2) something difficult to counterfeit that the user possesses, like a credit card or a badge; and (3) some measurable biometric characteristics such as the fingerprints and the hand geometry.

In the second case considered, in which AFIS is seen as an enhanced information technology that can possibly put some aspects of personal privacy in further danger, it could be feared that its application in the criminal justice setting could put personal privacy in more danger than it already is. But scores of privacy laws have

³¹⁸ G. O'Shea, *Security in Computer Operating Systems* (Manchester: NCC Blackwell, 1991), 119.

³¹⁹ Mark LaPedus, “PCs Catch Criminals Using Fingerprint Analysis,” *Byte*, October 1993, 34.

been proposed or enacted to protect the access to criminal records in jurisdictions where they are not considered as public records. The best example is probably provided by the number of laws protecting the federal criminal record system. In 1992, the IAFIS, the NCIC 2000 and the UCR were integrated to form the Criminal Justice Information Services (CJIS) Division, with the mission "to serve as the focal point and central repository for criminal justice information services in the FBI."³²⁰ The data held in the files of the CJIS Division are unclassified but sensitive and need therefore particular protection. So, compliance with a wide range of laws and regulations has been proposed in the framework of the security plans developed for the CJIS Division's automation programs. Among them, there are the Privacy Act, the Computer Security Act of 1987, the FBI Automated Data Processing and Telecommunications Security Policy, the FBI Data Access Policy, and the FBI Microcomputer Security Policy.³²¹

Legal protection is of course vital, but, as seen above, despite the many privacy laws in force, despite the security policies in place and the technical procedures devised to protect the access to AFIS systems and criminal data, reports show that computer crimes within the criminal justice setting do occur.

The crux of the matter regarding privacy in an AFIS environment and, as a matter of fact, in any automated context, lies mainly in the lack of ethics, of responsibility and of professionalism of some of a system's users who can easily access, retrieve and disseminate large amounts of confidential data.

To conclude this chapter, two observations can be made.

First, given the general nature of this paper, the real impact of AFIS technology on the issues briefly outlined could not be assessed in-depth. Each of them could in fact be the topic of specialized research. In addition, there is a lack of available statistical data to correctly estimate the influence of AFIS technology on any of them.

Second, the issues presented are indicative of weaknesses within law enforcement and, on a larger scale, within the entire criminal justice system. It has been shown that there are human errors and that unethical behavior occur as well.

³²⁰ U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, *Automated Information Systems Plan - Tactical Plan Fiscal Years 1993-1995* (Washington, D.C.: 1993), 1.

³²¹ *Ibid.*, Systems Engineering Project 5, 2-3.

Henderson studied the criminal offenses perpetrated at all the levels of the criminal justice system and some of his conclusions reveal a general feeling of discomfort. "Wrongdoing by members of executive and legislative branches of government, prosecutors, judges, and law enforcement personnel takes many forms and could be widespread in the American criminal justice system. Further, the various acts of wrongdoing committed by criminal justice system personnel not only result in acts of great physical and financial harm, but threaten the legitimacy of the entire political system as well."³²²

However, despite all the issues that touch many citizens, the reported confidence in law enforcement is quite high. At the national level, 58% of the population have a great deal or quite a lot of confidence in police, 30% have some confidence in police and 10% have very little confidence in police. In contrast, the reported confidence in the criminal justice system is more scattered. 19% of the population express a great deal or quite a lot of confidence in the system, 37% express some confidence and 37% express very little confidence in the criminal justice system.³²³

³²² Joel H. Henderson and David R. Simon, *Crimes of the Criminal Justice System* (Cincinnati, OH: Anderson Publishing Co, 1994), 14.

³²³ U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Sourcebook of Criminal Justice Statistics - 1994* (Washington, D.C.: GPO, 1995), 146-147.

CHAPTER 9

THE USE OF AFIS TECHNOLOGY IN THE WELFARE SYSTEM

General

As suggested in the previous chapter, computerization has introduced unprecedented possibilities for the gathering, analysis, management and dissemination of personal information held in government databases. In the society in general, which is the focus of this chapter, automated systems are used for a variety of managerial and administrative tasks aiming at improving the quality and the control of services provided to the population. A recent illustration of an application designed to better monitor the assistance to a specific group of people is the Oklahoma Statewide Automated Child Welfare Information System (SACWIS) which became, in 1995, the nation's first fully implemented statewide computerized system for child welfare.³²⁴ Automated systems are also used to combat fraud in social services.

A 1994 Report to Congressional Committees, reviewing fraud, waste and abuse in the Food Stamp Program, the nation's largest food assistance program and one of its major welfare programs, charges that:

For the 6-year period covering fiscal years 1988-93, \$7.44 billion in benefits was issued to ineligible households and to households who received more benefits than they should have. About \$1.78 billion or 24 percent of the overissued benefits, was given to individuals who intentionally provided inaccurate information when seeking benefits. The remaining \$5.66 billion in overpayments occurred because of recipients' unintentional errors in providing eligibility information or state agency caseworkers' errors in determining applicants' eligibility and benefits levels.³²⁵

In addressing the reasons for which overpayments occur in the Food Stamp Program, the report indicates that "Investigations have disclosed elaborated schemes

³²⁴ « Automated Child Welfare Information System Implemented in Oklahoma,» *Government Imaging* (September 1995): 8.

³²⁵ General Accounting Office, *Food Assistance - Potential Impacts of Alternative Systems for Delivering Food Stamp Program Benefits*, Report to Congressional Committee, GAO/RCED-95-13 (December 1994), Chapter 4.1.

involving false documents, fictitious identities, and even fraud by state welfare system employees who create 'ghost' recipients and pocket the benefits."³²⁶

Computer matching technology, which is a method based on the comparison of the names of welfare recipients stored in an agency database, is a first way to spot and deter double-dippers, i.e., the individuals who collect multiple benefits either by using different names or by registering in more than one welfare office. Another method appeared in the early 1990s, when the Department of Social Services of a few counties of the nation started using AFIS technology in an attempt to reduce or prevent this type of welfare fraud.

The procedure is simple. A new applicant is requested to place one or more fingers on a fingerprint scanner. The person's fingerprint digitized images are automatically processed and stored in the AFIS system of the social service. At the time of the benefit payment, welfare recipients are asked to have their fingerprint(s) scanned again so that the AFIS system can verify their identity by comparing the incoming fingerprint(s) to the database of fingerprints stored in the computer memory. If a person is caught double-dipping, various measures are taken. In the General Relief program of Los Angeles County, for instance, the applicant is advised of the situation and no further action is taken. "If the applicant contests the match, a second opinion is requested from the fraud investigation group, which can remotely view both prints on its terminal. There are other procedures if the applicant continues to pursue a claim."³²⁷ In New York State, on the other hand, people suspected of double-dipping in two counties have "to appear before a hearing in both places within ten days or lose their benefits immediately."³²⁸

The first county to use the automated fingerprinting technology to detect and deter duplicate claims in its social services is Los Angeles County. The original idea, which emanated from Eddy Tanaka, Director of the Department of Public Social

³²⁶ Ibid., Chapter 2:1.1.1.

³²⁷ "LA Social Services Taps Fingerprint Technology," *Government Imaging* (November-December 1994): 18.

³²⁸ Ian Fisher, "Pataki Unveils New Rules To Fight Welfare Fraud," *New York Times*, 10 September 1995, 52.

Services (DPSS) for Los Angeles County, dates back to 1977, when the technology was not yet fast enough to serve such a purpose. The need for a system able to quickly identify applicants was reinforced in December 1983 when the Superior Court ruled that Los Angeles County could not deny benefits to General Relief (GR) applicants who did not have identification.³²⁹

AFIRM, the Automated Fingerprint Image Reporting and Match Systems, is the electronic system that replaced the manual processing of fingerprints in 1991. Since its implementation, electronic fingerprinting is a condition to receive General Relief in Los Angeles County. AFIRM, which saved \$5.4 million in the first six months of operation, was first tested in three district offices and officials noticed that the number of applicants in these offices dropped from 150 to 100 a day, while the number of applicants in surrounding offices where the AFIRM system had not been implemented rose from 100 to 150 a day.³³⁰ AFIRM was subsequently implemented in all the 14 General Relief offices of Los Angeles County and it allowed the county to conduct in 1994 between three thousand and five thousand searches a day in a database containing a little less than half a million of individuals. This initiative is considered as the first extensive use of fingerprints outside law enforcement.³³¹

In February 1993, Alameda County, which has the third largest General Assistance (GA) case load in California,³³² became the second county in California to fingerprint welfare recipients when it joined Los Angeles County and also used the AFIRM system. The fingerprints of the welfare recipients of Alameda County "are transmitted by telephone to Los Angeles, where they are compared to other prints on file. . . . The county will discover within 24 hours whether the print matches another print in the system."³³³ Within the following two years, the City of San Francisco along

³²⁹ "Los Angeles County Stops Fraud With Automated Fingerprint Matching System," [text on-line]; available from <http://www.hp.com>; Internet; accessed 21 February 1996.

³³⁰ Linda Rohrbough, "Intel Neural Network Chip Most Like Human Brain," *Newsbytes, Los Angeles*, July 21, 1993.

³³¹ "LA Social Services Taps Fingerprint Technology," 18.

³³² Rohrbough, "Intel Neural Network Chip Most Like Human Brain," 21 July 1993.

³³³ Frances Dinkelspiel, "County Fingerprinting Those on Welfare," *San Jose Mercury News*, 26 February 1993, 1B.

with other counties in California, such as Contra Costa and San Diego Counties, also started projects to deter welfare fraud through the electronic fingerprinting method.³³⁴

The application of fingerprint technology to welfare recipients opposed the State of New York Senate, which wanted to establish a statewide fingerprinting program, to the State Assembly, which viewed the method with skepticism because of the parallel it establishes between welfare recipients and criminals. In November 1992, under a compromise, the counties of Rockland and Onondaga started a pilot program similar to the one in place in Los Angeles County, fingerprinting new applicants to Home Relief, a state program helping single adults and childless couples. The \$150,000 program was to be extended to all the recipients of Home Relief of the two counties in the beginning of 1993, to 4,000 recipients in Onondaga and to 620 in Rockland.³³⁵ In September 1993, challenging the State authorities which had allowed the testing of a fingerprinting program only in these two counties, the officials of Suffolk County decided to take measures to implement a similar program in their own jurisdiction, arguing that "There is no statute that prohibits the county from doing so if it picks up the costs."³³⁶ In June 1994, the Governor and the legislative leaders of the State of New York agreed to expand the fingerprinting program to the following counties: Rockland, Onondaga, Suffolk, Orange, Oneida, Broome, Rensselaer, Niagara, Allegany, Steuben, Dutchess, and Osego. New York City, however, where two-third of the welfare recipients of the state lived was excluded from the two-year program until June 1994 when it was finally integrated into it along with the counties of Nassau and Westchester.

In some of the social services where automated fingerprint systems are used to thwart welfare fraud, officials wanted to expand their application to include recipients of programs such as to Aid to Families with Dependent Children (AFDC), to food stamps programs, and to health services. The implementation of these programs can be very

³³⁴ Our review of the implementation of AFIS technology in the welfare administration stops in 1994.

³³⁵ Jacques Steinberg, "Coming Soon: Fingerprints at Many Fingertips," *New York Times*, 10 January 1993, B1 and B6.

difficult. As an example, Los Angeles County was obliged in 1993 to put on hold its project to fingerprint the recipients of AFDC because neither the county nor the state administration adequately proved that the program would be cost-effective. Assemblywoman Barbara Friedman (D-North Hollywood) gave two reasons for her rejection of the proposed program. First, she observed that the estimation of the savings were based on a study of Los Angeles General Relief Recipients. She argued that, as the recipients of GR are, for the most part, single men while the recipients of AFDC are, for the most part, mothers and children, the behavior of the first group could be used to accurately predict the behavior of the second. Secondly, she reported the concerns of the legislators "about county calculations showing that 1.5% of General Relief dropped off the rolls to avoid being fingerprinted." Barbara Friedman contested the assumption of fraud underlying this observation and stated that no validation had been done "to show that people who didn't come in for fingerprinting were actually committing fraud."³³⁷ Despite the divergence of opinion, the electronic fingerprinting of new applicants started in five district offices of the Los Angeles County AFDC program in April 1994.

Issues

Advocates for the poor, social workers, lawyers, lawmakers, welfare applicants and welfare recipients count among the opponents to the electronic fingerprinting of the welfare population.³³⁸ Some of them consider the method as a reminiscence of a police state.³³⁹ Others charge that "for many African-American clients it conjures up

³³⁶ Paul Sabatino, Counsel of the County Legislature; quoted in "Suffolk Votes Fingerprinting for Welfare," *New York Times*, 15 September 1993, B1.

³³⁷ Quoted in Virginia Ellis, "Officials Can't Lift a Finger to Curb Fraud," *Los Angeles Times*, 3 August 1993, B8.

³³⁸ This section is based on (1) the documentation sent to us by the Los Angeles and San Francisco social services; (2) press articles covering the period 1992 through 1995; and (3) the texts published by James I. Davis on Internet in 1993. The informative nature of this material limits the extent of the conclusions that can be reached. It constitutes nevertheless an adequate reflection of the information provided to the general public on the electronic fingerprinting method in the social welfare environment.

³³⁹ "Suffolk Votes Fingerprinting for Welfare, State Officials Oppose Measure to Fight Fraud," *New York Times*, 15 September 1993, B6.

notions of tracking . . . and makes them feel they have no right to privacy once they are on welfare.”³⁴⁰

The fingerprinting method, whether manual or electronic, is still strongly associated in the collective consciousness with the image of criminals being brought to justice. Therefore, numerous opponents to the technique feel that, by being fingerprinted, welfare recipients are treated like criminals. This concern is expressed in different ways. Some find the method dehumanizing and demeaning and think that it makes the “humiliating process of applying for welfare even more unpleasant, putting the needy through a process that many people associate with criminals.”³⁴¹ Other opponents to the technique believe that the “technology is unproven and that it stigmatizes the poor by equating welfare recipients with criminals.”³⁴²

One of the most vehement and prolific critics in the debate regarding the application of electronic fingerprinting to the welfare system is James I. Davis, the Western Regional Director for Computer Professionals for Social Responsibility (CPSR). In 1993, he made available on Internet criticisms aimed at preventing or discouraging the implementation in San Francisco of the AFIRM system that he considered as an expensive and additional obstacle to receiving General Assistance (GA). He also shares the belief that “Being poor is technically not a crime, but the fingerprinting scheme reinforces this too common perception.”³⁴³

Davis’ major criticisms against the implementation of electronic fingerprinting in San Francisco illustrate the magnitude and the diversity of issues involved in the debate. They can be summarized as follows:

1. Davis thinks that AFIRM “is based on a presumption of guilt. That is, unless you confirm your innocence of not double-dipping, your are assumed to be guilty of it.

³⁴⁰ «Fingerprint Policy Shrinks Welfare Roll,” *San Jose Mercury News*, 11 June 1993, 1B.

³⁴¹ Steinberg, «Coming Soon: Fingerprints at Many Fingertips,” B1.

³⁴² Kevin Sack, «Cuomo Sanctions Fingerprint Scans. Efforts Against Welfare Fraud May Face Legal Challenge,” *New York Times*, 9 July 1994, 22.

³⁴³ James I. Davis, «New Hearing Set for July 27 on Electronic Fingerprinting for Welfare Recipients in San Francisco,” 21 July 1993 [on-line]; available from <ftp://cpsr.org/ftp/cpsr/fingerprints/sffinger.analysis>; Internet; accessed 29 March 1995.

This contravenes a basic constitutional principle."³⁴⁴ The burden of proof is not written in the Constitution, but it is one of the principles which have a constitutional status.³⁴⁵ It means that it is not up to the defendant to prove his/her innocence but that it is rather up to the government to prove the defendant's guilt beyond a reasonable doubt.

2. The official reason for the implementation of AFIRM in the San Francisco welfare system is the detection of duplicate claims. However, Davis points out that the state identity cards or the driving licenses that welfare applicants have to present before they can receive their grant have already been tightly controlled for potential fraudulent duplication not only by experts from other government agencies such as DMV, but also through existing DSS security measures. Therefore, Davis states that the AFIRM system is unnecessary, that it duplicates government resources and that it cannot be justified for the official reason given by DSS. However, as mentioned in the previous chapter, official documents are often falsified and, as a consequence, unlike fingerprints, they are not totally reliable as far as personal identification is concerned.
3. There are a number of problems which can arise from the mere computerization of fingerprint data. First, the storage of pieces of personal information into government computer systems raises usual and expected privacy concerns. In *Electronic Fingerprinting for General Assistance Recipients in San Francisco*, Davis writes that "Something is given up by individuals when they must surrender personal information to the government; as such, requiring fingerprinting is an erosion of one's right to privacy, which is guaranteed under the California state constitution." Second, the sophisticated technology used in social services can frighten some people. This can result in discouraging eligible candidates from enrolling in welfare programs and can prevent them from receiving benefits they are entitled to. Protagonists of the system, however, do not agree with Davis. Ray Garcia, assistant director of Los Angeles Public Social Services, for example, sees the method as a

³⁴⁴ James I. Davis, *Statement Before the San Francisco Social Services Commission Regarding the AFIRM System*, 16 May 1993 [mailing list on-line]; available from cpsr-activists@CSLI.Stanford.EDU; Internet; accessed 29 March 1995.

way which “merely requires pressing a forefinger on a glass plate for a few seconds,” and he thinks that the process is therefore not scary, not intimidating, and not coercive.³⁴⁶

Third, Davis points out that, contrary to what many people believe, computers are not infallible and they can miss actual cases of fraud. On the other hand, the detection of a match by an AFIS system does not necessarily mean that a fraud occurred. As a matter of fact, some advocates for the poor argue that the administrative hearings held in New York State when the system detects a match take place in order to determine whether the automated system made an error during the matching process.³⁴⁷

Fourth, Davis raises the issue of the general security of computerized data, that is to say, the relative easiness in which they can be duplicated, modified, and transmitted without authorization. Deploing the lack of guarantee against the unofficial and unauthorized use of computerized data, he evokes various cases involving police officers using police records in illegal manners and other cases involving DSS employees sharing information with the police without the proper authorization.

4. Davis underlines an atmosphere of intimidation and confusion among the general welfare population, which is generated by the perception of fingerprinting as a law enforcement method, combined with the perception of computers as infallible systems that can retrieve any data on individuals. The large percentage of welfare recipients suffering from mental illness and/or drug or alcohol addiction probably presents a higher degree of vulnerability in coping with any of the fears associated with a new technology.
5. A further source of concern lies in the sharing of fingerprint data with other government agencies - especially with law enforcement agencies. Davis summarizes some of his concerns as follows:

³⁴⁵ Leonard W. Levy, Kenneth L. Karst, and Dennis J. Mahoney, *Encyclopedia of the American Constitution* (New York: Macmillan Publishing Company, 1986), 170.

³⁴⁶ Quoted in Ellis, “Officials Can’t Lift a Finger to Curb Fraud,” *Los Angeles Times*, 3 August 1993, B8.

³⁴⁷ Fisher, “Pataki Unveils New Rules To Fight Welfare Fraud,” 52.

DSS has assured the Mayor's Office that AFIRM fingerprint information will not be shared with police agencies. The AFIRM and police computer systems are distinct, and department policy forbids sharing of information. However, such assurances are not, and cannot be enough. First, the line between social services and law enforcement is becoming increasingly blurred. The stated rationale for the fingerprinting system is in fact a law enforcement one -- to prevent criminal activity. DSS already works closely with the District Attorney's office in investigating alleged fraud. Information is shared between the agencies; and whether it is the fingerprint itself or information derived from fingerprint searches, the protestations that data sharing will not take place are seriously weakened.³⁴⁸

Davis adds two observations. They show that fingerprint data may become instrumental in increasing the amount of information exchanged between DSS and law enforcement.

First, pursuant section 17006.5 of the California Welfare and Institutions Code, DSS has the authorization, under the conditions it specifies, to provide law enforcement with welfare information. The physical description of a person, which traditionally refers to characteristics such as the height, weight, color of the eyes, etc., is one of them - but Davis finds it conceivable that fingerprints could be encompassed in this general expression.

Second, as police are currently allowed to request DSS officials to search for the name of a person in its database, Davis does not preclude the possibility that similar searches could be conducted in the AFIRM system on the basis of fingerprints provided by law enforcement agencies.

6. Another problem to be considered is the application of electronic fingerprinting to an increasing number of welfare programs. Davis envisions that the method could possibly touch in the future every recipient of government support programs. Such a venture could lead to the creation of what Davis calls a *national poverty database*. Dozens of millions of people could be potentially touched by the AFIS method if it is implemented throughout the welfare system. Statistics clearly indicate that the number of individuals benefiting from welfare assistance has systematically increased in the course of these last decades. For example, between 1988 and

³⁴⁸ Davis, *Statement Before the San Francisco Social Services Commission Regarding the AFIRM System*.

1993, the total number of recipients of Social Security Benefits for the U.S. rose from 37,706,000 to 41,230,000. As for the data regarding programs mentioned earlier in this chapter, the total number of recipients of AFDC rose from 10,707,200 to 14,061,000; and the total number of participants in the Federal Food Stamp Program rose from 18,325,000 to 26,952,000.³⁴⁹ The overall picture is thus of a significant and fast increase in the number of people on welfare. In addition to the above, Davis expresses the concern that AFIS technology could also be applied to children. This would arise new issues, such as the length of time these data would remain in the system. To sum up this point, Davis believes that the application of AFIS technology to more government programs makes it a threat to everyone.

7. Important criticisms concern the evaluation of the savings resulting from the use of AFIS technology in the welfare system. For some authors, "Taken together, the decrease in general assistance clients could result in millions of dollars of savings."³⁵⁰ For others, such as Davis, nobody knows how much will be saved by using the automated method. However, writing specifically about Los Angeles and Alameda Counties, he thinks that the issue of double-dipping may be "quite minuscule."³⁵¹

According to Davis, the savings reported by social services are not accurately measured and they do not reflect real benefits for the social administration. He insists in particular that the savings generated by the automated system have most likely been exaggerated and the costs probably underestimated. AFIRM increases in fact the expenditures and bureaucracy of GA administration because the administrators must purchase, install and maintain new computers, train employees to use the system and adjust their office procedures to the new system.

³⁴⁹ U.S. Department of Commerce, Economic and Statistics Administration, Bureau of the Census, *Statistical Abstract of the United States*. 1995, 15th ed., (Washington, D.C.: GPO, 1995), 381, 388-389; and U.S. Department of Commerce, Economic and Statistics Administration, Bureau of the Census, *State and Metropolitan Area Data Book 1991* (Washington, D.C.: GPO, 1991), 229-230.

³⁵⁰ «Fingerprint Police Shrinks Welfare Roll,» *San Jose Mercury News*, 11 June 1993, 1B.

³⁵¹ Davis, «New Hearing Set for July 27 on Electronic Fingerprinting for Welfare Recipients in San Francisco.»

A second problem concerns the figures used to determine the benefits brought by AFIS technology to the welfare system. It is argued that, while some of them reflect real savings, others do not. The first type of figures is represented by the number of fraudulent cases that have been duly proved; the second, more subjective, includes the savings generated when people refuse to be fingerprinted and, as a consequence of that decision, are not allowed to receive welfare benefits.

In the first place, there are instances reflecting the objective savings generated when the system detects real cases of double-dipping. A few examples follow.

- (1) Within the first six months of the installation of AFIRM in Los Angeles County, "297 welfare recipients were caught, through their fingerprints, trying to apply for duplicate benefits."³⁵² Two years later, the exact cost of fraudulent claims for the General Relief Program in Los Angeles was evaluated at 1.28 percent, which represents an estimated 3-year savings of \$51 million.³⁵³
- (2) LA DSS reports that, through March 1996, the implementation of AFIRM resulted in the application of sanctions against 125 GR recipients.
- (3) As for the fraud in the LA AFDC program, the same report indicates that the District Attorney decided to prosecute 75 of 111 suspected fraud matches that had been investigated through March 1996.³⁵⁴
- (4) In Alameda County, Davis writes that only six fraudulent matches were found among the 9,000 GA cases processed during the first six months of the implementation of AFIRM in that county.
- (5) Finally, in New York State, there are "expanded efforts to detect fraud, both through statewide electronic fingerprinting of welfare recipients and programs to match welfare rolls with other states," namely New Jersey,

³⁵² Steinberg, "Coming Soon: Fingerprints At Many Fingertips", B1.

³⁵³ "Los Angeles Taps Fingerprint Technology," *Government Imaging* (November-December 1994), 19.

³⁵⁴ County of Los Angeles, Department of Public Social Services, *Los Angeles County Department of Public Social Services (DPSS) Automated Fingerprint Image Reporting and Match (AFIRM) System* (16 May 1996), 8.

Pennsylvania, Vermont, Connecticut, Florida, Virginia, and the District of Columbia.³⁵⁵ While the matching method led to the closing of 1,699 welfare cases and therefore to the saving for New York of \$8 million, Fisher writes that “the results of the statewide fingerprinting . . . have been less measurable. The program was running in 38 of the state’s 58 social services districts and has so far found fewer than 100 instances of double-dipping.”

It should also be mentioned that, in some cases, a doubt is clearly expressed regarding the fraudulent origin of the fingerprint match. For example, Davis reports data from the LA DSS Computer Services Division in which it is indicated that eleven duplicate claims were found after six months of the implementation of AFIRM, but no data indicates how many of them were fraudulent.

In the second place, there are instances in which the refusal to be fingerprinted results in the denial of welfare benefits. The question is that the savings occurring in these situations are of a different nature than the objective savings mentioned above because they do not necessarily reflect a fraudulent behavior. Despite the importance of the matter, officials of some social departments did not investigate at first the cause of the rejection of the method by a number of welfare applicants and recipients. This was the case in Alameda County, for instance, where “County officials aren’t sure why people are avoiding the fingerprint requirement, and have no plans to poll them to find out.”³⁵⁶ To the contrary, in the course of its studies conducted prior to the implementation of AFIRM in Los Angeles County, a Fingerprint Sub-Committee established by the Department’s Automation Steering Committee took into consideration a report by DMV showing among other things the positive acceptance of the public to AFIS technology.³⁵⁷ Public reactions - as well as the technology used in the welfare administration - were also surveyed at the request of the federal government by an independent auditor, Ernst & Young. Welfare recipients and community leaders were interviewed “for any hint of fear or resentment about the

³⁵⁵ Fisher, «Pataki Unveils New Rules To Fight Welfare Fraud,» 52.

³⁵⁶ «Fingerprint Policy Shrinks Welfare Roll,» *San Jose Mercury News*, 1B.

³⁵⁷ County of Los Angeles, Department of Public Social Services, *Los Angeles County Department of Public Social Services (DPSS) Automated Fingerprint Image Reporting and Match (AFIRM) System*, 2.

fingerprint requirement, as well as evaluation of the technology.”³⁵⁸ A preliminary evaluation of this study done in October 1994 showed that only three percent of the client population experienced negative feelings about being fingerprinted.³⁵⁹

These negative feelings are expressed in three ways. Some individuals, among which 476 people in Alameda County who balked at the idea of being fingerprinted,³⁶⁰ express their dissatisfaction with the measure. Other people decide to leave the system to avoid being fingerprinted. Finally, some people refuse to be fingerprinted and are therefore immediately rejected from the system. The LA DPSS report states that the number of people who refused to be fingerprinted in the framework of the AFDC program was very low - a total of 50 people.³⁶¹ As for the GR program, the New York Times indicates that 3,010 GR applicants in Los Angeles County were dropped from the system within the first six months of the implementation of AFIRM because they refused to submit to the electronic fingerprinting.³⁶²

Opponents to electronic fingerprinting argue that the savings related to these situations are most likely to occur at a bigger scale during the first phase of the implementation of the method and that they should not be included in the calculation of the projection of future savings. They believe that the implementation of AFIS systems does not deter fraud but results in a diminution in caseloads, causing in that way a large part of the savings. In New York State, for example, when the first evaluations of the automated method were made in the counties of Rockland and Onondaga, no welfare cheater was caught. However, “the counties did save money under the

³⁵⁸ “LA Social Services Taps Fingerprint Technology,” *Government Imaging* (November-December 1994), 18.

³⁵⁹ General Accounting Office, *Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program*, [report on-line]; available from <http://www.vitro.bloomington.in.us:8080/~BC/REPORTS/OSI-9520.html>; Internet; accessed 22 March 1996.

³⁶⁰ “Fingerprint Policy Shrinks Welfare Roll,” *San Jose Mercury News*, 11 June 1993, 1B.

³⁶¹ County of Los Angeles, Department of Public Social Services, *Los Angeles County Department of Public Social Services (DPSS) Automated Fingerprint Image Reporting and Match (AFIRM) System*, 8.

³⁶² Steinberg, “Coming Soon: Fingerprints at Many Fingertips,” B1.

program because fewer people applied for benefits; but it is inconclusive whether the fingerprint was the reason.”³⁶³

Finally, Davis criticizes the notion of “non-compliance” which has been used by social services to deny welfare benefits to hundreds of people in both Los Angeles and Alameda Counties. To his opinion, the concept of “non compliance” includes paperwork’s problems, failure to show up for the fingerprint appointment, confusion about the change in rules, mental disability, etc.³⁶⁴ “Without any data as to why the case load dropped, it is spurious logic at best to assert that fraud has been rooted out. Much more likely reasons for the caseload drop are missed appointments, perhaps because of lost or missed mail; fears about being fingerprinted; concerns about privacy; or the inevitable problems of processing 11,000 cases. A 98.5% rate of success in processing would be admirable in most quality assurance managers’ book; but the other 1.5% that are failures could still account for all the dropped cases.”³⁶⁵

This chapter offered a glance at areas about which opponents of the application of AFIS technology to the welfare system have expressed concerns. Their criticisms are not only about computers and technology, but relate also to the social structure where AFIS systems are implemented and, most importantly, to the effects exerted by the automated systems on a vulnerable segment of the population. They are about sensitive issues such as privacy, responsibility, the rights and duties of the citizens and of the government.

This study cannot demonstrate whether or not AFIS technology is a good fraud deterrent for applications based on multiple identities or for applications made in multiple social service offices. Neither can conclusive comment can be made from the information available in the public domain because there are discrepancies between the figures reported by various authors and organisms, and also because there is no functional definition of what these figures represent. What is sure is that, despite

³⁶³ Ian Fisher, «Albany to Expand Fingerprinting Plan For Welfare Funds,» *New York Times*, B4.

³⁶⁴ Fingerprint Policy Shrinks Welfare Roll, *San Jose Mercury News*, 11 June 1993, 1B.

³⁶⁵ Davis, *Statement Before the San Francisco Social Services Commission Regarding the AFIRM System*.

waves of protests, AFIS systems are being implemented in more social services, and in more social programs. This trend illustrates the determination of government to apply computers to human affairs which in turn raises social and political questions. For example, does the application of AFIS technology to social services lead to discriminatory policies against the welfare population? What does the increasing use of AFIS in the social environment reflect about the U.S. government and the way it deals with social issues? Are we attending the dawn of a tighter "biological surveillance"³⁶⁶ era of the population?

Ultimately, it seems that Michael B. Katz is right when he says that "Welfare in America will never be satisfactory. It cannot escape the contradictions between its goals - deterrence, compassion, discipline and control, and patronage - or resolve the tension between entitlements and the market."³⁶⁷

³⁶⁶ The expression «biological surveillance» is used by Andre Bacard, *The Computer Privacy Handbook* (Berkeley, CA: Peachpit Press, 1995), 30.

³⁶⁷ Michael B. Katz, *In the Shadow of the Poorhouse* (New York: Basic Books, Inc., 1986), 290.

CHAPTER 10

SUMMARY AND GENERAL CONCLUSIONS

The purpose of this study has been to examine the origin, the evolution and the diffusion of the electronic fingerprinting method. More precisely, it investigated the general history of fingerprinting; the manual processing of fingerprints; their automated processing; the evolution of AFIS technology within law enforcement; and the expansion of AFIS technology from law enforcement to other components of the criminal justice system and to other government agencies as well as to the private sector. Finally, the study discussed some issues arising from the use of electronic fingerprinting in the criminal justice setting and in the welfare administration.

The relevant literature published for the most part in the U.S. and available in the public domain was reviewed, including criminal justice publications, U.S. government documents, and articles from the end of the nineteenth century to the mid-1990s. In addition, documentation provided by business corporations, government agencies and scholars was reviewed. Finally, a few complementary interviews were conducted.

The scientific study of fingerprints started in the seventeenth century, but it was not until the beginning of the twentieth century that fingerprints became an identification tool for police in the United States when it replaced the anthropometric system of identification conceived and developed by Alphonse Bertillon, the French criminologist. Fingerprints were systematically gathered, manually processed and recorded on tenprint cards stored in police file cabinets and/or in state and federal repositories. They were traditionally used in a great deal of criminal and noncriminal applications, including the determination or the verification of the identity of victims, unrecognizable bodies, suspects, applicants to a large number of jobs, licenses and permits. Fingerprints were also used in other scientific research such as in medicine in the establishment of the potential relationships between a number of diseases and specific dactylograms; and in anthropology, in the determination of dermatoglyphic patterns differentiating various groups of the population.

There were severe problems in using the manual fingerprinting technique in law enforcement. Among the insufficiencies and drawbacks which seriously limited its efficiency, were the length of time it took to process and exchange fingerprints

between police departments; the classification of the fingerprint patterns in a growing number of subdivisions; mistakes in the filing of fingerprint records; and the poor quality of both latent and inked prints. Moreover, in criminal cases, a major drawback of manual dactyloscopy was that the identification process based on latent prints presupposed the knowledge of the identity of a suspect.

The science of fingerprinting entered a new phase in the early 1960s when the research and development work for its automation was undertaken, signing the beginning of the revolutionary AFIS technology era that permanently changed the fingerprint-based identification processing. It was also an early step in the government record-keeping practice to store biological elements of individuals in its computerized systems.

The criminal justice literature reveals a high level of overall satisfaction related to the use of AFIS technology, especially in local police departments. The crucial importance of using and diffusing the technology is indicative of its increasing institutionalization.

Extremely powerful, fast, and accurate, AFIS systems capture, sort, compress, store, search and print large amounts of fingerprint data. The application of high technologies such as laser technology and computer imaging produces fingerprint images of very high resolution and quality that replicate fingerprint patterns in minute detail. Prints of mediocre quality can be enhanced by the computer or manually enhanced on the screen. This is particularly beneficial in the processing of latent prints which are often, by nature, partial or unclear. The use of portable scanners linked to a central computer makes it possible to perform direct identifications outside police agencies.

AFIS systems can be integrated with various criminal justice information systems and connected to other AFIS systems in intricate networks through which fingerprint images and other vital pieces of criminal information are electronically retrieved and exchanged. These possibilities improve and accelerate the interactions between law enforcement agencies. They also increase the quality of police cooperation through a better access, exploitation and circulation of the wealth of criminal justice information already computerized.

For all these remarkable possibilities, however, AFIS systems are not infallible systems. For example, their operation can be affected by errors or problems in the computer hardware or software. The entire process also depends on the quality of the original prints. Despite possible technological enhancement, some of them are still of such a poor quality that they cannot be accurately read by an AFIS. This of course increases the risk of wrong identifications.

Practical effects of the adoption of AFIS systems are becoming apparent. They include the following: (1) Compared to the manual fingerprinting method, AFIS systems produce a net increase in the number of searches and in the number of identifications that can be done for both criminal and noncriminal purposes in a given period of time. (2) Effective cold searches run on digitized prints can be successfully conducted in databases of any size and lead to the elucidation of new and previously unsolved crimes. (3) Electronic systems increase the accuracy of the processing of fingerprints. It is generally agreed that, among other effects, this has a positive influence on the protection of people's civil rights because, as the number of mistaken and missed identifications is reduced, dramatic situations such as the incarceration of innocent people are better prevented. In addition, the release of wanted criminals who can now be accurately identified within the required time is also prevented. (4) AFIS systems are becoming effective electronic crime fighting devices. In 1987, a report published by the Department of Justice indicated that they seemed to have contributed to a downtrend in crime statistics. The rate of residential burglary in San Francisco decreased by 25 to 26 percent between 1983 and 1987, that is, during the first four years of the installation of the police AFIS system.

The automation of fingerprint records cannot be studied apart from the global computerization of criminal justice information. It is important to remind that a decisive step in the irreversible trend towards the automation of police records occurred with the 1967 report of the President's Commission on Law Enforcement and Administration of Justice. "According to the Commission, the American criminal justice system of the late 1960's was overburdened and fragmented; information concerning

crime was often incomplete, inaccurate, or unavailable. The Commission proposed the use in the criminal justice system of 'computer-based information systems'.³⁶⁸

Thirty years after the publication of this report, the following observations can be made. First, a large amount of law enforcement computer-based information systems have been devised over the years. Soon, the NCIC 2000 will probably stand out as the most remarkable system in the world, in particular because of the changes it will enable in the dynamics of the identification process across the country. The complexity and the comprehensiveness of law enforcement automated systems keep increasing with the continuous advances in information technology. For example, they encompass not only information based on text (like criminal justice records and other documents), but also on images (like fingerprints, foot prints, mug shots, etc.), sound (voice print), genetic material (DNA prints), etc.

Second, a large percentage of computerized criminal justice records are still characterized by their poor quality. It has been noted that, as AFIS technology has not been conceived to deal with this critical issue, it is hardly surprising that it cannot solve it. However, the combination of several factors can possibly result in the intensification of the ongoing process of improvement of existing criminal justice record systems. They include the following: (1) thanks to their capability to detect aliases, to recognize people who hide their identity, and to connect various electronic fingerprinting systems, AFIS can help in the consolidation and in the updating of records filed under different names or numbers, or stored in various jurisdictions; (2) because it is a relatively recent technology still in the process of being implemented on a large scale, AFIS can contribute to the establishment of new priorities, revised standards or procedures for the correction and maintenance of dependable criminal justice records. The pressure exerted by citizens and the government can further intensify this whole process.

The crucial importance of such a task is due primarily to the direct relationship between the concepts of *identification* provided by the fingerprint record of a person, the quality of the *information* found in criminal justice records, and the fairness of the *decisions* made on the basis of these data.

³⁶⁸ Donald L. Doernberg and Donald H. Zeigler, "Due Process Versus Data Processing: An Analysis of Computerized Criminal History Systems," *New York University Law Review*, December 1980, 1120.

Third, AFIS technology has the potential to tie up criminal record systems in integrated justice information systems based on unique biometric features. Identifications done in a booking facility with an AFIS system can be directly transmitted online to other components of the criminal justice system, without duplicating the criminal records.

Although it tends to enhance the running of the criminal justice system, the computerization of criminal information also creates new problems. "The major advantage of computerized criminal information is that information is accessible to users nationwide. Computerized information, however, is not necessarily more accurate than manual file systems, and because computer data bases increase accessibility, the effect of inaccuracies is magnified."³⁶⁹ As a matter of fact, the unauthorized access and the improper use of the information by police officers have been cited as a particular source of concern.

Originally designed mainly as law enforcement devices, AFIS systems began to spread outside that field, constantly broadening the spectrum of their applications in a society largely based on the quest for identity and on the request of identification. The definite promotion of AFIS technology after about thirty years of research and development can be explained by the conjunction of factors such as its remarkable technological efficiency, a significant decrease in the cost of the systems, and their possible adjustment to a variety of identification needs. By way of illustration, they are successfully implemented in such settings as a number of government agencies such as the DEA, DMV, INS, IRS, NASA, and the U.S. Secret Service. They are also spreading in the private sector, that is, in banks; high security corporations; plants; in the medical field; in the fight for child protection, etc. At a smaller scale, they can enhance personal safety when, used instead of keys, they authorize the access to private facilities.

The review of the literature related to the implementation of AFIS technology outside law enforcement indicates that it is generally well-accepted when it is used in a

³⁶⁹ Patrick Hand, "Probable Cause Based on Inaccurate Computer Information: Taking Judicial Notice of NCIC Operating Policies and Procedures," *Fordham Urban Law Journal*, 10, no. 3, (22 June 1982), 498.

number of security purposes or in the identification of criminals. However, a new trend appears in which the public seems to display some reluctance to adopt the method. Therefore, more surveys attempt to determine its level of acceptability before introducing it in new applications. A case in point is the proposal, eventually rejected, to adopt the AFIS concept in the identification of all the travelers in U.S. airports.

A number of important questions also arise when AFIS technology is used as a solution for deterring specific cases of fraud. This is particularly true for the introduction of AFIS technology in several welfare administrations that have been plagued over the years with a fraudulent practice known as double-dipping. In order to fight this type of fraud, applicants and recipients of welfare benefits in a few counties of the country are requested to submit to the electronic fingerprinting procedure. Two major observations can be made. First, this mandatory practice is vividly associated with the identification of criminals by law enforcement and it is therefore perceived by several opponents as a coercive and dehumanizing procedure that stigmatizes a vulnerable segment of the population. Second, although it seems clear that identifications based on positive identifiers should in theory curb the double-dipping fraud, it is impossible to assert, from the conflicting data we gathered, whether this objective has been met up until now and whether the technique is cost-effective in welfare administrations.

What is clear is that the introduction of AFIS technology in social welfare administration and its possible extension to all the existing government support programs sustain definite fears about the creation of what has been referred to as a *national poverty database*. This also reinforces the ongoing debate about the bulk of personal information massively gathered, computerized and stored by government agencies. Underlying these critical issues is of course the controversy surrounding the delicate balance between the individual right to privacy and the government need for personal information. Andre Bacard perfectly illustrates some of the concerns related to these points when he writes that "Biological surveillance is a new fashionable enemy to privacy."

There are overriding questions that emerge from the application of AFIS technology in law enforcement and in the welfare administration. They include the following.

First, it has been noted that there is an increasing demand for police and for welfare information and that a larger number of government employees in each setting have now access to these data. Unfortunately, while it is true that there are stringent measures aiming at protecting both the integrity of the data stored in government computers and the personal privacy of the record subjects, it is also true that there are documented cases of misuse of these confidential data by a number of government employees. This highlights the growing importance of data reliability; the necessity to improve the existing safeguard measures and to establish a stricter control over computerized information; and lastly but maybe more importantly, this highlights the need for more ethics, integrity and professionalism on behalf of those with access to personal information.

Second, as AFIS technology becomes more institutionalized and therefore more powerful, concern has grown about the creation of new national identification systems and about database sharing between government agencies, mainly between criminal justice institutions, DMV, INS and the welfare administration. It should be remembered that, at the present time, AFIS technology is not yet implemented at the national scale, neither in law enforcement, nor in the welfare administration. But it seems that it will be just a matter of time before this happens.

Through a general presentation of the implementation and diffusion of electronic fingerprinting technology, this paper has illustrated several conflicts and interrogations expressed by a fast-moving society in search of new ways to express itself, a digital society that we are building a little more every day. However the way it is perceived, it is clear that AFIS technology will keep on spreading in multiple applications. And so, paradoxically, starting from the analysis of simple fingerprint patterns symbolizing the uniqueness of each of us, the scope of AFIS technology is growing so that it can now be used in the screening of the expectations, motivations, goals, values, and needs of an entire nation.

BIBLIOGRAPHY

- Abbinanti, C.A. "Computers Help Match Fingerprints." *Chicago Tribune* (10 January 1994): L3.
- Adams, Thomas F. *Law Enforcement: An Introduction to the Police Role in the Criminal Justice System*. 2d ed. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1973.
- "Adaptive Pattern Recognition Applied to Fingerprint Identification." *Government Imaging* 3, no. 5 (July 1994): 16.
- Adelson, Andrea. "Faster, More Accurate Fingerprint Matching." *New York Times* (11 October 1992): 9.
- "Advanced Technology Meets Toughest-Yet Federal Requirement; FBI Awards Image Quality Specifications 'IQS' Accreditation to Identix TouchPrint 600 Live-Scan Fingerprint System; First and Only Such Approval Granted Worldwide." *Business Wire* 29 March 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 5 April 1995.
- "ADVISORY/LaserCard to Be Demonstrated at Card Technology/Card Security Conference." *Business Wire* (11 April 1995) [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 16 April 1995.
- Alpert, Geoffrey P. *The American System of Criminal Justice*. vol. 1, *Law and Criminal Justice Series*. Beverly Hills: Sage Publications, 1984.
- American Civil Liberties Union. *Thumbs Down! The Fingerprint Menace to Civil Liberties*. New York: American Civil Liberties Union, 1938.
- Anenson, Joyce V. "The FBI's First 75 Years." *FBI Law Enforcement Bulletin* 52, no. 7 (July 1983): 2-11.
- Anthes, Gary H. "A Picture's Worth a Thousand Passwords." *Computerworld* (29 May 1995): 66.
- "AT&T Smart Cards May Become World Standard for Cashless Wallets, Electronic Commerce." *Business Wire* 31 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 6 June 1995.
- "Attorney General and INS Commissioner Showcase High Tech Tools in Fight Against Illegal Immigration." *PR Newswire* 23 March 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 29 March 1995.
- "Attorney General Announces New Initiatives to Remove Criminal Aliens; Los Angeles County Jail Site of Landmark Pilot Project." *PR Newswire* 22 May 1995 [wire

services on-line]; available from <http://www.infoseek.com>; Internet; accessed 27 May 1995.

"Automated Child Welfare Information System Implemented in Oklahoma." *Government Imaging* (September 1995): 8.

Bacard, Andre. *The Computer Privacy Handbook*. Berkeley, CA: Peachpit Press, 1995.

Bailey, William G., ed. *The Encyclopedia of Police Science*. New York: Garland Publishing, Inc., 1989.

Baker, Bob, and Paul Lieberman. "Faulty Ballistics in Deputy's Arrest. Eagerness to 'Make' Gun Cited in LAPD Lab Error." *Los Angeles Times* (22 May 1989): 1, 3, 18.

Ballinger, Tom. *Clean Slate: A State-by-State Guide to Expunging an Arrest Record*. New York: Harmony Books, 1979.

Bank, David. "FBI Fighting its Own War of Security vs. Freedom." *San Jose Mercury News* (4 February 1991): 1A.

Bank, David. "FBI War Powers Stir Civil Rights Concerns." *San Jose Mercury News* (4 February 1991): 1A.

"Banks Seek Ways to Thwart Bogus-ATM Scheme." *San Jose Mercury News* (21 May 1993): 3C.

Banner, Conrad S., and Robert M. Stock. "The FBI's Approach to Automatic Fingerprint Identification (Part I)." *FBI Law Enforcement Bulletin* 44, no. 1 (January 1975): 2, 24.

-----, "The FBI's Approach to Automatic Fingerprint Identification (Part II)." *FBI Law Enforcement Bulletin* 44, no. 2 (February 1975): 26, 31.

Barnow, Erik, ed., et al. *International Encyclopedia of Communications*. New York: Oxford University Press, 1989.

Battley, Harry. *Single Finger Prints: A New and Practical Method of Classifying and Filing Single Finger Prints and Fragmentary Impressions*. New Haven: Yale University Press, 1948.

Baxes, Gregory A. *Digital Image Processing. A Practical Primer*. Engelwood Cliffs, NJ :Prentic-Hall, Inc., 1984.

Becklund, Laurie, and Ted Rohrich. "Crime Computer is a Help, but Can't Do It All." *Los Angeles Times* (5 January 1991): A31.

- Beckman, Erik. *The Criminal Justice Dictionary*. 2d ed., rev. Ann Arbor, Mi: Pierian Press, 1983.
- Belair, Robert R. 1988. See U.S. Department of Justice. 1988.
- Bennet, Robert A. "Refining the Art of Fingerprinting." *New York Times* (11 November 1987): D10.
- Bennun, Mervyl E., ed. *Computers, Artificial Intelligence and the Law*. Chichester, West Sussex (England): Ellis Horwood Limited, 1991.
- Bentfield, Ken. "A Quiet, Deadly Weapon Against Crime: The Integrated Criminal Justice Information System." *Government Imaging* (August 1995): 14-15.
- Berens, John F. *Criminal Justice Documents: A Selective, Annotated Bibliography of U.S. Government Publications since 1975*. Bibliographies and Indexes in Law and Political Science, Number 7. New York: Greenwood Press, 1987.
- Berg, Bruce L. *Law Enforcement: An Introduction to Police in Society*. Boston : Allyn and Bacon, 1992.
- Bertillon, Alphonse. *Signaletic Instructions: Including the Theory and Practice of Anthropometrical Identification*. New York: Werner Company, 1896.
- Berton, Lee. "Software Matches Thief and Prints, Just Like the Movies." *Wall Street Journal* (2 March 1994): B1, B2.
- Betts, Mitch. "Computer Matching Nabs Double-Dippers." *Computerworld* (18 April 1994): 90.
- , "Fed Budget Proposal Kicks in Extra Grant, Technology Funds." *Computerworld* (14 February 1994): 4.
- , "Gun Law Mandates Criminal Database in Five Years." *Computerworld* (6 December 1993): 24.
- , "Personal Data More Public Than You Think." *Computerworld* (9 March 1992): 1, 14.
- Black, Henry Campbell. *Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern*. 5th ed., abr. St Paul, MN: West Publisher Co., 1983.
- , *Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern*. 6th ed., abr. St Paul, MN: West Publisher Co., 1991.

- Block, Eugene B. *Fingerprinting: Magic Weapon against Crime*. New York: David McKay Company, Inc., 1969.
- Bohan, Caren. "FBI Backs Bill That Would Crack Down on Information Brokers." *Reuter Business Report* (30 July 1992).
- Booker, Ellis. "Digital Photo Bank Aids Missing-Kid Search." *Computerworld* (28 February 1994): 41.
- "Border Busts: Targeting Casual Drug Users." *Time* (4 April 1988): 22.
- Bouza, Anthony V. *The Police Mystique: An Insider's Look at Cops, Crime, and the Criminal Justice System*. New York: Plenum Press, 1990.
- Brancheau, JamesC., and James C. Wetherbe. "Key Issues in Information Systems Management." *MIS Quarterly* (March 1987): 23-36.
- Branscomb, Anne Wells. *Who Owns Information? From Privacy to Public Access*. New York: HarperCollins Publishers, Inc., 1994.
- Breslin, Anne. "Imaging in the Court Room." *Inform* (September 1994): 28.
- Brooks, Daniel T. and Suzan H. Nycum. *Computer Crime: Prevention, Detection, Prosecution*. New York: Law & Business, Inc., 1983.
- Brotman, Bruce J., and Rhonda K. Pavel. "Identification: A Move toward the Future." *FBI Law Enforcement Bulletin* 60 (July 1991): 1-6.
- Brown, David. "Arches, Loops and Whorls Make Your Mark on the World Unique." *Washington Post* (3 July 1995): A3.
- Browne, Douglas, and Alan Brock. *Fingerprints: Fifty Years of Scientific Crime Detection*. New York: E. P. Dutton and Co., Inc., 1954.
- Bulkeley, William M. "Police Turn to Databases to Link Crimes." *Wall Street Journal* (8 March 1993): B5.
- Buraker, Carroll D., and William K. Stover. "Automated Fingerprint Identification: Regional Application of Technology." *FBI Law Enforcement Bulletin* (August 1984): 1-5.
- Burnham, David. "F.B.I. Says 12,000 Faulty Reports on Suspects Are Issued Each Day." *New York Times* (25 August 1986): 1, 30.
- Cameron, Jerry. "Artificial Intelligence, Expert Systems, Microcomputers and Law Enforcement." *The Police Chief* 57, no. 3 (March 1990): 36-41.

- Campbell, Dennis and Joy Fisher, eds. *Data Transmission and Privacy*. Boston: Martinus Nijhoff Publishers, 1994.
- Carr, Rebecca, and Jim Casey. "Fingerprint Controversy Adds to Palatine Puzzle." *Chicago Sun-Times* (23 March 1994): 16.
- Caudle, Sharon L. "High Tech to Better Effect." *The Bureaucrat* (Spring 1987): 47-52.
- Chapel, Charles Edward. *Fingerprinting: A Manual of Identification*. New York: Coward McCann, Inc., 1941.
- Cherrill, Frederick R. *The Finger Print System at Scotland Yard: A Practical Treatise on Finger Print Identification for the Use of Students and Experts and a Guide for Investigators when Dealing with Imprints Left at the Scenes of Crime*. London: Her Majesty's Stationery Office, 1954.
- Chu, Jeannette L. "Alien Smuggling." *The Police Chief* (June 1994): 20-27.
- Clancy, Heather. "Inkless Fingerprints Aids Field Users -- Crime Fighter: Printrak Technology." *Computer Reseller News* (28 March 1994): 53.
- Clarke, Roger A. "Information Technology and Dataveillance." *Communications of the ACM* 31, no. 5 (May 1988): 498-512.
- Clements, Wendell W. *The Study of Latent Fingerprints: A Science*. Springfield, IL: Charles C. Thomas, Publisher, 1987.
- Clinton, Terry W. *Policing Society: An Occupational View*. New York: Wiley, 1985.
- The Commission on Peace Officer Standards and Training. *Law Enforcement Records Management*. 2d ed. State of California, 1991.
- "Comparator Systems Corp. Banks Product Development Funding; Final Fingerprint ID Production Model Now in Engineering." *Business Wire* 5 June 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 10 June 1995.
- "Comparator Systems Corp. Chosen for Use in National Identification Card Project." *Business Wire* 6 March 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 11 March 1995.
- "Comparator Systems Corp. Gears up for Financing, Foreign Contract." *Business Wire* 9 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 15 May 1995.
- "Computerized Child Fingerprint Repository." *Law and Order* (March 1992): 111.

"Conviction Through Enhanced Fingerprint Identification." *FBI Law Enforcement Bulletin* (December 1992): 16-17.

County of Los Angeles. Department of Public Social Services. *Los Angeles County Department of Public Social Services (DPSS) Automated Fingerprint Image Reporting and Match (AFIRM) System*. 16 May 1996.

"County Uses Magic to Automate Its Welfare System." *Government Imaging* (March 1995): 16

"Court Won't Back Fingerprint Ruling." *San Jose Mercury News* (13 June 1992): 3B.

Cowger, James F. *Friction Ridge Skin: Comparison and Identification of Fingerprints*. New York: Elsevier, 1983.

Cox, Steven M., and John E. Wade. *The Criminal Justice Network: An Introduction*. Wm. C. Brown Publishers, 1985.

Culnan, Mary J. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use." *MIS Quarterly* (September 1993): 341-360.

Cummings, Harold, and Charles Midlo. *Finger Prints, Palms and Soles*. South Berlin, MA: Research Pub. Co., 1976.

Danzinger, James N., and Kenneth L. Kraemer. "Computerized Data-Based Systems and Productivity among Professional Workers: The Case of Detectives." *Public Administration Review* (January/February 1985): 196-209.

Davis, James I. "New Hearing Set for July 27 on Electronic Fingerprinting for Welfare Recipients in San Francisco." 21 July 1993 [on-line]; available from <ftp://cpsr.org/ftp/cpsr/fingerprints/sffinger.analysis>; Internet; accessed 29 March 1995.

----- "Electronic Fingerprinting of Welfare Recipients in CA." Presented at the PRIVACY Forum Digest, Topanga, CA., 27 May 1993 [on-line]; available from <http://www.vortex.com/privacy.htm>; Internet; accessed 29 March 1995.

----- "Statement Before the San Francisco Social Services Commission Regarding the AFIRM System." 16 May 1993 [mailing list on-line]; available from cpsr-activists@CSLI.Stanford.EDU; Internet; accessed 29 March 1995.

Davis, Paul R. "Records of Arrest and Conviction: A Comparative Study of Institutional Abuse." *Creighton Law Review* 13 (1980): 863-888.

- Deakin, Thomas J. *Police Professionalism: The Renaissance of American Law Enforcement*. Springfield, IL: Charles C. Thomas Publisher, 1988.
- Dictionary of National Biography*. Oxford: Oxford University Press. 1965.
- Diehm, James W. "Federal Expungement: A Concept in Need of a Definition." *St. John's Law Review* 66, no. 1: 73-106.
- "Digital Biometrics Announces Orders." *PR Newswire* 11 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 17 May 1995.
- "Digital Imaging Discourages Child Abduction." *Law and Order* (June 1994): 29-34
- Dilulio, John J. 1992. See U.S. Department of Justice. 1992.
- Dinkelspiel, Frances. "County Fingerprinting Those on Welfare." *San Jose Mercury News* (26 February 1993): 1B, 6B.
- Doernberg, Donald L., and Donald H. Zeigler. "Due Process versus Data Processing: An Analysis of Computerized Criminal History Information Systems." *New York University Law Review* 55, no. 6 (December 1980): 1110-1230.
- Dunlop, Charles and Rob Kling. *Computerization and Controversy. Value Conflicts and Social Choices*. San Diego: Academic Press, Inc., 1991.
- Eckert, William G., and Stuart H. James. *Interpretation of Bloodstain Evidence at Crime Scenes* New York: Elsevier, 1989.
- Ekstrand, Laurie E. 1993. See U.S. General Accounting Office. 1993.
- Ellis, Virginia. "Officials Can't Lift a Finger to Curb Fraud." *Los Angeles Times* (3 August 1993): B1, B8.
- Emigh, Jacqueline. "Miro's Intros 'Computer Face Recognition' Technology." *Newsbytes, Boston - News* (9 June 1994).
- Faulds, Henry. "On the Skin-furrows of the Hand." *Nature* (28 October 1880): 605.
- Fay, John J. *The Police Dictionary and Encyclopedia*. Springfield, IL: Charles Thomas Publisher. 1988.
- "FBI Announces Multi-Million Dollar Contract in Effort to Modernize National Crime Information Center." *U.S. Newswire* (19 March 1993).
- "FBI Says Reported Crimes Rose 8% in First Half of Year." *New York Times* (15 October 1986): B13.

- Ferraro, Donald W. "The Integrated Computerization of a Small Department." *The Police Chief* (December 1994): 14-18.
- Field, Annita T. *Fingerprint Handbook*. Springfield, IL: Charles C. Thomas, Publisher, 1959.
- Fielding, Jeannine R. "Imaging an Integral Part of INS Border Control Improvements." *Government Imaging* 3, no. 8 (October 1994): 1, 8.
- Fincher, Jack. "Lifting 'Latents' Is Now Very Much a High-Tech Matter." *Smithsonian* (October 1989): 201-202.
- "Fingermatrix Introduces New High-Performance Live Fingerprint Scanner." *Business Wire* 8 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 13 May 1995.
- "Fingermatrix Patents Advanced Electronic Fingerprinting Technology." *Business Wire* 1 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 7 May 1995.
- "The Fingerprint Myth Turns Real." *New York Times* (18 April 1992): K18.
- "Fingerprint Plan for School Workers." *Washington Post* (19 January 1988): B4.
- "Fingerprint Policy Shrinks Welfare Roll." *San Jose Mercury News* (11 June 1993): 1B.
- "Fingerprints of Workers May Be Kept." *Finger Print and Identification Magazine* (May 1972): 23.
- Fisher, Barry A. *Techniques of Crime Scene Investigation*. 5th ed. New York: Elsevier, 1992.
- Fisher, Ian. "Albany to Expand Fingerprinting Plan for Welfare Funds." *New York Times* (7 June 1994): A1, B4.
- , "Pataki Unveils New Rules to Fight Welfare Fraud." *New York Times* (10 September 1995): 52.
- Fjetland, Raymond, and Charles Robbins. "The AFIS Advantage: A Milestone in Fingerprint Identification Technology." *The Police Chief* (June 1989): 20-22.
- Flaherty, David H. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." *Science, Technology and Human Values* 11, no. 1 (Winter 1986): 7-18.
- "Focus on NCIC." *FBI Law Enforcement Bulletin* 59 (January 1990): 27.

- Folsom, William. "Automated Fingerprint Identification Systems." *Law and Order* (July 1986): 26-28.
- Freedberg, Louis. "Reno Wants to Fingerprint Illegals Who Get Caught." *San Francisco Chronicle* (3 June 1994): A3.
- Gamble, F. T., L.M. Frye, and D.R. Grieser. "Real-Time Fingerprint Verification System." *Applied Optics* 31, no. 5 (10 February 1992): 652-655.
- General Accounting Office. *Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program*. [report on-line]; available from <http://www.vitro.bloomington.in.us:8080/~BC/REPORTS/OSI-9520.html>; Internet; accessed 22 March 1996.
- General Accounting Office. *Food Assistance - Potential Impacts of Alternative Systems for Delivering Food Stamp Program Benefits*. Report to Congressional Committee. Chapter Report. GAO/RCED-95-13. 16 December 1994.
- Glasheen, L. "Crime and Politics." *Security Management* 26, no. 1 (January 1982): 66-68.
- Goldston Linda. "State Lags in Checking Day Care Workers." *San Jose Mercury News* (22 December 1993): 1A.
- Goodpasture, Victor. "Kodak's Project KIDS - The Latest in Law Enforcement." *Inform* (September 1994): 23-28.
- Gordon, Diana R. "The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System." *Politics and Society* 15, no. 4 (1986-1987): 483-511.
- Gray, Susan H. "Electronic Data Bases and Privacy: Policy for the 1990s." *Science, Technology & Human Values* 14, no. 3 (Summer 1989): 249.
- Greene, William B. *Digital Image Processing. A Systems Approach*. New York: Van Nostrand Reinhold Company. 1983.
- Greenhouse, Linda. "Court Weighs Ramifications of Digital Age." *New York Times* (8 December 1994): A21.
- Greenwood, Peter W., Jan M. Chaiken, and Joan Petersilia. *The Criminal Investigation Process*. Lexington, MA: D.C. Heath and Company, 1977.
- Greguras, Fred M. and David J. Sykes. "Authentication in EFT: The Legal Standard and the Operational Reality." *The Computer Law Journal* (1980) : 67-85.

- The Guide to American Law: Everyone's Legal Encyclopedia*. San Francisco: West Publishing Company, 1984.
- Gunn, Angela. "Catching Criminals." *PC Magazine* (27 October 1992): 32.
- Gunnison, Robert B. "Wilson Welfare Ideas Scotched. Fingerprinting Would Continue." *San Francisco Chronicle* (21 April 1994): A17, A24.
- Haglund, William D. "The National Crime Information Center (NCIC) Missing and Unidentified Persons System Revisited." *Journal of Forensic Sciences* 38, no. 2 (March 1993): 365-378.
- Haines, Gerald K., and David A. Langbart. *Unlocking the Files of the FBI: A Guide to Its Records and Classification System*. Wilmington, DE: Scholarly Resources Inc., 1993.
- Hall, David G. "New Remote, Interactive Technology Enables Linkage of AFIS Systems." *The Police Chief* (October 1987): 61-63.
- Hand, Patrick. "Probable Cause Based on Inaccurate Computer Information: Taking Judicial Notice of NCIC Operating Policies and Procedures." *Fordham Urban Law Journal* 10, no. 3 (22 June 1982): 497-510.
- "Handwriting on the Wall: Fingerprint Technology Buying Surges in 1995." *Business Wire* 30 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 6 June 1995.
- "Harris Corporation Wins \$47 Million Contract to Upgrade FBI's National Crime Information Center." *PR Newswire* (19 March 1993).
- Hazlett, Bill. "Fingerprints: The Only Certain ID." *Los Angeles Times* (22 April 1973): II 1-3.
- Hebenton, Bill, and Terry Thomas. *Criminal Records: State, Citizen and the Politics of Protection*. Brookfield, Vermont: Avebury, 1993.
- Hedges, Michael. "Clinton, Giuliani Discuss Nationwide Gun Licensing." *Washington Times* (8 December 1993): A4.
- Hempel, Walter T. "INS Offers Investigative Aid." *The Police Chief* (June 1994): 36.
- Henderson, Joel H., and David R. Simon. *Crimes of the Criminal Justice System*. Cincinnati, OH: Anderson Publishing Company, 1994.
- Herschel, William James. "Skin Furrows of the Hand." *Nature* (25 November 1880): 76.
- Higgins, Joan C. "NCIC and Alien Apprehensions." *The Police Chief* (June 1994): 28-29.

"Homestead NAACP Chided on Fingerprint Support [sic]." *Jet* 73 (28 September 1987): 7.

Hoover, John Edgar. 1937. See U.S. Department of Justice. 1937.

-----, The Role of Identification in Law Enforcement: An Historical Adventure (Part One). *FBI Law Enforcement Bulletin*. (March 1973): 8-13, 29-30.

-----, The Role of Identification in Law Enforcement: An Historical Adventure (Part Two). *FBI Law Enforcement Bulletin*. (April 1973): 22-25.

Horten, Monica. "Long Arm of Law Puts a Finger on High Tech Computers." *Daily Telegraph* (16 August 1993): 25

Hrechak, Andrew K. "Police Automation: Automated Fingerprint Recognition." Ph.D. diss., State University of New Jersey, 1988.

Hutt, Arthur E., ed. et al. *Computer Security Handbook*. New York: John Wiley and Sons, Inc., 1995.

"IAFIS: The Real Story." [file on-line]; available from <http://www.fbi.gov/iafis/story.htm#results>; Internet; accessed 2 March 1997.

"Identix Chosen for Fingerprint Identification by NRI, Unisys for Respective Welfare Verification Systems in New Jersey, San Diego; Exclusive Live-Scan in All Such Systems." *Business Wire* 24 April 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 30 April 1995.

"Identix Contracts with Maryland Department of Public Safety for Statewide Fingerprint, Mug Shot Verification System; Initial Order Worth approximately \$900,000." *Business Wire* 1 June 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 6 June 1995.

"Identix, Oracle Agree to Market Integrated Database Security Software System with Fingerprint Verification; Oracle Databases Hold Half of World's Information." *Business Wire* 2 May 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 7 May 1995.

"Identix, Morpho to Install Statewide Fingerprint Capture, Transmission System for Arizona Law Enforcement Agencies; Identix Orders Valued at about \$1.7 Million." *Business Wire* 8 August 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 13 August 1995.

Icove, David, Karl Segers and William VonStorch. *Computer Crime: A Crimefighter's Handbook*. Sebastopol, CA: O'Reilly & Associates, Inc., 1995.

- "Innovative Identification Technology Delivers a One-Two Punch on Crime; Printrak's Live-Scan Station Integrates Fingerprint/Mugshot Imaging." *PR Newswire* 8 August 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 13 August 1995.
- Irwin, Don. "Study Cites Automated Fingerprint Identification System; Computer Technology Reportedly Cutting Crime Rate." *Los Angeles Times* (4 May 1987): 4.
- Isikoff, Michael. "Theft of U.S. Data Seen as Growing Threat to Privacy." *Washington Post* (28 December 1991): A1-A4.
- Jacobs, Joanne. "A Decade after '1984': I.D. Cards?" *San Jose Mercury News* (15 August 1994): 7B.
- Janosik, Robert J., ed. *Encyclopedia of the American Judicial System: Studies of the Principal Institutions and Processes of Law*. 3 vols. New York: Charles Scribner's sons, 1987.
- Johnson, Don M. "NCIC Training. Hit or Miss." *FBI Law Enforcement Bulletin* 60 (January 1991): 1-3.
- Johnson, Steve. "Someday, Computers May Recognize Your Face." *San Jose Mercury News* (2 June 1993): 13A.
- Kadish, Sanford H., ed. *Encyclopedia of Crime and Justice*. 4 vols. New York: The Free Press, 1983.
- Kallman, Ernest A., and John P. Grillo. *Ethical Decision Making and Information Technology: An Introduction with Cases*. San Francisco: Mitchell McGraw-Hill, 1993.
- Katz, Michael B. *In the Shadow of the Poorhouse*. New York: Basic Books, Inc., 1986.
- Kenney, Dennis Jay, ed. *Police and Policing: Contemporary Issues*. New York: Praeger, 1989.
- "Kids' Clothes and Toy Fair." *San Jose Mercury News* (30 September 1993): 10C.
- Kirkland, Michael. "New Technology to Process Aliens." *BC Cycle* (2 June 1994).
- ". "Technology Would Free up Officers." *BC Cycle* (2 June 1994).
- Klein, Michael W. "A Case of Mistaken Identity." *Newsweek* (19 December 1994): 20.

- Klug, David, Joseph L. Peterson, and David A. Stoney. *Automated Fingerprint Identification Systems: Their Acquisition, Management, Performance, and Organizational Impact*. National Institute of Justice, 1992. NCI-13749.
- Kuhne, Frederick. *The Fingerprint Instructor*. New York: Munn and Co., Inc., 1935.
- Kurre, Dennis G. "FBI Felon Identification System." *Congressional Digest* 70, nos 6-7 (June-July 1991): 168-169.
- ". "On-line Exchange of Fingerprint Identification Data." *FBI Law Enforcement Bulletin* 56, no.12 (December 1987): 14-16.
- LaFraniere, Sharon, and George Lardner. "U.S. Set to Photograph, Fingerprint All New Iraqi and Kuwaiti Visitors. Unusual Move Taken to Try to Counter Possible Terrorist Attacks." *Washington Post* (11 January 1991): A23, A27.
- Lambert, Jean L. F., comp. 1991. See Ministry of the Solicitor General.1991.
- LaPedus, Mark, and Dave Andrew. "PCs Catch Criminals Using Fingerprint Analysis." *Byte* (October 1993): 34.
- Lardner, George, and Walter Pincus. "George's Prints Found on Portion of Iran-Contra Paper, FBI Expert Says." *Washington Post* (7 August 1992): A6.
- "LA Social Services Taps Fingerprint Technology." *Government Imaging* 3, no. 9 (November/ December 1994): 18-19.
- Laudon, Kenneth C. *Dossier Society. Value Choices in the Design of National Information Systems*. New York: Columbia University Press, 1986.
- Law Enforcement Reference Manual and Police Official Diary*. Trenton, NJ: Irving B. Zeichner editor, 1979.
- "Law Enforcement Enlists Fingerprint Technology to Fight Crime; Contract Awards Latest in String of Wins for Printrak International." *Business Wire* 27 April 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 3 May 1995.
- "Laws Alone Won't Stop Child Abuse." *San Jose Mercury News* (29 December 1993): 6B.
- Lee Henry C., and R.E. Gaensslen. *Advances in Fingerprint Technology*. New York: Elsevier. 1991.
- Leland, Joachim. "Club Project Will Fingerprint, Videotape Kids for Parents." *San Jose Mercury News* (24 February 1993): 2.

- Leonard, Vivian Anderson. *The Police Records System*. Springfield, IL: Charles C. Thomas Publisher, 1970.
- Lesce, Tony. *The Privacy Poachers: How the Government and Big Corporations Gather, Use and Sell Information About You*. Port Townsend, WA: Loompanics Unlimited, 1992.
- Levander, Michelle. "Employers, Investigators Trample Privacy." *San Jose Mercury News* (27 June 1993): 1E.
- Levine, Emil H. *Information Science: Law Enforcement Applications*. n.p. Anderson Publishing Co., 1979.
- Lindberg, Richard. *To Serve and Collect*. New York: Praeger, 1991.
- Loch, Karen D., Houston H. Carr, and Merrill E. Warkentin. "Threats to Information Systems: Today's Reality, Yesterday's Understanding." *MIS Quarterly* 16, no. 2 (June 1992): 173-186.
- Lochhead, Carolyn, and Rob Haeseler. "Database Could Have Helped Polly." *San Francisco Chronicle* (8 December 1993): A15-A16.
- Loesch, Danuta Z. *Quantitative Dermatoglyphics. Classification, Genetics and Pathology*. New York: Oxford University Press. Oxford Monographs on Medical Genetics, 1983.
- "Los Angeles County Stops Fraud With Automated Fingerprint Matching System." [text on-line]; available from <http://www.hp.com>; Internet; accessed 21 February 1996.
- Lyford, George, and Udy Wood. "National Crime Information Center: Your Silent Partner." *FBI Law Enforcement Bulletin* 52 (March 1983): 10-15.
- Lyman, Michael D. *Criminal Investigation: The Art and the Science*. Englewood Cliffs, NJ: Regents/Prentice Hall, 1993.
- Macdonald, John M., and Thomas P. Haney. *Criminal Investigation*. Denver, CO: Apache Press, 1990.
- McAllister, Bill. "Byrd's Big Prize: Bringing Home the FBI. Appropriations Maneuver Sends Fingerprint Center to West Virginia." *Washington Post* (13 March 1991): A1, A7.
- , "House Review Sees Problems in FBI Project." *Washington Post* (14 March 1991): A16.
- McAuliffe, Kathleen. "The Germs of Schizophrenia: Abnormal Fingerprints May Point to Origins of Mental Disease." *Omni* 16 (March 1994): 13.

- McCormick, John. "Identix Wins Fed Contract." *Newsbytes, Washington News* (2 September 1993).
- . "INS Tests Hand Scanners to Speed Immigration Entry." *Newsbyte, Washington - News* (10 June 1993).
- McEwen, Thomas J. 1990. See U.S. Department of Justice. 1990.
- McKenna, Patrick. "Texas Instruments Intros Multimedia DSP." *Newsbyte, San Francisco News* (10 March 1994).
- McKinley, James C., "New Fingerprint Computers Speed Rape Suspect's Arrest." *New York Times* (2 March 1991): L27.
- McLaughlin, Ken. "Border Patrol Goes High-Tech." *San Jose Mercury News* (24 October 1994): 1A.
- Maize, Kennedy. "FBI Picks Teams for Fingerprint Work." *Newsbytes, Washington - News* (1 June 1994).
- . "IRS Tightens Rules on Electronic Filing." *Newsbytes, Washington - News* (21 September 1994).
- . "PRC Wins \$75 Million FBI Fingerprint Contract." *Newsbytes, Washington - News* (29 April 1994).
- Mallory, Jim. "Coloradans to Get Digitized Driver's Licenses." *Newsbytes, Denver - News* (21 January 1994).
- . "Consumer Apps for Electronic Fingerprint Reader." *Newsbytes, Denver - News* (29 July 1994).
- . "Electronic Fingerprint Technology." *Law and Order* (May 1992): 116-118.
- . Fingerprint Reader to Provide Positive Identification. *Newsbytes, Denver - News* (8 February 1994).
- Marchand, Donald Adelard. "Criminal Justice Information Systems and Information Policy: The Politics of the Social Costs of Technological Change." Ph.D. diss., University of California, Los Angeles, 1976.
- . *The Politics of Privacy, Computers, and Criminal Justice Records: Controlling the Social Costs of Technological Change*. Arlington, VA: Information Resources Press, 1980.
- Masland, Andrew T. "Networks Restructure Law Enforcement." *American & City County* (October 1987): 20.

- Meinhardt, Jane, and Karen Datko. "High-Tech Sleuthing at Finger Tips." *St. Petersburg Times* (4 July 1991): 1B.
- Miller, Frak, et al. *The Police Function*. 4th ed. Mineola, New York: The Foundation Press, Inc. 1986.
- "Milwaukee Installs Electronic System for Criminal Suspect Booking." *Government Imaging* (March-April 1994): 1, 28.
- Minahan, Tim. "FBI Begins Effort to Overhaul Its Fingerprint ID System." *Government Computer News* (30 August 1993): 16.
- Ministry of the Solicitor General. Royal Canadian Mounted Police. *International Illustrated Vocabulary of English-French Fingerprint Technology with a Short Index in Six Languages*. 3d ed. (revised and enlarged). Fingerprinting Centennial Edition 1891-1991, Lambert, Jean L. F., comp., Ottawa, Canada: Canada Communication Group-Publishing, 1991.
- Mintz, John. "Firms Picked to Work on Fingerprint System." *Washington Post* (7 June 1994): D3.
- Mitchell, Alison. "Fingerprints Being Studied in Bomb Case. F.B.I. Seeks Matches for up to 18 People." *New York Times* (20 May 1993): B1-B2.
- "Mobile Fingerprint and Mugshot Scanner." *Law and Order* (November 1989): 104-105.
- Morgan, J. Brian. *The Police Function and the Investigation of Crime*. Brookfield USA : Avebury, 1990
- Morris, Christopher, ed. *Academic Press Dictionary of Science and Technology*. New York: Academic Press, 1992.
- Morris, Jack. *Police Intelligence Files: An Introduction to the Use of Confidential Police Files*. Orangevale. CA: Palmer Enterprises, 1983.
- Moses, Jonathan B. "Fingerprint Advances Help Solve Crime." *Wall Street Journal* (23 September 1992): B20.
- "Mytec Technologies Makes Announcement." *Wire Services* 8 August 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 13 August 1995.
- Nagel, Stuart S. *Law, Decision-Making and Microcomputers: Cross-National Perspectives*. New York: Quorum Books, 1991.
- Narayanan, Ajit, and Mervyn Bennun, ed. *Law, Computer Science and Artificial Intelligence*. Norwood, NJ: Ablex Publishing Corporation, 1991.

- Nash, Donald J. *Individual Identification and the Law Enforcement Officer*. Springfield, IL: Charles C. Thomas Publisher, 1978.
- Nash, Jay Robert. *Encyclopedia of World Crime: Criminal Justice, Criminology, and Law Enforcement*. Wilmette, IL: CrimeBook, Inc. 1989.
- The National Cyclopaedia of American Biography*. New York: James T. White and Company. 1950.
- "The National Registry Inc. Announces Development of Low-Cost Digital Finger Image Reader." *PR Newswire* 8 February 1994 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 14 February 1994.
- "NCIC 2000," 31 March 1993 [forwarded message on-line]; available from Usenet newsgroup: austin.eff; Internet; accessed 1994.
- Neier, Aryeh. *Dossier: The Secret Files They Keep on You*. New York: Stein and Day, Publishers, 1974.
- Nemecek, David F. "NCIC 2000: Technology Adds a New Weapon to Law Enforcement's Arsenal." *The Police Chief* (April 1990): 30-33.
- Neudorfer, Charles D. "Fingerprint Automation: Progress in the FBI's Identification Division." *FBI Law Enforcement Bulletin* 55 (March 1986): 3-8.
- "New Age Fingerprints." *Washington Post* (17 April 1992): A22.
- "New Fingerprint Standard Approved." *Government Imaging* 3, no. 5 (July 1994): 14.
- "New ID System Could Keep Credit Card Out of Wrong Hands." *San Jose Mercury News* (21 October 1992): 1F.
- "New York Bomb Probe Finds More Suspects." *San Jose Mercury News* (22 May 1993): 4A.
- "New York State Police Alter Evidence Procedures." *New York Times* (9 March 1993): B1, B6.
- Nickell, Joe. "The Two 'Will Wests': A New Verdict." *Journal of Police Science and Administration* 8, no. 4 (1980): 406-413.
- Niederman, Fred, James C. Brancheau, and James C. Wetherbe. "Information Systems Management Issues for the 1990s." *MIS Quarterly* (December 1991): 475-502.
- "No Pictures, Please." *Newsweek* (18 November 1991): 4.

- Nordheimer, Jon. "Trooper's Fall Shakes Both Police and Public." *New York Times* (15 November 1992): 41, 56.
- "North American Morpho Systems Wins FBI Imaging Contract." *Government Imaging* (August 1995): 17
- "NY State Launches Photo ID System." *Government Imaging* (December 1995): 10
- O'Shea, G. *Security in Computer Operating Systems*. Manchester: NCC Blackwell, 1991.
- Overstreet, Harry and Bonaro. *The FBI in Our Open Society*. New York: W.W. Norton and Company, Inc., 1969.
- Parker, William W. "Authority to Fingerprint Arrestee Is Clear - But What to Do When He Resists?" *The Police Chief* 59, no. 11 (November 1992): 10, 12.
- Paul, Nora. "For the Record: Information on Individuals." *Database* 14 (April 1991): 15-23.
- Pavlis, John J. "Mug-Shot Imaging Systems." *FBI Law Enforcement Bulletin* (August 1992): 20-22.
- "(PBI) ADVISORY/New Technology Bows at Special Olympics; Pitney Bowes' High Tech Veritas System Provides Instant and Secure Access to Medical Records of Special Olympians." *Business Wire* 30 June 1995 [wire services on-line]; available from [http:// www.infoseek.com](http://www.infoseek.com); Internet; accessed 5 July 1995.
- Pennisi, Elizabeth. "Mathematics Aids Fingerprint Detection." *Science News* 142, no. 21 (21 November 1992): 350.
- Peterson, Joseph L., and Julie L. Moore. *The Status of AFIS Systems Worldwide: Issues of Organizations, Performance and Impact*. (revised September 1995) Presented at the International Symposium on Fingerprint Detection, and Identification, Ne' urim, Israel, June 1995.
- Pilant, Lois. "Exploiting Fingerprint Technology." *The Police Chief* (February 1994): 29-34.
- , "Image Processing Technology." *The Police Chief* (June 1994): 45-50.
- "Pitney Bowes Showcases Advanced Technology at 1995 Special Olympics World Games; Veritas™ System Speeds Access to Critical Medical Information on Athletes." *Business Wire* 29 June 1995 <http://www.infoseek.com>; Internet; accessed 5 July 1995.
- Plato, Chris. ed., et al. *Dermatoglyphics: Science in Transition*. New York: Wiley-Liss, 1991.

- "Polaroid and AT&T GIS Announce Strategic Partnership for Electronic ID Systems." *PR Newswire* 27 June 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 1 July 1995.
- "Police Build Bridges to Children." *San Jose Mercury News* (21 May 1993): 1B.
- "Police Computers Used for Improper Tasks." *New York Times* (1 November 1992): 38L.
- "Police Offer Fingerprinting on Law Day." *San Jose Mercury News* (29 April 1993): 4B.
- "Police Performance Enhanced with Affordable AFIS for Local Agencies." *Law and Order* (November 1992): 39-40.
- "PRC Snags FBI Fingerprint Contract." *Government Imaging* 3, no. 5 (July 1994): 20.
- "Print Match After 30 Years Puts Finger on Murder Suspect." *San Jose Mercury News* (12 September 1993).
- "Printrak Gives Law Enforcement Agencies On-Site Identification Capability for the War Against Crime." *Business Wire* 9 March 1994 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 14 March 1994.
- "Privacy." *Business Week* (28 March 1988): 61-68.
- "Privacy Versus Database Statistics." *Science News* 114, no. 20 (16 November 1991): 315.
- Quindlen, Terrey Hatcher. "FBI Shops for a Speedy Fingerprint System." *Government Computer News* (9 December 1991): 6.
- , "Harris Will Overhaul FBI's NCIC." *Government Computer News* (29 March 1993): 1.
- Ransom, Lou. "Fingerprinting Only Black Males in Town Sparks Tension, Fear." *Jet* 72 (21 September 1987): 12-18.
- Rathbun, Emmet A. "Interstate Identification Index." *FBI Law Enforcement Bulletin* 54, no. 1 (January 1985): 14-17.
- Ratledge, Edward, and Joan E. Jacoby. *Handbook on Artificial Intelligence and Expert Systems in Law Enforcement*. New York: Greenwood Press, 1989.
- Redlich, James W. "Supreme Court Rules on FOIA Access to Informant Information." *The Police Chief* (November 1993): 13.
- Rhodes, Henry T.F. *Alphonse Bertillon, Father of Scientific Detection*. New York: Abelard-Schuman, 1956.

- Rieder, Robert J. *Law Enforcement Information Systems*. Springfield, IL: Charles C. Thomas Publisher, 1972.
- Riggin, Stephen P. "U.S. Information Access Laws: Are They a Threat to Law Enforcement." *FBI Law Enforcement Bulletin* (July 1984): 13-19.
- "The RISS Program: A \$12 Million Bargain." *The Police Chief* (August 1987): 29-35.
- Rohrbough, Linda. "Intel Neural Network Chip Most Like Human Brain." *Newsbytes, Los Angeles - News* (22 February 1993).
- . "LA Fingerprint Sys Saves County \$5.4M in Welfare Fraud." *Newsbytes, Los Angeles - News* (21 July 1993).
- Rosen, Daniel M. "Police and Computers: The Revolution That Never Happened." *Police Magazine* (September 1982): 9-18.
- Rosenblatt, Robert A. "Securities Field to Check Prints." *Los Angeles Times* (13 July 1976): I1, I10.
- Rothfeder, Jeffrey. *Privacy. How Computerization Has Made Everyone's Private Life an Open Secret*. New York: Simon & Shuster, 1992.
- "Rules of the Road for Checking Remote-User IDs." *InfoWorld* 16, no. 44 (31 October 1994): 96.
- Sack, Kevin. "Cuomo Sanctions Fingerprint Scans. Effort Against Welfare Fraud May Face Legal Challenge." *New York Times* (9 July 1994): 1, 22.
- "SafeCard Launches Child Registration and Search Service; Comprehensive Initiative Addresses Major National Problem." *PR Newswire* 11 April 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 16 April 1995.
- Salottolo, A. Lawrence. *Modern Police Service Encyclopedia*. 2d ed. New York: Arco Publishing Company, 1973.
- "San Diego County Fights Welfare Fraud" *Government Imaging* (September 1995): 20.
- "San Diego County Teams with Unisys to Fight Welfare Fraud Using Automated Fingerprint Identification." *Business Wire* 5 April 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 11 April 1995.
- "Santa Clara County Law Enforcement Agencies Launch High-Tech Fingerprint Identification Program." *Government Imaging* 3, no.3 (May 1994): 19.

- "Saving Other Children. AB 2053, If Wilson Signs It, Would Screen Care Givers." *San Jose Mercury News* (29 September 1993): 6B.
- Scherpenzeel, Richard, ed. *Computerization of Criminal Justice Information Systems*. 2 vols. The Hague: Helsinki Institute for Crime Prevention and Control. 1992.
- Schmidt, George J. "Computer System Improves Law Enforcement Operation." *The Police Chief* (December 1994): 20-24.
- Schmitt, Christopher H. "Computerized Public Records Not Very Public." *San Jose Mercury News* (9 February 1992): 1A, 20A.
- Schmitt, Judith Blair. "Computerized ID Systems." *The Police Chief* (February 1992): 33-45.
- "A School's Digital Imaging Program." *The Police Chief* (December 1994): 28.
- "Schools, Cops and Corporations Cooperate to Store Kids' Photos on CDs." *School and College* (February 1994): 10.
- Schwartau, Winn. "New Keys to Network Security. Now You Can Secure Your LAN without Paying an Arm and a Leg." *InfoWorld* 17, no. 20 (15 May 1995): 51.
- Scott, William B. "Defense Skills Applied to Biometric ID." *Aviation Week and Space Technology* 144 (17 October 1994): 54.
- SEARCH Group, Inc. *The American Criminal History Record: Present Status and Future Requirements*. (September 1976) Technical Report no.14. Sacramento, CA, 1976.
- , *Standards for the Security and Privacy of Criminal History Record Information*. (July 1988), 3d ed. Technical Report no. 13. Sacramento, CA, 1988.
- "The Search for a Rapist." *Newsweek* (14 September 1987): 42.
- "Security by Fingerprints." *High Technology Business* 8 (July 1988): 11.
- Segen, JC, ed. *The Dictionary of Modern Medicine*. Park Ridge, NJ: The Parthenon Publishing Group, 1992.
- Sessions, William S. "Criminal Justice Information Services Gearing Up for the Future." *FBI Law Enforcement Bulletin* (February 1993): 1-3.
- , "The FBI and the Challenges of the 21st Century." *FBI Law Enforcement Bulletin* 58, no. 1 (January 1989) : 1-6.

- . "Using Microcomputers to Enhance Police Productivity." *The Police Chief* (March 1990): 10-13.
- "Should Private Security Have Access to Criminal Conviction Files?" *The Police Chief* 4, no.6 (June 1987): 35
- Silbert, Jeffrey Mark. "Criminal Justice Information Systems and the Criminal Justice 'System'." Ph.D. diss., New York University, 1972.
- Sjoquist, Karl-Erik, and Paul Astrom. *Pylos: Palmprints and Palmleaves*. Göteborg (Sweden): Paul Astrom Forlag. 1985.
- Slade, Margot. "Fingerprint System Extends Arm of the Law." *New York Times* (12 November 1993): B20.
- Slotnick, Daniel L., et al. *Computers and Applications: an Introduction to Data Processing*. Lexington, MA: D.C. Heath and Company, 1986.
- Smith, Larry. "Digital Imaging Pilot in Riverside County. Using Technology to Find Missing Kids." *California County* (July/August 1994): 26-27.
- Southerland, Daniel. "Your Prints Will Come - Any Second Now." *Washington Post* (10 April 1993): F1, F2.
- Sparrow, Malcolm K. "Information Systems: A Help or Hindrance in the Evolution of Policing?" *The Police Chief* 58, no.4 (April 1991): 26-44.
- . "Measuring AFIS Matcher Accuracy." *The Police Chief* (April 1994): 147-151.
- "St. Lucie County Orders Mug Shot and Fingerprint System." *Government Imaging* (July 1994): 19.
- Stapleton, Michael E. "Best Foot Forward: Infant Footprints for Personal Identification." *FBI Law Enforcement Bulletin* (November 1994): 14-17.
- Starrs, James E. "Fingerprint Scans: Why We Should Worry." *Washington Post* (25 April 1993): C6.
- "State Has Nation's 2nd Biggest Fingerprint File." *San Francisco Chronicle* (22 August 1994): 5.
- "State of Nebraska, Florida County Install Advanced Fingerprint Systems." *Government Imaging* (August 1995): 16
- Stead, Philip John. *Pioneers in Policing*. Montclair, NJ: Patterson Smith Publishing Corporation, 1977.

- Steinberg, Jacques. "Fingerprinting Welfare Applicants." *New York Times* (25 November 1992): B1, B6.
- . "Coming Soon: Fingerprints at Many Fingertips." *New York Times* (10 January 1993).
- Steppe, Cecil H. "What Wilson Wants." *San Jose Mercury News* (5 September 1993): 7P.
- "Suffolk Votes Fingerprinting for Welfare. State Officials Oppose Measure to Fight Fraud." *New York Times* (15 September 1993): B1, B6.
- Sullivan, John L. *Introduction to Police Science*. 3d ed. San Francisco: McGraw-Hill Book Company, 1977.
- "Supervisors Explore Gun-control Options." *San Jose Mercury News* (24 March 1993): 8B.
- Suro, Roberto. "INS to Continue Fingerprint Checks." *Washington Post* (19 April 1994): A8.
- . "U.S. Halts Immigrant Fingerprint Checks." *Washington Post* (14 April 1994): A11.
- "Suspect List Grows in N.Y. Bomb Probe." *San Jose Mercury News* (20 May 1993): 16A.
- Suthard, R.L. "Implementing an Automated Fingerprint System in Virginia." *The Police Chief* 56, no. 6 (June 1989): 24-27.
- Tackett, Michael. "FBI's Vaunted Fingerprint Files a 'National Resource on Decline.'" *Chicago Tribune* (23 May 1993): 3C
- Tafoya, William J. "Law Enforcement beyond the Year 2000." *The Futurist* (September-October 1986): 33-36.
- Thannisch, Larry T. "Development of an Automated Single Fingerprint System." Ph.D diss., San Jose State University. 1976.
- Thinès, Georges, and Agnès Lempereur. *Dictionnaire Général des Sciences Humaines*. Paris: Editions Universitaires, 1975.
- "Third State Trooper Arrested in Evidence-Tampering Case." *New York Times* (1 May 1993): 29.
- Thomas, Terry, and Bill Heberton. "Disclosure of Criminal Records: A Comparative Review." *Police Studies* 14, no. 2 (Summer 1991): 51-61.

- Thompson, Fletcher D. "Golden Anniversary of FBI Identification Division." *FBI Law Enforcement Bulletin* (July 1974): 3-9.
- "Thumb Tracks." *Forbes ASAP* (August 1994): 129.
- "To Finger Print All?" *Finger Print and Identification Magazine* (May 1972): 2.
- Torres, Donald A. *Handbook of Federal Police and Investigative Agencies*. Westport, CT: Greenwood Press, 1985.
- . *Handbook of State Police, Highway Patrols, and Investigative Agencies*. New York: Greenwood Press, 1987.
- "Toys 'R' Us and Playskool Team Up to Offer Free Child Identification Kits on June 3." *PR Newswire* 1 June 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 6 June 1995.
- "Toys 'R' Us, Playskool Offer Child ID Kits." *Reuters News Service* 1 June 1995 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 6 June 1995.
- Trautman, Neal E. *A Study of Law Enforcement. A Comprehensive Study of the World's Greatest, Yet Most Difficult, Profession*. Springfield, IL: Charles C. Thomas Publisher, 1990.
- "Truly Digital." *The Economist* (21 May 1994): 94.
- "TRW Awarded Design Concept Contract for FBI Automated Fingerprint Identification System." *Business Wire* 27 May 1994 [wire services on-line]; available from <http://www.infoseek.com>; Internet; accessed 4 June 1994.
- University of Illinois at Chicago. Department of Criminal Justice. Section of Forensic Sciences. Center for Research in Law and Justice. *Preliminary Results: AFIS Operating Agency Survey*, 8 February 1991.
- U.S. Comptroller General. *The Federal Bureau of Investigation (FBI) Operates Two Computerized Criminal History Information Systems*. (7 September 1979). Washington, D.C.: GPO, 1979. GGD-79-81.
- U.S. Congress. The Attorney General's Report to Congress on the Option Selected for Identifying Felons Who Attempt to Purchase Firearms: *Hearing Bfore the Subcommittee on Crime of the Committee on the Judiciary House of Representatives*. 101st Cong., 2d sess., 25 January 1990.
- U.S. Congress. House. Committee on Government Operations. *Regional Information Sharing Systems: Their Place in the National Criminal Justice System*. 15th report. 99st Cong., 1st sess., Washington, D.C.: GPO, 1985.

- U.S. Congress. Office of Technology Assessment. *Automated Record Checks of Firearm Purchasers: Issues and Options*. OTA-TCT-497. Washington, D.C.: GPO, 1991.
- U.S. Congress. Office of Technology Assessment. *The FBI Fingerprint Identification Automation Program: Issues and Options - Background Paper*. OTA-BP-TCT-84. Washington, DC: GPO, 1991.
- U.S. Congress. Office of Technology Assessment. *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*. OTA-CIT-296. Washington, D.C.: GPO, 1986.
- U.S. Congress. *Sale of Criminal History Records: Hearing before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary House of Representatives*. 102d Cong., 2d sess., 30 July 1992.
- U.S. Department of Commerce. Economics and Statistics Administration. Bureau of the Census. *Statistical Abstract of the United States*. 1995. 115th ed. Washington, D.C.: GPO, 1995.
- U.S. Department of Commerce. Economics and Statistics Administration. Bureau of the Census. *State and Metropolitan Area Data Book 1991*. Washington, D.C.: GPO, 1991.
- U.S. Department of Justice. Bureau of Justice Statistics. *Automated Fingerprint Identification Systems: Technology and Policy Issues*. (April 1987), by Thomas F. Wilson and Paul L. Woodard. Washington, D.C.: GPO, 1987. NCJ-104342.
- U.S. Department of Justice. Bureau of Justice Statistics. *Criminal Justice "Hot" Files*. (November 1986), Criminal Justice Information Policy. Washington, D.C.: GPO, 1986. NCJ-101850.
- U.S. Department of Justice. Bureau of Justice Statistics. *Data Quality of Criminal History Records*. (October 1985), Criminal Justice Information Policy. Washington, D.C.: GPO, 1985.
- U.S. Department of Justice. Bureau of Justice Statistics. *Open vs. Confidential Records: Proceedings of a BJS/SEARCH Conference (November 1988)*, Washington, D.C.: GPO, 1988. NCJ-113560.
- U.S. Department of Justice. Bureau of Justice Statistics. *Public Access to Criminal History Record Information (November 1988)*, by Robert R. Belair. Criminal Justice Information Policy. Washington, D.C.: GPO, 1988. NCJ-111458.
- U.S. Department of Justice. Federal Bureau of Investigation. *Automated Information Systems Plan: Tactical Plan (Fiscal Years 1993-1995)*. Criminal Justice Information Services Division. Washington, D.C.: GPO, 1993.

- U.S. Department of Justice. Federal Bureau of Investigation. *The Civil Identification Section. (15 August 1935)*, Washington, D.C.: n.p. 1935.
- U.S. Department of Justice. Federal Bureau of Investigation. *CJIS: Criminal Justice Information Services. A Newsletter for the Criminal Justice Community*. vol.1, no.1. Washington, D.C.: GPO, Fall 1994.
- U.S. Department of Justice. Federal Bureau of Investigation. *Crime in the United States 1994*. Washington D.C.: GPO, 1995.
- U.S. Department of Justice. Federal Bureau of Investigation. *Criminal Identification and the Functions of the Identification Division of the Federal Bureau of Investigation. (1 July 1937)*, by John Edgar Hoover. np. 1937.
- U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Statistics. *Criminal Justice Information Services*. vol. 1, no.1., Washington, D.C.: GPO, Fall 1994.
- U.S. Department of Justice. Federal Bureau of Investigation. *FBI: Facts and History*. Washington, D.C.: GPO, 1990.
- U.S. Department of Justice. Federal Bureau of Investigation. *The Identification Division of the FBI: A Brief Outline of the History, Services, and Operating Techniques of the World's Largest Repository of Fingerprints*. Washington, D.C.: GPO, 1991.
- U.S. Department of Justice. Federal Bureau of Investigation. *Integrated Automated Fingerprint Identification System (IAFIS)*. Criminal Justice Information Services Division. Washington, D.C.: GPO, 1994.
- U.S. Department of Justice. Federal Bureau of Investigation. *International Exchange of Fingerprints*. n.p. 1 April 1935.
- U.S. Department of Justice. Federal Bureau of Investigation. *Know your FBI*. Washington, D.C.: GPO, 1970.
- U.S. Department of Justice. Federal Bureau of Investigation. *Know your FBI*. Washington, D.C.: GPO, 1974.
- U.S. Department of Justice. Federal Bureau of Investigation. National Crime Information Center (NCIC). *National Crime Information Center. The Investigative Tool. A Guide to the Use and Benefits of NCIC. (June 1984)*, Washington, D.C.: GPO, 1984.
- U.S. Department of Justice. Federal Bureau of Investigation. *Problems and Practices in Fingerprinting the Dead*. Reprinted from the FBI Law Enforcement Bulletin, April, 1949. Revised November, 1980. Washington, D.C.: GPO, 1984.

- U.S. Department of Justice. Federal Bureau of Investigation. *The Science of Fingerprinting: Classification and Uses*. Washington, D.C.: GPO, 1977.
- U.S. Department of Justice. Federal Bureau of Investigation. *The Story of the Federal Bureau of Investigation*. np. 1945.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Assistance. *Edward Byrne Memorial State and Local Law Enforcement Assistance Program. FY 1992 Discretionary Program Plan (10 February 1992)*, Washington, D.C.: GPO, 1992. NCJ-134225.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Assistance. *Edward Byrne Memorial State and Local Law Enforcement Assistance Program. FY 1993 Discretionary Program Plan (2 November 1992)*, Washington, D.C.: GPO, 1992. NCJ-139200.
- U.S. Department of Statistics. Office of Justice Programs. Bureau of Justice Assistance. *Guidance for the Improvement of Criminal Justice Records (10 December 1992)*, Washington, D.C.: GPO, 1991.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Assessing Completeness and Accuracy of Criminal History Record Systems: Audit Guide (January 1992)*, Criminal Justice Information Policy. Washington, DC: GPO, 1992. NCJ-133651.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Criminal History Record Information: Compendium of State Privacy and Security Legislation, 1992: Current Status of the Law. Summary of State Statutes by Category, by State*. The National Consortium for Justice Information and Statistics. Washington, D.C.: GPO, 1992.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Highlights from 20 Years of Surveying Crime Victims: The National Crime Victimization Survey, 1973-92. (October 1993)*, Washington, D.C.: GPO, 1993. NCJ-144525.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Identifying Persons, Other Than Felons, Ineligible to Purchase Firearms: A Feasibility Study. (May 1990)*, Washington, D.C.: GPO, 1990. NCJ-123050.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *National Conference on Improving the Quality of Criminal History Records: Proceedings of a BJS/SEARCH Conference (January 1992)*, Washington, D.C.: GPO, 1992.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Rethinking the Criminal Justice System: Toward a New Paradigm (December 1992)*, by John J. Dilulio. Washington, D.C.: GPO, 1992. NCJ-139670.

- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Report of the National Task Force on Criminal History Record Disposition Reporting. Findings. Recommendations. (June 1992)*. Criminal Justice Information Policy. Washington, D.C.: GPO, 1992. NCJ-135836.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Statutes Requiring the Use of Criminal History Record Information. (June 1991)*, Criminal Justice Information Policy. Washington, DC: GPO., 1991.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Survey of Criminal History Information Systems (March 1991)*. Criminal Justice Information Policy. Washington, D.C.: GPO, 1991. NCJ-125620.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Survey of Criminal History Information Systems, 1993, with Supplementary Information on Presale Firearm Checks, 1994. (January 1995)*. Criminal Justice Information Policy. Washington, D.C.: GPO, 1995. NCJ-148951.
- U.S. Department of Justice. Office of Justice Programs. National Institute of Justice. *National Criminal Justice Thesaurus 1992: Descriptors for Indexing Law Enforcement and Criminal Justice Information*. Washington, D.C.: GPO, 1992.
- U.S. Department of Justice. Office of Justice Programs. National Institute of Justice. Office of Communication and Research Utilization. *Use of Microcomputers in Criminal Justice Agencies (May 1990)*, by Thomas J. McEwen. Washington, D.C.: GPO, 1990.
- U.S. Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. *Sourcebook of Criminal Justice Statistics. 1994*. Washington, D.C.: GPO, 1995.
- U.S. Department of Justice. Office of Justice Programs. National Institute of Justice. *Directory of Criminal Justice Information Sources (June 1992)*. 8th ed., N. Vanden Heuvel, comp. . NCJ- 125728. Washington, D.C.: GPO, 1992.
- U.S. Department of Justice. Office of Legal Policy. *Report to the Attorney General: The Admission of Criminal Histories at Trial (August 14, 1986)*, Truth in Criminal Justice Series. Report no. 4. Washington, D.C.: GPO, 1986.
- U.S. Department of Justice. *Report to the Attorney General on Systems for Identifying Felons Who Attempt to Purchase Firearms (October 1989)*, Task force on Felon Identification in Firearm Sales. n.p. 1989.
- U.S. General Accounting Office. *Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program*. Report to the Honorable Kenneth E. Bentsen, Jr., House of Representatives. 29 September 1995; GAO/OSI-95-20. [letter report on-line]; available from

<http://www.vitro.bloomington.in.us:8080/~BC/REPORTS/OSI-9520.html>; Internet; accessed 22 March 1996.

- U.S. General Accounting Office. *National Crime Information Center. Legislation Needed to Deter Misuse of Criminal Justice Information*. By Ekstrand, Laurie E. Testimony Before the Subcommittee on Information, Justice, Agriculture, and Transportation, Committee on Government Operations, and the Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, House of Representatives, 1993 GAO/T-GGD-93-41. [on-line]; available from <http://www.cpsr.org/cpsr/privacy/misc-privacy/gao-ncic-abuses-report-1993.txt>; Internet; accessed 22 March 1996.
- "U.S. to Fingerprint Visiting Iraqis, Kuwaitis." *San Jose Mercury News* (11 January 1991): 9A.
- Valentine, Paul W. "1 Fingerprint Worth 1,000 Words on Md. Computer." *Washington Post* (30 May 1991): C1, C4.
- , "Md. Police Enter New Age of Fingerprint Technology." *Washington Post* (5 January 1991): B1, B4.
- Vanden Heuvel, N., comp. 1992. See U.S. Department of Justice. 1992.
- Van Duyn, J. *Automated Crime Information Systems*. Blue Ridge Summit, PA.: TAB Professional and Reference Books, 1991.
- Vogel, Shawna. "The Case of the Unraveling DNA." *Discover* 11, no. 11 (January 1990): 46-47.
- von Hirsch, Andrew. "Desert and Previous Convictions in Sentencing." *Minnesota Law Review* 65, no. 4 : 591-634.
- Walket, Samuel. *A Critical History of Police Reform: The Emergence of Professionalism*. Lexington, MA: Lexington Books, 1977.
- Wasik, Martin. *Crime and the Computer*. Oxford: Clarendon Press, 1991.
- Webb, Margaret K. "Silver Spring Firm Working on High-Tech Identification." *Washington Post* (23 October 1989): 9.
- "Welfare Board Says No on Fingerprints." *San Francisco Chronicle* (23 July 1976): 2.
- Whisenand, Paul M., and Tug T. Tamaru. *Automated Police Information Systems*. New York: John Wiley and Sons, Inc., 1970.
- Whitehead, Don. *The FBI Story: A Report to the People*. New York: Random House, 1956.

- Who Was Who: A Companion to "Who's Who" Containing the Biographies of Those Who Died during the period 1916-1928.* London: A. & C. Limited, 1929.
- Wilder, Clinton. "Expanding Database Searches -- With Excalibur's TRS, Images Don't Have to Be Etched in Stone." *Information Week* 519 (27 February 1995): 142.
- Wilson, Thomas F., and Paul L. Woodard. 1987. See U.S. Department of Justice. Bureau of Justice Statistics. 1987.
- "WIN: AFIS Technology for Rural States." *FBI Law Enforcement Bulletin* (November 1990): 24-25.
- Witkin, Gordon, et al. "Gun Control's Limits." *U.S. News and World Report* (6 December 1993): 24-26
- Womack, Ralph. "Imaging Law Enforcement Records Management." *Government Imaging* (July 1994): 15,18.
- Wooden, Kenneth. *The Children of Jonestown.* San Francisco: McGraw-Hill Book Company, 1981.
- Zonderman, Jon. *Beyond the Crime Lab. The New Science of Investigation.* New York : Wiley Science Editions, 1990.