# Privacy Policies and Warrant Systems

*By Owen Greenspan*
*Director, Law and Policy Program, SEARCH*

On the national level, many, but certainly not all, warrants are reported to the Wanted Person File of the FBI administered National Crime Information Center (NCIC).

## Persons Covered by the NCIC Wanted Person File

- Individuals for whom Federal warrants are outstanding

- Individuals who have committed or have been identified with an offense which is classified as a felony or serious misdemeanor under the existing statutes of the jurisdiction originating the entry and for whom a felony or misdemeanor warrant has been issued with respect to the offense which was the basis of the entry.

- Probation and Parole violators who have committed an offense which is classified as a felony or serious misdemeanor.

- A "temporary felony want" may be entered when law enforcement must take prompt action to establish a "want" entry to apprehend a person who has committed (or the officer has reasonable grounds to believe has committed) a felony and who may flee the jurisdiction and circumstances preclude the immediate procurement of a felony warrant.

- Juveniles who have been adjudicated delinquent and who have escaped or absconded from custody, even though no arrest warrants were issued.

- Juveniles who have been charged with the commission of a delinquent act that would be a crime if committed by an adult, and who have fled from the state where the act was committed.

- Individuals who have committed or have been identified with an offense committed in a foreign country, which would be a felony if committed in the United States, and for whom a warrant of arrest is outstanding and for which act an extradition treaty exists between the United States and that country.

- Individuals who have committed or have been identified with an offense committed in Canada and for whom a Canada-Wide Warrant has been issued which meets the requirements of the Canada-United States Extradition Treaty.

## Privacy Requirements for NCIC

Federal law recognizes the ever growing amount of information stored in government systems and the speed with which this information can be accessed, shared and transferred between data systems. The Privacy Act of 1974 controls the Federal government's use of personal information. It places restrictions on the collection, use, maintenance and release of information about individuals. The E-Government Act of 2002 mandates an assessment of the privacy impact of any substantially revised or new information technology system because of the potential privacy impacts from maintenance of electronic databases. The Privacy Impact Assessment is focused on how personally identifiable information is collected, stored, protected, shared and managed. Personally identifiable information is information from which an individual can be uniquely identified, such as name, address, date of birth and social security numbers, and any information linked or linkable to the individual. For example, the entry of a warrant into NCIC may include a driver's license number, or a military number, or any other miscellaneous number that serves to uniquely identify the subject of the warrant.

NCIC predates the enactment of the E-Government Act. Consequently, older NCIC databases that have not undergone substantial revision have not been the subject of a Privacy Impact Assessment. Further, under the authority of the Privacy Act, the Attorney General has exempted NCIC from certain provisions of the Act, including its access and contest procedures. Alternatively, the FBI has promulgated and published rules in the Federal Register, along with policies and practices affecting all contributors of information to NCIC and how that information is verified, validated, and may be accessed. Collectively, the rules, policies and practices surrounding NCIC use represent extensive privacy safeguards.

## State and Local Warrant Systems

Nearly all States and many local jurisdictions maintain automated warrant systems that enable entry, access, retrieval, updating, and cancellation of warrant information. Frequently the state system also serves as the conduit for entering information on NCIC. It is widely understood that state and local warrant systems have significantly more records than are reported to NCIC. This comes about largely as a product of three factors – 1) the volume of warrants for lesser offenses, such as those that are traffic related, 2) policy decisions that limit which warrants are entered on NCIC due to the overhead workload associated with record maintenance, verification and validation or, 3) the cost in dollars and lost personnel time associated with carrying out extraditions of wanted persons who have fled the jurisdiction.

## Privacy and State and Local Warrant Systems

Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. It is protected by federal and state constitutions and at least as importantly for the effectiveness of justice entities is that there is a high degree of expectancy by citizens when it comes to the privacy of government held information. The FBI has implemented far-

reaching safeguards affecting the privacy of NCIC wanted person information that are consistent with federal law.

States generally do not have laws equivalent to the Privacy Act or E-Government Act. States do however; often have laws that address the collection, retention, and dissemination of information. Some have characterized compliance with such laws as satisfying State level privacy interests. In the privacy and civil liberties realm, relying on such statutes, without developing written and implementing privacy policies and practices may place a justice entity's reputation and perceived effectiveness at risk.

To assist justice entities to implement privacy policies and protections for the information they collect, store, maintain, access, share and disseminate, the U.S. Department of Justice Global Justice Information Sharing Initiative has published a series of resource documents. In sum these documents provide a road map that guides justice entities through privacy policy development and implementation. These resources are available at www.it.ojp.gov/privacy and include:

- *Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development*

  This flyer is designed to engender awareness about the topic, make the case for privacy policy development, and underscore the importance of promoting privacy protections within justice agencies.

- *7 Steps to Privacy, Civil Rights and Civil Liberties Policy*

  Designed for both justice executives and agency personnel, this document educates readers on the seven basic steps involved in the preparation of a policy as recommended in the Department of Justice's *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities.*

- *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities*

  This document provides a framework with which to examine the privacy implications of information systems and information sharing collaborations.

- *Privacy, Civil Rights and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (Privacy Guide)

  This guide is a practical, hands-on tool for practitioners charged with drafting the privacy policy, providing guidance for articulating privacy obligations in the manner that protects the justice agency, the individual and the public.

- *Privacy, Civil Rights and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (Policy Development Template)

Each section of the template represents a fundamental component of a comprehensive policy that includes baseline provisions on information collection, information quality, collation and analysis, merging, access and disclosure, redress, security, retention and destruction, accountability and enforcement, and training.

- *Policy Review Checklist*

  This checklist is a companion piece to the Policy Development Template.

- *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework*

  This resource was developed for technical practitioners to provide guidelines for supporting the electronic expression of a privacy policy and how to convert a privacy policy so that it is understandable to computers and software.

This document was created through a collaboration of the National Center for State Courts and SEARCH, and was supported by Grant No. 2010-DG-BX-K164, awarded by the Bureau of Justice Assistance, Office of Justice Programs, United States Department of Justice. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office of Crime. Points of view or opinions expressed in this document do not represent the official position of the United States Department of Justice.