United States Participation in Interpol Computerized Search File Project

Neither state nor federal law would prohibit participation by the United States National Central Bureau of Interpol (USNCB) in a proposed computerized information exchange system, provided the USNCB complies with all disclosure, accounting, and publication requirements imposed by applicable federal statutes, such as 22 U.S.C. § 263a, the Privacy Act, and other federal restrictions on the exchange of criminal history information. As a matter of comity, the USNCB may comply with relevant state laws and regulations that restrict the disclosure and dissemination of personally identifiable information; however, under the Supremacy Clause, as a federal law enforcement agency it is not bound to do so.

The requirements of the Privacy Act may affect the structure and functioning of any computerized information exchange system in which the USNCB participates, particularly insofar as it would require the USNCB to verify the accuracy of data in its records prior to disclosure.

Applicable international guidelines and agreements relating to information exchange and privacy protection are broader in scope than the Privacy Act, and may restrict federal law enforcement agencies' ability to participate fully in the proposed system. Moreover, there are a number of possible international conflicts of law issues raised by the United States' participation in Interpol generally, and in any automated information exchange system it may implement.

December 9, 1981

MEMORANDUM OPINION FOR THE ASSISTANT ATTORNEY GENERAL FOR ADMINISTRATION

This responds to your request for this Office's advice on legal issues implicated by the proposed Interpol Computerized Search File Project, Fisher Informatise de Recherches (F.I.R.). This project, if approved by the Interpol General Assembly, will result in computerization of information now maintained by the Interpol General Secretariat and the exchange of information among member national central bureaus (NCBs) and the General Secretariat. While our discussion focuses on the F.I.R. project, our analysis may, as you recognize in your request, have implications for other recent initiatives dealing with the computerized exchange of personally identifiable information. One such initiative would be the recommendation of the Attorney General's Task Force on Violent Crime for establishment of an Interstate Identification Index as an alternative to a national centralized computerized criminal history file. We will, as appropriate, point out that overlap and the possible effects of our analysis on the Interstate Identification Index proposal.

We understand that the primary purpose of the F.I.R. project is to facilitate more rapid exchange of information through Interpol; such exchanges are presently accomplished largely on a manual basis. Implementation of the F.I.R. project would not alter the obligations and responsibilities of member NCBs with respect to the exchange of information, except insofar as will be necessary for technical operation of the system. Therefore, we do not believe that the computerization of the General Secretariat's files and the exchange of information among members of Interpol raise any unique legal issues. The more difficult questions will undoubtedly be those of policy and technical feasibility. You have also asked us to address more generally, however, the legal issues raised with respect to the collection and exchange of information among the member NCBs and the General Secretariat, so that you may evaluate how they affect the usefulness, desirability, and design of the F.I.R. project. We focus in this memorandum on the following: (1) restrictions imposed by state or federal law on the information that the United States National Central Bureau (USNCB) may contribute to the F.I.R. system; (2) the USNCB's responsibility to verify data it discloses through the system; and (3) the effect on federal law enforcement agencies of the voluntary privacy protection guidelines recently adopted by the Organization for Economic Cooperation and Development and of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data adopted by the Council of Europe. We will also discuss briefly conflict of laws problems raised by the F.I.R. project.

I. Background

Currently, NCBs exchange criminal justice and certain humanitarian information directly with the General Secretariat, which maintains a centralized file in St. Cloud, France, and directly with other NCBs. Under the F.I.R. project, the centralized records now maintained by the General Secretariat in manual form, which consist primarily of information contributed by member NCBs, would be put in a computerized data base accessible by member NCBs through remote terminals. This would be similar in design to the Computerized Criminal History File (CCH) now maintained as part of the Federal Bureau of Investigation's (FBI's) National Crime Information Center (NCIC). Channels would also be created between member NCBs allowing direct communication of requests and information without intermediate processing at the Interpol General Secretariat. It is our understanding that the FBI's NCIC system does not permit direct communication between state and local governments, but that such communication may be accomplished independently through the National Law Enforcement Telecommunications System (NLETS).

An alternative system design would be a central index maintained by the General Secretariat which would include only names or other identifying characteristics and corresponding index entries indicating which NCB maintains relevant information. A requesting NCB could not obtain information directly from the General Secretariat under such a system, but would be referred to the NCB that has information responsive to the request. The FBI's proposed Interstate Identification Index, which has been undergoing a trial in Florida, is based on the index concept.

We understand that the F.I.R. project has as yet only been proposed in principle, and that it will be submitted to the Interpol General Assembly early in 1982 for approval. Assuming the project is approved, the details of its design and operation will be addressed by the General Assembly only after the project has been approved in concept.[1]

II. Restrictions on Exchanges of Information

You have asked us to address specifically whether state or federal laws impose binding restrictions on the types of information the USNCB can contribute to the F.I.R. system. The USNCB now exchanges a wide variety of information with other NCBs and the Interpol General Secretariat, including: humanitarian records (missing persons, amnesia victims, victim locate requests, and identification of decedents); criminal subject records (stolen property, wanted persons, criminal history records); criminal investigative records (persons involved in or property associated with a criminal act); and criminal intelligence records (information indicating that a specific individual may commit a specific criminal act). Upon occasion, other types of personal assistance data may be communicated through Interpol to facilitate humanitarian efforts.[2] As we discuss below, we do not believe that state or federal law would prohibit the USNCB from continuing to exchange those categories of information through Interpol, provided the USNCB complies with all disclosure, accounting, and publication requirements imposed by the applicable federal statutes.

A. Restrictions Imposed by State Laws

A significant portion of information communicated by the USNCB through Interpol comes from cooperating state and local law enforce-

[1] Rules governing the processing of police information within Interpol, including treatment of data in an automated data processing system, have recently been discussed by the General Assembly. In our memorandum of October 17, 1981, we commented on the acceptability of those rules under United States law. We understand that because many countries did not have an adequate opportunity to review those rules before the General Assembly meeting, a committee has been established to consider the draft further, and that the rules, as modified, will be resubmitted to the General Assembly next year.

[2] For example, information relating to adoptions of Peruvian babies is communicated between Peruvian authorities and the adopting parents only through Interpol channels.

ment agencies, either directly through the NLETS system or indirectly through other federal law enforcement systems such as the Treasury Enforcement Communications Systems (TECS).[3] Most, if not all, states have laws restricting secondary dissemination of particular types of information, ranging from omnibus privacy legislation modeled on the federal Privacy Act, to specific limitations on disclosure of tax, welfare, criminal history, or other personal information.[4] The first question you have posed is whether the USNCB must or should comply with state laws that restrict the disclosure of personal history information, either (1) on the principle that the records submitted by a state remain the property of the state and therefore subject to state statutory restrictions; or (2) on a principle of voluntary compliance based on federal/state comity.

Many federal law enforcement agencies, including the FBI and the USNCB, recognize that the primary responsibility lies with state and local law enforcement agencies for determining what information can or should be disclosed to federal agencies. Neither the FBI nor the USNCB requires state and local agencies to disclose any information, or particular types of information. Disclosure is on a voluntary, cooperative basis. In some instances, if the state or local agency undertakes to exchange information, it becomes subject to federal restrictions on maintenance and disclosure of that information, but those restrictions do not affect the state's authority to decide, in the first instance, whether it will transmit particular types of information to the federal agency and whether such transmittal would comply with state law.[5] Both the FBI and the USNCB routinely honor requests by state and local law enforcement agencies for return, deletion, or modification of

---

[3] The USNCB has direct access to TECS, which includes data bases of a number of Treasury and other federal agencies, including the U.S. Customs Service, the Bureau of Alcohol, Tobacco and Firearms, the Internal Revenue Service, and, to a limited extent, the United States Coast Guard and the Department of State Through TECS, the USNCB also has access to the FBI's criminal record information files.

[4] Although we have not undertaken an exhaustive survey of state laws that regulate the disclosure of personal information, several state statutes we have reviewed apply only to disclosure of information by state agencies and officials, and therefore would not restrict disclosure by federal agencies or officials. For example, the Minnesota statute referred to in your request, which prohibits disclosure to "the private international organization known as Interpol," applies only to state agencies and political subdivisions. Minn. Stat. Ann. § 15.1643 (West Supp. 1980) *See also Ark.* Stat. Ann. §§ 16-801 to 810 (1979) (omnibus privacy act applicable to "an agency of the State Government or any local government or other political subdivision of the State"); Conn. Gen Stat Ann §§ 4-190 to 197 (West Supp. 1980) (restrictions on transfer of "personal data" by any "state board, commission, department, or officer"); *but see* Me. Rev. Stat. Ann. tit. 16, §§ 611-22 (West Supp. 1979-80) (limiting use of criminal justice information by "criminal justice agencies," including "federal, state . . . or local government agenc[ies]").

[5] For example, the regulations governing disclosure of criminal justice information by state agencies that receive Law Enforcement Assistance Administration funding under the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 42 U.S.C. §§ 3701-3797 (Supp. IV 1980), provide that, "Subsection (b) [limiting dissemination of criminal justice information by states] does not mandate dissemination of criminal history record information to any agency or individual. States and local governments will determine the purposes for which dissemination of criminal history record information is authorized by state law, executive order, local ordinance, court rule, decision or order." 28 C.F.R. § 20.21(c)(3), interpreting 42 U.S.C. § 3789g(b).

records previously forwarded to the federal agency. Thus, the FBI and USNCB recognize that states have a legitimate interest in and considerable control over what criminal justice information will be exchanged.

We believe that this recognition of the states' interest in criminal justice information communicated to federal agencies is only a matter of comity between state and federal law enforcement agencies. While federal agencies may choose to honor states' requests or statutory restrictions in the exchange of information, they are not bound by state laws that restrict secondary dissemination of criminal justice information. Under the Supremacy Clause of the Constitution, Art. VI, cl. 2, it is settled that the states cannot subject instrumentalities of the federal government to state regulation or control, in the absence of a clear congressional mandate to make federal authority subject to state regulation.[6] In particular, courts have held that state statutes restricting disclosure of certain types of information must give way where they are inconsistent with an Act of Congress or the Constitution, as, for example, where a federal grand jury subpoenas records otherwise protected by state statute.[7] Where the agency is not subject to state statutes or regulations restricting the disclosure of information, *a fortiori* its officers and employees are not subject to prosecution for violation of those regulations, if they are acting in furtherance of their responsibilities under federal law.[8]

Here, the relevant statutes that affect the ability of federal agencies to collect and disseminate data contain no "clear congressional mandate" that the federal agencies and their employees are subject to the restrictions contained in the various state statutes on use of criminal justice information except as a matter of comity. *See, e.g.,* 28 U.S.C. § 534 (authorizing the Attorney General to "acquire, collect, classify and preserve identification, criminal identification, crime and other records" and to "exchange these records with and for the official use of authorized officials of the Federal Government, the States, cities and penal and other institutions"); Omnibus Crime Control and Safe Streets Act of 1968, *supra*; 22 U.S.C. § 263a (authorizing the Attorney General to "accept and maintain membership . . . in Interpol").

You suggest in your request that language in *Tarlton* v. *Saxbe,* 507 F.2d 1116 (D.C. Cir. 1974) and Department of Justice regulations

---

[6] *See Mayo* v. *United States,* 319 U.S. 441, 447–48 (1943); *Kern-Limerick, Inc.* v. *Scurlock,* 347 U.S. 110, 122 (1954).

[7] *In re Grand Jury Subpoena, May 1978, at Baltimore,* 596 F.2d 630, 632 (4th Cir. 1979); *In re Special April 1977 Grand Jury,* 581 F.2d 589, 592 (7th Cir.) *cert. denied sub. nom. Scott* v. *United States* 439, U.S. 1046 (1978); *see In re Grand Jury Subpoena for N.Y. State Income Tax Records,* 468 F. Supp. 575, 577 (N.D N Y 1979); *see also United States* v. *Thorne,* 467 F. Supp. 938, 940 (D. Conn. 1979).

[8] *See In re Neagle,* 135 U.S. 1, 62 (1890); *Ohio* v. *Thomas,* 173 U.S. 276, 282 (1899), *Massachusetts* v. *Hills,* 437 F. Supp 351, 353 (D. Mass. 1977) (Secretary of HUD not subject to criminal prosecution for alleged violations of Massachusetts Sanitary Code in buildings owned by department); Memorandum for the Attorney General from Mary C. Lawton, Deputy Assistant Attorney General, Office of Legal Counsel (Nov. 30, 1976); *see generally United States* v. *Georgia Public Service Comm'n,* 371 U.S. 285, 292–93 (1963).

governing the disclosure of criminal history information under the Omnibus Crime Control and Safe Streets Act, *supra,* might embody a concept of "data ownership" whereby information contributed by a state to a federal agency would remain the property of, and therefore under the control of, the contributing state. We do not believe that such a concept is inherent in either the *Tarlton* decision or the pertinent regulations. In *Tarlton,* an action for expungement of FBI arrest records, the Court of Appeals for the District of Columbia Circuit suggested that 28 U.S.C. § 534, *supra,* may require the FBI to make "reasonable efforts" to maintain "constitutionally accurate criminal files." It bolstered that suggestion by reference to § 524(b) of the Omnibus Crime Control and Safe Streets Act, which requires state officials subject to the Act to make efforts to assure the accuracy and completeness of criminal history record information submitted to the FBI. The court noted in a footnote that:

> Congress surely cannot be presumed to undercut its action in [28 U.S.C.] § 534 by intending that the FBI be authorized to receive and disseminate without reasonable precautions the sort of incomplete, unchallengable information from state or local officials which those officials themselves are forbidden to disseminate.

507 F.2d at 1125 n.28. The court's reference to "the sort of . . . information from state or local officials which the officials themselves are forbidden to disseminate," involves only the obligations imposed on state officials under the Omnibus Act, and not those obligations imposed under state laws. This language therefore does not suggest that the FBI (or any other federal agency) is bound by state laws restricting the disclosure of criminal history information. Likewise, 28 C.F.R. § 20.21(c), quoted at n.5 *supra,* recognizes only that a state is not required to disclose information if disclosure would contravene its own law, regulations, or orders. That subsection does not suggest that the FBI is bound by such state laws.

Moreover, the concept of "data ownership" would imply that the receiving agency does not have control over data that it did not develop itself, and therefore that the receiving agency is not bound by federal laws or regulations governing use and disclosure of that information, such as the Privacy Act or the Freedom of Information Act (FOIA). There is no suggestion, however, in either the Privacy Act or FOIA that records collected by a federal agency are exempt from the requirements of those statutes if they are contributed by a state agency.[9]

[9]The Privacy Act applies broadly to any "system of records" maintained, collected, used, or disseminated by a federal agency. "Record" is defined in terms of the nature of the information (*i.e.,* information about an individual) and not the source of the information. 5 U.S.C. § 552a(a)(4). The definition of "system of records" is intended to exclude only groupings of records over which the

Continued

Finally, because federal agencies collect information from thousands of sources, including an estimated 20,000 state and local law enforcement agencies, it would clearly be impracticable to require the federal agencies to abide by the varying and inconsistent restrictions imposed by individual state laws. Where state regulation will frustrate the purpose and operation of a duly authorized federal program, the state statute must give way. *See Public Utilities Commission of California* v. *United States*, 355 U.S. 534, 540–44 (1958); *Mayo* v. *United States*, 319 U.S. at 445; *City of Los Angeles* v. *United States*, 355 F. Supp. 461, 465 (C.D. Calif. 1972).

Thus, we conclude that federal agencies such as the USNCB or the FBI may, as a matter of comity, comply with state restrictions on the use of data or state requests with respect to disclosure of data, at least so long as those restrictions are not themselves inconsistent with federal law, but are not obligated to abide by the laws of the various states in the handling of data submitted by the states. In addition, federal agencies are not required to comply with restrictions on disclosure of data imposed by the domestic laws of foreign countries, but may choose to honor those restrictions as a matter of international comity.[10]

B. Restrictions Imposed by Federal Law

While the USNCB need not comply with limitations imposed by state law except as a matter of comity, there are federal statutes and

---

agency has no "control"—*i.e.*, if it does not have access to the records; the ability to include, exclude, or modify information included in the grouping; or the responsibility to ensure the physical safety and integrity of the records—and records which, although in the physical possession of agency employees and used by them in performing official functions, are not "agency" records, such as uncirculated personal notes, papers, and records retained or discarded at the author's discretion and over which the agency exercises no control or dominion. *See* Office of Management and Budget Privacy Act Guidelines. 40 Fed. Reg. 28,949, 28,952, (July 9, 1975) (OMB Guidelines). The FOIA applies generally to "records" of an agency, except as specifically exempted by the statute. 5 U S.C. § 552(a)(3)(b). With the exception of the exemption in FOIA for "trade secrets and commercial or financial information obtained from a person and privileged or confidential," we are unaware of any statutory or regulatory provision or administrative or judicial interpretations suggesting that the Privacy Act and FOIA do not apply to records maintained by agencies on the sole ground that the records were obtained from a source outside the agency.

[10] For example, the federal agency could agree, by contract or otherwise, to restrict dissemination of state-supplied data and to honor states' requests for modification or return of information, so long as that agreement is not inconsistent with the agency's obligations under federal statutes As we discuss *infra*, however, such agreement would not in any sense exempt information contributed by the states from the Privacy Act, FOIA, or other federal disclosure statutes, once that information has been incorporated in the records of the federal agency. An index system, either at the federal or international level, would clearly have advantages in enabling the responsible central authority to honor restrictions requested by the states or foreign governments, because the central authority would not retain or disclose the information itself, but would only refer the requesting entity to the state or country that has relevant information. It would be the responsibility of that state or government to determine if disclosure is consisent with its laws, regulations, and policies. Even with a centralized data base, however, it may be possible to accommodate differing state or national disclosure requirements by allowing the source of the information unilaterally to restrict or qualify subsequent uses of information disclosed to the authority. The Interpol draft rules, for example (*see* n.1 *supra*), contemplate that an NCB may classify information as intended only for the use of the General Secretariat (Art. 6, ¶ 3) or only for the use of the country to which the information is communicated (Art. 12, ¶ 3). As a technical matter, codes or safeguards would have to be built into the F.I.R. project to accommodate such limitations.

regulations that restrict the types of data that can be collected and disseminated by the USNCB and the circumstances under which information can be disclosed outside the agency. In particular, we consider here: (1) 22 U.S.C. § 263a (Supp. IV 1980), the legislation authorizing United States participation in Interpol; (2) the Privacy Act; and (3) other federal restrictions on the exchange of criminal history information.

1. 22 U.S.C. § 263a

The statutory authority for participation by the United States in Interpol is 22 U.S.C. § 263a, which authorizes the Attorney General "to accept and maintain, on behalf of the United States, membership in the International Criminal Police Organization, and to designate any departments and agencies which may participate in the United States representation with that organization." Participation by the United States in Interpol is accomplished through the USNCB, which is part of the Department of Justice.[11] No statutory or regulatory authority expressly authorizes the USNCB to exchange criminal justice or humanitarian information through Interpol.[12] Such authority can be inferred, however, from the broad mandate in § 263a authorizing participation in the organization, and congressional approval of payment of dues to Interpol. *See, e.g., Fleming* v. *Mohawk Co.*, 331 U.S. 111, 116 (1947).[13]

We believe that the USNCB has broad authority to coordinate and communicate criminal investigative requests and humanitarian requests with the United States law enforcement agencies, the Interpol Secretariat, and other NCBs, consistent with the purposes of Interpol. The Interpol constitution describes the purposes of Interpol as follows:

---

[11] The Attorney General has approved a departmental reorganization that will make the USNCB a separate office within the Department of Justice. *See* memorandum from William French Smith, Attorney General, to Rudolph W. Giuliani, Associate Attorney General (Oct. 14, 1981).

[12] As part of the departmental reorganization (*see* n.10 *supra*), the Attorney General has also proposed an amendment to the Department of Justice's organizational regulations, which will specify the functions to be handled by the USNCB. Those functions include the authority to "transmit information of a criminal justice, humanitarian, or other law enforcement related nature between National Central Bureaus of INTERPOL member countries, and law enforcement agencies within the United States and abroad; and respond to requests by law enforcement agencies and other legitimate requests by appropriate organizations, institutions and individuals, when in agreement with the INTERPOL Constitution."

[13] Prior to 1978, § 263a included a ceiling on the amount of dues the United States could contribute to Interpol. Between 1957 and 1978, Congress raised that ceiling several times. *See, e.g.*, Pub. L. No. 85-768, 72 Stat. 921; Pub. L. No. 90-159, 81 Stat. 517; Pub. L. No. 92-380, § 1, 86 Stat. 531; Pub. L. No. 93-468, § 1, 88 Stat. 1422. In reports accompanying bills to increase the dues ceiling, Congress described in some detail the information-gathering functions of Interpol, and acknowledged that the United States' participation in Interpol is of substantial value for efforts to combat crime on an international scale. *See, e.g.*, S. Rep. No. 2403, 85th Cong., 2d Sess., *reprinted in* 1958 U.S. Code Cong. & Ad. News 3957; S. Rep. No. 1199, 93rd Cong., 2d Sess., *reprinted in* 1974 U.S. Code Cong. & Ad. News 5906. In 1978, Congress amended § 263a to provide that dues and expenses for the membership of the United States in Interpol "shall be paid out of sums authorized and appropriated for the Department of Justice." Pub. L No. 95-624, § 21(a), 92 Stat. 3466.

a) To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the "Universal Declaration of Human Rights."
b) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes.

Art. I. This specification of purpose is quite broad, and can be read to encompass the types of criminal justice and humanitarian information now collected and exchanged by the USNCB.[14]

2. Privacy Act, 5 U.S.C. § 552a

The USNCB must comply with the requirements of the Privacy Act with respect to any personal information maintained on United States citizens or permanent residents.[15] The Privacy Act limits the collection and dissemination of "personally identifiable" information by federal agencies generally to "such information . . . as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. § 552a(e)(1). The Act specifically prohibits the maintenance of any records "describing how any individual exercises rights guaranteed by the First Amendment." 5 U.S.C. § 552(e)(7). Criminal history information and certain law enforcement records, however, may be exempted from the requirements of subsections (e)(1) and (e)(7). 5 U.S.C. § 552a(j)(2). Pursuant to that authority, law enforcement records maintained by the USNCB in its Criminal Investigative Records System have been exempted from those requirements. The exemption from subsection (e)(1) means only, however, that the USNCB need not

[14] The authority of Interpol to investigate crimes is generally limited to "ordinary law crimes." Article III of the Interpol constitution expressly forbids the organization "to undertake any intervention or activities of a political, military, religious or racial character." We understand that because of this express limitation in the Interpol constitution, the USNCB will not provide through Interpol information related to incidents of a "political, military, religious or racial" character In addition, the draft rules on processing of police information recently considered by the Interpol General Assembly (*see* n.1 *supra*) would restrict the disclosure of information by the General Secretariat and the NCBs, although the rules do not restrict the prerogative of individual NCBs to determine what types of information can or should be disclosed under their own laws and policies. Under those rules, "police information" may be disclosed only for the following purposes:

> . . . to prevent ordinary law crimes, to bring the persons responsible to justice, to find the victims of such crimes, to find missing persons and to identify dead bodies . . . Items of police information other than names of persons may be processed for research and publication purposes. Any police information that has been published may also be processed for general reference purposes.

Art. 3, ¶¶ 3, 4. Items of police information may be further disseminated by the receiving NCB only to "official institutions concerned with the enforcement of the criminal law in its country." Art. 12, ¶(4).

[15] The Privacy Act does not apply to information maintained on foreign nationals unless they have permanent resident status in the United States Thus, information that the USNCB maintains on foreign nationals and nonresident aliens is not subject to the disclosure, accounting, and access requirements of the Act.

screen all information received from state, local, or foreign sources to determine if the information is relevant and necessary to the USNCB's statutory purpose. As we discuss below, the USNCB is required to make reasonable efforts prior to dissemination of any information subject to the Privacy Act to assure that the records disseminated are "relevant" to the USNCB's purposes. *See* 5 U.S.C. § 552a(e)(6). Moreover, independent of the requirements of the Privacy Act, the USNCB is without statutory authority to collect or disseminate information that is unrelated to the purposes of Interpol. *See* discussion in previous section.

Other than the limitations imposed by subsections (e)(1) and (e)(7), which may be of limited practical significance because of the exemption of law enforcement records, the Privacy Act does not limit the *types* of personal information that may be maintained and disseminated by a federal agency. The Privacy Act does, however, limit the *circumstances* under which such information may be disclosed. No personal information subject to the Act may be disclosed without the consent of the individual concerned unless one of eleven statutory exceptions is met. 5 U.S.C. § 552a(b). For law enforcement purposes, the most significant exception allowed is for a "routine use" of the agency, *i.e.*, a use which is "compatible with the purpose for which [the record] is collected." 5 U.S.C. § 552a(a)(5), (b)(3).

The legislative history of the Privacy Act does not provide much guidance as to the outer limits of the "routine use" exception. Congress chose not to define or prescribe a list of permissible "routine uses." Instead it provided a check on the scope of the exception by requiring publication of the nature of all "routine uses" in the Federal Register. Rep. Moorhead noted in House debate on the bill that:

> It would be an impossible legislative task to attempt to set forth all of the appropriate uses of Federal records about an identifiable individual. It is not the purpose of the bill to restrict such ordinary uses of the information. Rather than attempting to specify each proper use of such records, the bill gives each Federal agency the authority to set forth the "routine" purposes for which the records are to be used under the guidance contained in the committee's reports.
>
> In this sense "routine use" does not encompass merely the common and ordinary uses to which records are put, but also includes all of the proper and necessary uses even if any such use occurs infrequently . . . .
>
> Mr. Chairman, the bill obviously is not intended to prohibit . . . necessary exchanges of information, provided its rulemaking procedures are followed. It is in-

> tended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes. . . .

See 120 Cong. Rec. 36,967 (1974) (remarks of Rep. Moorhead); *see also* OMB Guidelines, 40 Fed. Reg. at 28,952. We are unaware of any judicial decisions that define the outer limits of the "routine use" exception. In the absence of definitive legislative history or court rulings to the contrary, we believe that the "routine use" exception affords considerable latitude to a federal agency to disclose information in furtherance of the purposes of that agency.

The USNCB, as well as other federal law enforcement agencies, have interpreted the "routine use" exception to authorize disclosure of criminal history, investigative, and intelligence records for a wide variety of law enforcement and humanitarian purposes. *See* 45 Fed. Reg. 75,902–03 (Nov. 17, 1980) (disclosure of routine uses of Interpol Criminal Investigative Records System). The USNCB has made the disclosures required by the Privacy Act. *See* 45 Fed. Reg. 16,473 (March 12, 1981); 45 Fed. Reg. 75,903 (Nov. 17, 1980). We have reviewed the routine uses listed by the USNCB, and believe they are consistent with the scope of the Privacy Act "routine use" exemption. If the F.I.R. project is implemented, however, the USNCB should consider at that point whether additional disclosures are necessary to describe the relationship between the F.I.R. system and the USNCB's system of records, and the exchange of information that will be made through the F.I.R. system.

The requirements of the Privacy Act may also affect how the F.I.R. system should be structured. For example, under subsections (c)(1) and (2), 5 U.S.C. § 552a(c)(1) and (2), the USNCB is required to keep an accurate accounting of the date, nature, and purpose of each disclosure of information subject to the Act, and the name and address of the person or agency to whom the disclosure is made. If disclosures are made directly through the F.I.R. system, the system must provide a mechanism for the USNCB to keep the required accounting. In addition, the USNCB must be able to ensure the "security and confidentiality" of records in its system by "appropriate administrative, technical and physical safeguards." 5 U.S.C. 552a § (e)(10). The system should allow the USNCB to screen incoming requests from other NCBs or from the General Secretariat and to verify that the disclosure of requested information would be consistent with the "routine uses" authorized for that information and with the Interpol constitution.[16] As we discuss below, the USNCB must also be able to screen outgoing information.

[16] The USNCB currently screens all requests from other NCBs for criminal history information to determine that: (1) a crime has been committed in the country requesting the information, and the crime would be considered a violation of U.S. law; (2) there is a link between the crime and the individual about whom the information is requested; and (3) the type of crime is not one encompassed by Article III of the Interpol constitution.

C. *Criminal History Record Exchange Restrictions*

When the USNCB obtains information from the FBI's Computerized Criminal History File or Identification Division systems, it is restricted in the use of that information by regulations promulgated under the Omnibus Crime Control and Safe Streets Act of 1968, *supra. See* 28 C.F.R. Part 20, Subpart C.[17] Subsection 20.33 provides that data from those systems will be made available by the FBI to, *inter alia,* "criminal justice agencies for criminal justice purposes" and to "federal agencies authorized to receive it pursuant to Federal statute or Executive Order." 28 C.F.R. § 20.33(a)(1) and (2). That exchange, however, is "subject to cancellation if dissemination [of the information] is made outside the receiving departments or related agencies." *Id.* § 20.33(b). We believe that disclosure of information from the FBI's NCIC or Identification Division files to Interpol and other NCBs is authorized by this provision, on the ground that the disclosure is to a "related agency." We note in that regard that the purpose of the FBI's exchange of information with the USNCB is to facilitate similar exchanges with constituents of Interpol, and that the FBI would be authorized under these regulations to disclose such information directly to "criminal justice agencies" in foreign countries, such as NCBs or the Interpol General Secretariat. Under § 20.33(b), however, if the USNCB discloses information obtained from the FBI's CCH or Identification Division files to foreign agencies not affiliated with Interpol or to private businesses, financial organizations, or individuals, its privilege of access to those files would be subject to cancellation.

III. The USNCB's Obligation to Verify Records

A separate question arising under the Privacy Act is the extent to which the USNCB must verify data disclosed to other NCBs, the Interpol General Secretariat, and state and local law enforcement agencies in the United States. Under the Privacy Act, prior to dissemination of any record about a United States citizen or permanent resident alien to anyone other than another federal agency, the USNCB is required to make "reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes." 5 U.S.C. § 552a(e)(6).[18]

---

[17] This subpart applies to "federal, state and local criminal justice agencies to the extent that they utilize the services of Department of Justice criminal history record information systems." 28 C.F.R. § 20.30. "Department of Justice criminal history record information system" is defined to include only the Identification Division and Computerized Criminal History File Systems operated by the FBI. 28 C.F.R. § 20.3(j).

[18] The Privacy Act authorizes exemption of law enforcement files such as the USNCB's Criminal Investigative System from most of the requirements of § 552a(e) relating to the quality of records collected and maintained by the agency. *See* 5 U.S.C. § 552a(j)(2) No exemption is authorized, however, from the requirements imposed by § 552a(e)(6). *Id.*

This provision does not require the USNCB to guarantee the accuracy, completeness, timeliness, and relevance of records disclosed, but only to make efforts that are reasonable given the administrative resources of the agency, the risk that erroneous information will be disseminated, and the possible consequences to an individual if erroneous information is disclosed. *See* OMB Guidelines, 40 Fed. Reg. at 28,953; *Smiertka* v. *United States Dep't of Treasury,* 447 F. Supp. 221, 225–26 & n.35 (D.D.C. 1978). Courts have noted in varying contexts that reasonable efforts may include, at a minimum, modification or deletion of information if the source of that information informs the agency that the information is incorrect or incomplete;[19] a request for additional factual information from the source if an individual submits evidence challenging the accurracy of information contained in the agency's files; [20] or modification or deletion of records if the agency's independent investigation and evaluation overwhelmingly shows that the information is incorrect or unfounded.[21] The OMB Guidelines suggest that, because the disclosing agency is often not in a position to evaluate "acceptable tolerances of error for the purposes of the recipient of the information," it may be appropriate for the agency "to advise recipients that the information disclosed was accurate as of a specific date . . . or of other known limits on its accuracy *e.g.,* its source." 40 Fed. Reg. 28,949, 28,965 (July 9, 1975).

Since implementation of the F.I.R. project may substantially increase the volume of requests and disclosures handled by the USNCB, it will be particularly important to establish workable procedures and guidelines to implement the USNCB's obligation under § 552a(e)(6). We cannot outline here what "reasonable efforts" would be for the USNCB, as that would require a detailed knowledge of how information is collected, stored, retrieved, and disclosed.[22] We note, however, that the F.I.R. system must provide an adequate opportunity for the USNCB to screen all data prior to their dissemination outside the federal government and to supplement information disclosed, as appropriate, with caveats about its source, timeliness, or reliability.

IV. International Initiatives

You have asked us specifically to address the potential impact on federal law enforcement systems of the OECD's Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

[19] *See Menard* v *Saxbe,* 498 F.2d 1017, 1027–28 (D.C Cir. 1974).

[20] *See id.; Tarlton* v. *Saxbe,* 507 F.2d 1116, 1129 (D.C. Cir. 1974).

[21] *See Murphy* v. *National Security Agency,* C.A. No. 79–1833 (D.D C. Sept. 29, 1981), memorandum op. at 9; *R.R.* v. *Dep't of Army,* 482 F. Supp. 770, 773 (D.D.C. 1980).

[22] This analysis would be more appropriate, for example, for the Interpol Policy Guidelines Working Group, which will be responsible for reviewing and updating policies applicable to the USNCB's day-to-day operations.

(OECD Guidelines) [23] and the Council of Europe's Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Council of Europe Convention),[24] and any international conflict of laws issues associated with United States participation in Interpol and the Interpol F.I.R. project. Both the OECD Guidelines and the Council of Europe Convention attempt to balance the need for protection of personal privacy arising out of increasing flows of personal information across national borders, and the political and economic necessity of maintaining transborder flows of data with minimal restrictions. The OECD adopted the approach of voluntary guidelines, based on certain "basic principles" of national application intended to provide minimum privacy protection,[25] and of international application, intended to encourage the free flow of data.[26] Member countries are encouraged to establish, through legislation, self-regulation, or voluntary efforts, legal, administrative, and other procedures or institutions for the protection of privacy, and to cooperate with other member countries to facilitate international exchanges of information. *See* Parts 4, 5. We understand that the United States participated in drafting the OECD Guidelines, and has undertaken to abide by the principles therein.

The Council of Europe Convention requires each Party [27] to "take the necessary measures in its domestic law to give effect to the basic principles for data protection" set out in the Convention. Chap. II, ¶ 1. Those principles resemble in content the principles outlined in the OECD Guidelines, with the addition of a specific provision that personal data that would reveal "racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life" or "personal data relating to criminal convictions" may not be processed automatically "unless domestic law provides appropriate safeguards." Art. 6. Parties are obligated to provide mutual assistance

[23] The OECD is an intergovernmental organization dedicated to problems of economic development, whose members include the 19 democratic countries of Europe, the United States, Japan, Australia, New Zealand, and Yugoslavia (special associate status).

[24] The Council of Europe is an intergovernmental organization of 21 European countries. Its members are pledged to cooperate at intergovernmental and interparliamentary levels to promote greater European unity. *See* Hondius, *Data Law in Europe*, 16 Stan. J. of Int'l L. 87, 91 (1980). The United States is not a member of the Council of Europe.

[25] These principles encompass limits to collection of personal data; accuracy, completeness, relevance, and timeliness of data; specification of uses of data and limitation to those uses; security safeguards; openness in the establishment of systems and method of access to data; individual participation and access; and accountability. Part 2.

[26] Member countries are to take into consideration the implications for other member countries of domestic processing and re-export of personal data; to take reasonable and appropriate steps to ensure that transborder flows of personal data are uninterrupted and secure; to refrain from restricting transborder flows of personal data except where necessary; and to avoid developing laws, policies, and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection. Part 3.

[27] No member of the Council of Europe has yet ratified the Convention. The Convention will not become effective until ratified by five members. Art. 22. Non-member states may be invited to accede to the Convention following its entry into force. Art 23.

to notify other parties of steps taken to implement the Convention, and to assist persons resident abroad to exercise rights conferred under the domestic laws that give effect to the principles set out in the Convention. Arts. 13, 14.

We note first that neither the OECD Guidelines nor the Council of Europe Convention imposes any binding obligations on the United States or on federal law enforcement agencies. The OECD Guidelines are voluntary. Parts 4 and 5 of the Guidelines discuss various methods for implementing the letter and spirit of the principles set forth through appropriate domestic legislation and policies and international cooperation, but do not impose any obligation upon parties other than mutual cooperation. The Council of Europe may, after the entry into force of the Convention, invite non-members to accede to the Convention. We are unaware whether the United States will be invited to accede, and whether the United States would accept that invitation. Since accession would obligate the United States to pass domestic legislation considerably broader in scope than that now in effect (*see infra*), it seems unlikely that the United States would accede to the Convention if invited, and we assume here that the United States will not accede to the Convention. Thus, the impact on federal law enforcement agencies will not stem from obligations imposed on the United States under either the OECD Guidelines or the Council of Europe Convention, but rather will most likely result from actions taken by other nations to implement the letter or spririt of those agreements.

In particular, both the OECD Guidelines and the Council of Europe Convention recognize the principle that a nation may restrict data flows to another nation if that nation does not afford the same protection to that data as is afforded by the originating state, or if the export of that data would circumvent the domestic privacy legislation of the originating country.[28] In that regard, the privacy protection contemplated by the OECD Guidelines and the Council of Europe Convention is broader than that afforded by the Privacy Act. The Guidelines and the Convention apply to all exchanges of information, private and public.[29] The Privacy Act, by contrast, leaves untouched information-gathering and disclosure by state and local governments and by private businesses or individuals.[30] Thus, even if the Privacy Act embodies most of the substantive requirements outlined in the OECD Guidelines and the Council of Europe Convention,[31] the coverage afforded by the

[28] *See, e.g.*, OECD Guidelines, Part 3, ¶ 17; Council of Europe Convention Arts. 3, 6, 12 (¶ 3(a)).

[29] The Council of Europe Convention, however, applies only to information transmitted through automatic data processing. Arts. 1, 2, 3.

[30] There are federal statutes that restrict the use and disclosure of information by state and local governments and private parties, but only in limited sectors. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681; Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (codified at scattered sections in 31 U.S.C.).

[31] The "basic principles" of data protection listed in Part 2 of the OECD Guidelines parallel in most respects the underlying principles of the Privacy Act. *See* n. 25 *supra*.

Privacy Act is narrower than that of those agreements. The practical result of this may be that nations adhering to one or both of those agreements may refuse to disclose information to federal law enforcement agencies within the United States, such as the USNCB, because the United States does not provide protection for personal data that is equivalent to that provided by the originating country.[32] Under the OECD Guidelines, United States agencies could similarly refuse to disclose data if the requesting country could not adequately protect the security or use of that information.

Of course, even without the express recognition of this principle contained in the OECD Guidelines and the Council of Europe Convention, individual NCBs are free to restrict data flows for any reason, including the lack of privacy legislation in the receiving country. The express recognition of that prerogative in the OECD Guidelines and the Council of Europe Convention has highlighted the problem of protecting transborder data flows while ensuring personal privacy, however, and we cannot predict what the practical impact will be on federal law enforcement. This is clearly an area in which mutual cooperation and voluntary compliance with privacy protection guidelines could alleviate future problems.

It would be premature for us at this point to comment other than generally on the possible international conflicts of law issues raised by U.S. participation in Interpol and in the F.I.R. system. We note first that Interpol, as an organization, occupies a somewhat anomalous position under our law, as it was not established by treaty or protocol, and is not generally accorded status as an international organization.[33] While our participation is authorized by statute, the Interpol constitution has never been expressly approved by Congress or the Executive Branch and does not have treaty status. Consequently, the Interpol constitution and resolutions and rules adopted by the Interpol General Assembly do not have the force of law in the United States and do not confer any rights on United States citizens or residents that are enforceable in our courts. *See* U.S. Const., Art. VI, cl. 2; *see generally, Mannington Mills, Inc.* v. *Congoleum Corp.*, 595 F.2d 1287, 1298 (3d Cir. 1979); *Bell* v. *Clark*, 427 F.2d 200 (4th Cir. 1971). Where there is a

[32] Federal, state, and local governments and private parties are not, of course, precluded from voluntarily supplementing the protections required by applicable domestic legislation, in an effort to avoid this potential problem.

[33] The Interpol constitution was adopted by the Interpol General Assembly in June, 1956. Ratification of the constitution does not require formal approval by member countries. All countries represented at Interpol are deemed to be Interpol members unless they subsequently declare through appropriate governmental authority that they cannot accept the constitution. The United States has never submitted any such nonacceptance declaration. The Interpol constitution has not been expressly approved by the Executive Branch or Congress. *See* Report of the Comptroller General of the United States, "United States Participation in INTERPOL, The International Criminal Police Organization" (Dec. 27, 1976) at 9, 25. Interpol is not listed as an "international organization" for purposes of immunity under the International Organizations Immunities Act, 22 U.S.C. § 288

conflict between the USNCB's obligations under the Interpol constitution or rules and its obligations under U.S. law, the latter will prevail.

Somewhat more difficult questions are presented under the domestic laws of the various countries that participate in Interpol. Particularly as the exchange of information among NCBs increases with implementation of the F.I.R. project, individuals of one country who are damaged by disclosures of information through Interpol may seek redress based on a variety of legal theories, such as defamation or invasion of privacy.[34] In the simplest situation, where an NCB in country A discloses information to an NCB in country B, and a person aggrieved by that disclosure sues in one of those countries, a conflict of law question would be presented as between the jurisdiction or substantive law of country A and country B which could probably be handled under existing principles of conflicts of law. *See Restatement of the Foreign Relations Law of the United States* (2d) § 40. Exchanges of information through the Interpol General Secretariat are more difficult because they would raise the possibility that the jurisdiction and law of yet another country (France) may be invoked. If the F.I.R. project is implemented, the conflicts problems could become yet more complicated, because information could be switched through a number of countries, either by design or for technical reasons, on its way between country A and country B.[35] The OECD Guidelines and Council of

[34] For example, in recent years at least two suits involving disclosures by the USNCB or by the Interpol General Secretariat have been filed in United States courts, both seeking recovery for alleged defamation by an official of the USNCB or by the General Secretariat in connection with requests forwarded through Interpol to detain or arrest an individual. *See Steinberg* v. *International Criminal Police Organization,* 672 F.2d 927 (D.C Cir. 1981); *Sami* v. *United States,* 617 F.2d 755 (D.C. Cir. 1979). In both decisions, the court discussed only jurisdictional questions arising under United States law, and did not address possible conflicts of law questions. In *Sami* v. *United States,* the court held that the Interpol General Secretariat was not "doing business" in the District of Columbia for purposes of exercise of the D.C. long-arm statute, D.C. Code §§ 13-334. The claim in that case arose out of communications made by an official of the USNCB to the German NCB through Interpol channels, requesting arrest of plaintiff, a citizen of Afghanistan, on the basis of an outstanding Florida warrant. By contrast, in *Steinberg* v. *International Criminal Police Organization,* the same court held that there was *in personam* jurisdiction over Interpol under the same statute, where the claim involved Interpol's transmission of a publication (a "Blue Notice" requesting arrest) into the District of Columbia. The court distinguished its result from that reached in *Sami* on the basis that the *Steinberg* case involved "an invocation of specific, not general, adjudicatory authority." Slip op. at 5. The court noted that it did not intend by its holding to foreclose any other defense, "jurisdictional or otherwise," that Interpol or its Secretary General might raise. *Id.* at 12, n.13.

[35] A recent article has hypothesized the following situation to illustrate the problem. The health records of a Swiss national are collected by his employer in Switzerland, and transmitted to corporate headquarters in Amsterdam where they are processed,. stored, and aggregated with health records of other nationals working in other countries. The aggregated data are then sent on via international facilities to a United States-owned data processing service in the United States. While they are being held in that facility, however, the main computer breaks down and an automatic switch sends the data through *international telecommunications facilities on to a secondary processing facility in Hong* Kong. The data are processed there and returned to the primary facility in the United States. A copy of the processed data is sent to storage at the primary site and the data are returned to Amsterdam. The employer then sends it along to the employer's insurance carrier, an Italian firm whose primary data processing facilities are stored in Spain The insurance carrier again processes the data, stores them in Madrid on magnetic tape, and issues the appropriate group health policy to the employer. *See* Fishman, *Introduction to Transborder Data Flows,* 16 Stan Int'l L.J. 1, 21 (1980). While this example is drawn from the private processing of data, it is not difficult to imagine equally convoluted trails for exchanges of criminal history information through F.I.R.

Europe Convention recognize that existing conflicts of laws principles may not be adequate to deal with exchanges of information through automated data processing in the future. The OECD's Expert Group, which drafted the guidelines, specifically rejected any detailed rules on conflicts of law questions, following extensive debate. *See* Explanatory Memorandum (Appendix), ¶22. The final Guidelines provide only that "Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data." OECD Guidelines Part 5, ¶22. The Council of Europe Convention does not address the possible conflicts of laws questions, other than to require Parties to render "mutual assistance" in implementation of the Convention, including any assistance necessary to facilitate the exercise of rights under a Party's domestic privacy legislation by "any person resident abroad." Art. 14.

It is thus clear that before the F.I.R. project is implemented, the members of Interpol will have to grapple with potential conflicts of laws problems. Since the resolution of those problems has implications beyond those arising out of Interpol's activities, it may not be possible for the members of Interpol to reach a definitive consensus. It may be possible, however, to avoid or mitigate some of the problems that may arise from technical operation of the system (*see* n.36 *supra*) in the way the system is structured. In the absence of concrete plans for the system, it is difficult for us to speculate on what the problems or possible solutions may be. We will, of course, be willing to work with you and other federal agencies to develop applicable principles and proposals, and to implement guidelines for operation of the F.I.R. system, if the project is approved.

LARRY L. SIMMS
Deputy Assistant Attorney General
Office of Legal Counsel