

Automation of American Criminal Justice

J. William Holland

Georgia Bureau of Investigation, USA

INTRODUCTION

Criminal Justice has been one of the public sectors in the forefront of the move toward automation and digital government. The effect of computerization on American criminal justice has been profound and it has transformed the criminal justice process in many fundamental ways. Starting with President Lyndon Johnson's government commission, *The Challenge of Crime in a Free Society: A Report by the President's Commission on Law Enforcement and the Administration of Justice*, public and private experts in criminal justice and technology laid out the information needs of the criminal justice system and the computer systems to meet those demands. At a time when computerization was minimal throughout the criminal justice system, these task force members developed the blueprint for today's multilayered automated criminal justice environment (Dallek, 1998, pp. 405-407, 409-411; *Challenge of crime in a free society*, 1967, pp. 268-271).

Among the major recommendations of the commission were the creation of a national directory of offenders' criminal records, what came to be known as Computerized Criminal History (CCH) and the development of similar directories at the state level. The commission also called for federal coordination of standards for criminal justice information and sharing. Finally, the report urged that a study of fingerprint classification techniques be undertaken with a view to automating much of the fingerprint search and identification effort and that work be intensified to create a national linkage of files on wanted persons and stolen vehicles under the name of the National Crime Information Center (NCIC) (*Challenge of crime in a free society*, 1967, pp. 255, 268-271; *Taskforce report: Science and technology*, 1967, p. 69).

BACKGROUND

One of the earliest responses to this report was the creation of the Law Enforcement Assistance Administration (LEAA) within the United States Department of Justice (DOJ). In 1969, LEAA funded Project SEARCH to create a nationwide computerized criminal history system. From this initial effort, SEARCH quickly evolved into an independent consortium of states with the mission of demonstrating a computerized system for the electronic

exchange of criminal history information. On the national level, the United States Attorney General assigned management responsibility for the interstate and national portion of this system to the Federal Bureau of Investigation. The states also formed the National Law Enforcement Telecommunications System (NLETS) electronically linking the states as well as the FBI and the Royal Canadian Mounted Police. By 1976, 26 states had used LEAA funding to create state level central repositories for computerized criminal history information (U.S. Department of Justice, 2001c, p. 26).

It became apparent during the last half of the 1970s, however, that greater decentralization of the nation's criminal history systems was urgently needed. To respond to these issues and concerns, the various states, FBI and SEARCH created the Interstate Identification Index or Triple I (III) concept in 1980 (U.S. Department of Justice, 2001c, pp. 26-27, 76-82, 88). Designed to replace a centralized national criminal history file, III was an index of criminal offenders that pointed to the state or states where detailed criminal history information could be found. There was widespread acceptance of III for criminal justice purposes: By 2001, 43 states participated. Legal restrictions and concerns, however, limited use of III for non-criminal justice use and weakened any effort to achieve a truly decentralized criminal history system. Consequently, the FBI continued to maintain criminal histories on individuals to meet interstate non-criminal justice needs (U.S. Department of Justice, 2001c, pp. 76-82).

Another factor that prevented the decentralization of criminal history information was the vast effort required in the time-consuming fingerprint identification process. A new system called the NCIC classification was implemented in the 1970s. It did little, however, to speed up the overall identification process (*Challenge of crime in a free society*, 1967, p. 255; *Taskforce report*, 1967, p. 16; Ms. Shirley Andrews, personal communication, September 9, 2002).

During the mid 1980s, new technological solutions for fingerprint identification emerged on the market. These systems, called automated fingerprint identification systems (AFIS), significantly reduced the manual tasks needed to search a fingerprint and made true searching of latent crime scene fingerprints possible. By the close of the 1980s, many states and a few local agencies had purchased these systems. Most were stand alone systems

dedicated to the fingerprint input, search, and presentation of potential candidates for human comparison. A few states, however, attempted to expand the capabilities of these systems and link them to other criminal history processes. When combined with the proven effectiveness of the AFIS latent search capability, the new technology contained the potential to transform criminal justice systems (U.S. Department of Justice, 2001b, pp. 43-44; U.S. Department of Justice, 2001c, pp. 61-63).

In the early 1990s, efforts were made through the National Institute of Standards and Technology (NIST) to devise a national fingerprint transmission standard; an effort spearheaded by the FBI. By 1993, a national standard for the electronic interchange of fingerprint information was approved by NIST and became the basis for the electronic linkage of local jurisdictions to state criminal history bureaus and the FBI. It formed the basis for the emerging national network of real-time identification and criminal history systems (See *Data format for the interchange of fingerprint, facial, and SMT information*, originally issued in 1993, amended in 1997 and further amended in 2000; U.S. Department of Justice, 2001c, pp. 61-63.)

CURRENT AND FUTURE TRENDS IN CRIMINAL JUSTICE AUTOMATION

Building on these past activities in fingerprint and criminal history automation, emphasis within state and national criminal justice circles has shifted to the need to share information, what is known as integrated criminal justice. With the explosion of the Internet and simultaneous cost limitations on criminal justice system development, both federal and state funding entities require that new criminal justice system developments build in the concept of information sharing, realignment of processing functions, and greater involvement of all criminal justice parties in individual systems development. The goal of this new focus is to eliminate duplicate entry of the same information and increase the overall completeness and accuracy of criminal justice information. (U.S. Department of Justice, 2001c, pp. 63-65; Harris, 2000, pp. 7, 14, 18-20, 41; U.S. Department of Justice, 2001b, pp. 47-48, 50; *Planning the integration of justice information systems*, 2002, pp. 2-3.)

Integrated justice efforts, however, have also resurrected older worries about privacy of such information and merged them with new concerns about greater linkage of criminal justice and non-criminal justice information on individuals. Questions about release of integrated information are linked to serious questions about the accuracy of the information released. These fears are intensified as private companies demand access to criminal history

information, gathered at public expense, to market to customers for profit. In many jurisdictions, the old line between public and private responsibilities and authority has faded as private companies have assumed many of the traditional criminal justice information systems functions. In addition, the heightened threat of terrorist attacks has led to efforts to gather large amounts of information on individuals into databases to search for terrorist patterns. These efforts have collided with fears about loss of privacy and misuse of such information by the government. Initiatives such as the Total Information Awareness effort and the MATRIX project to correlate private and public data on suspicious individuals have ground to a halt in the face of protest from citizens fearful of the loss of civil liberties. (Ideas that mattered in 2003:9. No future for terror market, 2003; MATRIX Updates, 2003; *Planning the integration of justice information systems*, 2002, p.5; Stanford, 2003; U.S. Department of Justice, 2001a, pp. 8, 12; U.S. Department of Justice, 2001b, pp. 2-3, 27-28, 50).

CONCLUSION

In 1967, a national commission developed *The Challenge of Crime in a Free Society*, the roadmap for today's highly automated but incomplete criminal justice system. This report served the nation well but it is time to move beyond its confining vistas, time to recognize that dramatic developments in computer technology and digital government demand new answers to old questions and the formulation of entirely new questions. The events of September 11, 2001 have raised anew questions about lack of information on potential threats to society and posed new questions on how we as a nation can weave together governmental and private computerized information to detect dangerous individuals intent on mass murder without compromising constitutional safeguards and individual liberties. It is time to convene a new national task force charged with the duty to assess the challenge of crime and terror in a free digital society. Only then can criminal justice automation and digital government move forward in a planned and comprehensive way.

REFERENCE LIST

(*References marked with an asterisk indicate reports included in the Commission report.)

Challenge of crime in a free society: A report by the President's Commission on Law Enforcement and Administration of Justice. (1967). Washington, DC: US Government Printing Office.

1 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/automation-american-criminal-justice/14236

Related Content

A Systematic Mapping Study on Requirements Engineering in Software Ecosystems

Aparna Vegendla, Anh Nguyen Duc, Shang Gao and Guttorm Sindre (2018). *Journal of Information Technology Research* (pp. 49-69).

www.irma-international.org/article/a-systematic-mapping-study-on-requirements-engineering-in-software-ecosystems/196206

Informed Governance: The Objective Definition Model

Carlos Páscoa, Benjamin Fernandes and José Tribolet (2016). *Handbook of Research on Information Architecture and Management in Modern Organizations* (pp. 363-381).

www.irma-international.org/chapter/informed-governance/135776

Empirical Evaluation of an Integrated Supply Chain Model for Small and Medium Sized Firms

Toru Sakaguchi, Stefan G. Nicovich and C. Clay Dibrell (2006). *Advanced Topics in Information Resources Management, Volume 5* (pp. 211-231).

www.irma-international.org/chapter/empirical-evaluation-integrated-supply-chain/4649

Electronic Commerce Travel: A Case Study in Information Technology Use, Market Flexibility, Adaptability, and Diversification

Eric Pedersen and David Paper (2007). *Journal of Cases on Information Technology* (pp. 73-89).

www.irma-international.org/article/electronic-commerce-travel/3195

Line Segment-Based Clustering Approach With Self-Organizing Maps

G. Chamundeswari, G. P. S. Varma and C. Satyanarayana (2021). *Journal of Information Technology Research* (pp. 33-44).

www.irma-international.org/article/line-segment-based-clustering-approach-with-self-organizing-maps/289855