

## **United States Secret Service Use of the National Crime Information Center**

The United States Secret Service (USSS) has authority under 18 U.S.C. § 3056 to investigate and maintain files on an individual who it reasonably believes might pose a threat to the physical safety of those it is responsible for protecting, even though that individual is not the subject of an arrest warrant or under investigation for any prior criminal activity.

The USSS has authority to disclose information in its investigative files to the Federal Bureau of Investigation (FBI) and other law enforcement agencies through entry of this information into the National Crime Information Center (NCIC). The Attorney General is also independently authorized by 28 U.S.C. § 534 to disseminate information on criminal investigations, including information on USSS-monitored subjects, for law enforcement purposes.

An exchange of information among law enforcement agencies through the NCIC must satisfy the requirements of the Privacy Act. In order to avoid that statute's general prohibition on disclosure, the USSS and FBI must satisfy the procedural requirements of the "routine use" exemption contained in 5 U.S.C. § 552a(b)(3).

Disclosure of information from the NCIC on USSS-monitored subjects for non-law enforcement purposes, such as employment or licensing, is prohibited by the Privacy Act, and may raise serious constitutional problems under the Fifth and Fourteenth Amendments.

Both 28 U.S.C. § 534 and the Privacy Act require that reasonable efforts be made to assure that information contained in the NCIC is accurate and relevant to its use for law enforcement purposes.

June 9, 1982

### **MEMORANDUM FOR THE ASSISTANT DIRECTOR, TECHNICAL SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION**

This memorandum responds to your request for our opinion regarding several issues raised by the proposed entry of data from the United States Secret Service (USSS) into the National Crime Information Center (NCIC). Specifically, you have asked: (1) whether the USSS has the authority to monitor the activities of individuals who are not the subject of outstanding arrest warrants but who may threaten the physical safety of the public figures it protects; and (2) whether the USSS may enter information about such individuals into the NCIC, the Federal Bureau of Investigation's (FBI's) computerized criminal justice information system. For the reasons set forth in detail below, we conclude that the USSS has the authority to gather information and maintain files on such individuals and enter the proposed information about them into the NCIC. We caution, however,

that the NCIC should disseminate this information, as you have proposed, only to law enforcement agencies for law enforcement purposes, and not for non-law enforcement purposes, such as employment or licensing.

## I. Background

The USSS is authorized by 18 U.S.C. § 3056 to “protect” various public figures, including the President and Vice President (protectees).<sup>1</sup> In discharging this responsibility, the USSS gathers information and maintains files on certain individuals “whose actions or spoken words indicate that [they] may constitute a threat” to protectees. Opinion Request, p. 1. We understand that most of these persons are not the subject of an outstanding arrest warrant.<sup>2</sup> The USSS has proposed to enter into the NCIC the names and certain information about those persons “who are determined to be dangerous and about whom a decision is made to ensure that the individual is not permitted to inflict harm on protectees.”

---

<sup>1</sup> Under 18 U.S.C. § 3056, the Secret Service is authorized to:

protect the person of the President of the United States, the members of his immediate family, the President-elect, the Vice President or other officer next in the order of succession to the Office of President, and the Vice President-elect, and the members of their immediate families unless the members decline such protection, protect the person of a former President and his wife during his lifetime, the person of a widow of a former President until her death or remarriage, and minor children of a former President until they reach sixteen years of age, unless such protection is declined; protect the person of a visiting head of a foreign state or foreign government and, at the direction of the President, other distinguished foreign visitors to the United States and official representatives of the United States performing special missions abroad

In addition, the Act of June 6, 1968, Pub. L. No. 90-331, 82 Stat. 170, as amended, *reprinted in* 18 U.S.C. § 3056 note, authorizes the USSS to “furnish protection to persons who are determined from time to time by the Secretary of the Treasury, after consultation with the advisory committee, as being major presidential or vice presidential candidates who should receive such protection,” and, in certain circumstances, their spouses.

<sup>2</sup> Pursuant to the Privacy Act, 5 U.S.C. § 552a(e)(4) & (11), the USSS has announced that it maintains protective information files on the following categories of individuals:

(a) Individuals who have been or are currently the subject of a criminal investigation by the U.S. Secret Service or another law enforcement agency for the violation of certain criminal statutes relating to the protection of persons or the security of properties; (b) Individuals who are the subjects of investigative records and reports supplied to the Secret Service by Federal, state, and local law enforcement agencies, foreign and domestic, other governmental agencies; private institutions and individuals for evaluation by the Secret Service in connection with the performance by that agency of its authorized protective functions; (c) Individuals who are the subjects of non-criminal protective and background investigations by the Secret Service and other law enforcement agencies where the evaluation of such individuals, in accordance with criteria established by the Secret Service, indicates a need for such investigations; (d) Individuals who are granted ingress and egress to areas secured by the Secret Service, the Executive Protective Service, or to areas in close proximity to persons protected by the Secret Service, including but not limited to invitees, passholders, tradesmen, law enforcement, maintenance and service personnel; (e) Individuals who have attempted or solicited unauthorized entry into areas secured by the Secret Service; individuals who have sought an audience or contact with persons protected by the Secret Service or who have been involved in incidents or events which relate to the protective functions of the Secret Service; (f) Individuals who are witnesses, protectees, complainants, informants, suspects, defendants, fugitives, released prisoners, and correspondents who have been identified by the Secret Service or from information supplied by other law enforcement agencies, governmental units, private institutions, and members of the general public in connection with the performance by the Secret Service of its authorized protective functions

Opinion Request, p. 2. It estimates this group to number at any given time between 300 to 400 individuals (USSS-monitored subjects).<sup>3</sup>

The stated purpose of this dissemination is to monitor the location and activities of these individuals by using the network of state and federal agencies which obtain information from the NCIC. At present, the NCIC contains separate files on wanted persons, missing persons, stolen property, and criminal histories. It supplies information about a particular individual or property from these files to federal, state, and local criminal justice agencies that make an inquiry about that individual or property.<sup>4</sup> Under the proposal, the NCIC would establish a new file on the USSS-monitored subjects which would be accessible to government law enforcement agencies seeking to use the information for law enforcement purposes, in particular, criminal investigation and arrests. Whenever any participating law enforcement agency seeks information for these purposes from the NCIC about an individual who is in this file, the USSS would be informed about the request. This would permit the USSS to contact the inquiring agency, learn the reasons for the request, and thereby monitor the subject's current activities. If a law enforcement agency seeks information on such an individual for non-law enforcement purposes, such as employment or licensing, the NCIC would not disclose any information about the subject.<sup>5</sup>

While the FBI has not determined finally the specific information which would be included in the NCIC entry on each USSS-monitored subject, we understand that it would probably include identifying information about the subject, such as his height and weight; a notation that the USSS considers him to be a "threat" or

---

<sup>3</sup> In determining whether an individual will be considered dangerous to a protectee and included in the NCIC file, the USSS would follow these procedures

- (A) Through numerous and varied means, individuals may be brought to the attention of the USSS. An investigation is begun which usually includes a personal interview with the individual. Some criteria used in a determination are: the interview, the facts of the action bringing the subject to the attention of USSS, the potential or capability of the subject to carry out any threat, and a background investigation including criminal and mental checks/inquiries.
- (B) If, based upon this initial investigation, an individual is determined to be a potential threat by an investigatory agent, his evaluation and determination are reviewed for concurrence by field supervisors
- (C) The original investigation and evaluation, and the field evaluation are reviewed at USSS Headquarters by a Senior Agent/Intelligence Research Specialist
- (D) These evaluations are then reviewed and approved by an Intelligence Division supervisor
- (E) Once evaluated as dangerous, the individual is subject to a periodic review process.
- (F) The decision to enter such individual into the NCIC System will be under the Assistant Director for Protective Research, with the Special Agent in Charge, Intelligence Division, acting on his behalf

Opinion Request, p. 3.

<sup>4</sup> Access to the criminal history file is currently more limited than access to the other files. The non-criminal history files are generally available to state or federal "criminal justice agencies" for any authorized purpose. See 46 Fed. Reg. 60293, 60294 (1981) (description of system's operation) While criminal history files are accessible to criminal justice agencies for any criminal justice purpose, and to any federal agency authorized to receive it, state criminal justice agencies can only obtain the information for non-law enforcement purposes, such as licensing or employment, if access is specifically authorized by state law and approved by the Attorney General. *Id.* See 28 C.F.R. § 20.33 (1981)

<sup>5</sup> Our understanding that dissemination of this information from the NCIC would be limited to government law enforcement agencies using the information for law enforcement purposes is based on a discussion with B. Bryan Masterson, Editorial Staff, NCIC.

“potentially dangerous” to a protectee; and a request that any agency inquiring about the subject contact the USSS. In addition, in order to protect law enforcement officials who come into contact with a subject, the USSS would also include a brief description of the subject’s dangerous characteristics, for example, that he is “mentally unstable” or “armed and dangerous.” Finally, the entry would warn officials not to arrest the subject based on the NCIC entry.<sup>6</sup>

## II. Authority of the USSS to Investigate and Maintain Files on Individuals Who Are Not the Subject of an Outstanding Arrest Warrant

Under 18 U.S.C. § 3056, the USSS is authorized to “protect” the person of the President, Vice President, and other designated public figures,<sup>7</sup> and to “detect and arrest” any person who has made a threat against the President or his successor in violation of 18 U.S.C. § 871. Although neither the language of § 3056 nor its legislative history explains what specific activities are included within the protective responsibilities of the USSS, it is clear that the USSS’s duties necessarily require it to engage in a broad range of prophylactic investigations and preventive actions.<sup>8</sup> The USSS is not only charged with identifying and apprehending persons who have threatened the safety of the President or other protectees, but also with *preventing* any person from jeopardizing their physical safety. This charge necessarily presumes that the USSS has the authority to investigate individuals who might threaten the safety of protectees but who have not yet taken any concrete action toward realizing that goal.<sup>9</sup>

This authority was specifically recognized by the Fifth Circuit in *Moorefield v. United States Secret Service*, 611 F.2d 1021 (5th Cir.), *cert. denied*, 449 U.S. 909 (1980). In that case, the plaintiff, Moorefield, had sought disclosure under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, of a USSS protective file maintained on him. Even though he was not being investigated to detect any

---

<sup>6</sup> This description of the NCIC entry is based on an “example” of an “NCIC inquiry” and “a positive U.S. Secret Service response” which was furnished us by the staff of the NCIC.

<sup>7</sup> The public figures are listed in note 1, *supra*

<sup>8</sup> The Supreme Court has described the USSS’s responsibility for assuring the physical safety of the President as representing an “overwhelming” national interest *Watts v. United States*, 394 U.S. 705, 707 (1969) (*per curiam*)

<sup>9</sup> The implied authority of the executive branch generally to take appropriate action to prevent the commission of federal crimes was recognized over 90 years ago in *In Re Neagle*, 135 U.S. 1 (1890). There the Supreme Court noted.

It has in modern times become apparent that the physical health of the community is more efficiently promoted by hygienic and preventive means, than by the skill which is applied to the cure of disease after it has become fully developed. So also the law, which is intended to prevent crime, in its general spread among the community, by regulations, police organization, and otherwise, which are adapted for the protection of the lives and property of citizens, for the dispersion of mobs, for the arrest of thieves and assassins, for the watch which is kept over the community, as well as over this class of people, is more efficient than punishment of crimes after they have been committed. *Id.* at 59 More recently, the Office of Management and Budget has specifically observed that “[a]gencies can derive authority to collect information about individuals [either by direct constitutional or statutory authorization] or [b]y the Constitution, a statute, or Executive order authorizing or directing the agency to perform a function, the discharge of which requires the maintenance of a system of records” Office of Management and Budget Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28960 (1975) Section 3056, which directs the USSS to assure the physical safety of protectees, is a statute “directing the agency to perform a function, the discharge of which requires the maintenance of a system of records.”

prior criminal activity,<sup>10</sup> the court held that the file was maintained pursuant to the USSS's statutory authority and therefore constituted "investigatory records" prepared for "law enforcement purposes" within the meaning of FOIA, 5 U.S.C. § 552(b)(7)(A).<sup>11</sup> The materials in the file, it reasoned,

include[d] background and other matters specifically relevant to Moorefield, and were prepared to help the Service fulfill its duty under 18 U.S.C. § 3056 (1976) [of] ensuring the lives and safety of the President, members of his family, and certain other persons.

*Id.* at 1024 (footnote omitted). Gathering of this information, therefore, served the "prophylactic purpose of keeping Service protectees from harm." *Id.* at 1024 n.3. The court went on to conclude that the file was exempt from disclosure under FOIA because disclosure would have directly undermined an "enforcement proceeding," which the court defined to mean, in that case, the protection of the President:

In discharging its responsibility to protect the President, the Secret Service does not conduct its routine investigations with a view towards apprehending law-breakers and bringing them to justice. Thus, if the Service has succeeded in its prophylactic mission, it should never appear in an adjudicatory proceeding to prosecute the assailant of a President, or any of its other protectees. Its job is to *prevent* an attack from ever being made. . . . Notwithstanding that Service investigations are not directed toward trials or hearings, they are certainly directed toward an active and concrete effort to enforce the law—in fact, nothing could be more "active and concrete" than activities that are part of the security apparatus that surrounds the President of the United States.

*Id.* at 1025 (citations omitted and emphasis in original).<sup>12</sup>

Congress also recognized the broad scope of the USSS's investigatory authority and protective files when it passed the Privacy Act, 5 U.S.C. § 552a. Although the Privacy Act grants the subject of many agency records access to

---

<sup>10</sup> Moorefield had previously been convicted of making threats against the President. See 611 F.2d at 1022, 1024.  
<sup>11</sup> Section 552(b)(7)(A) prohibits disclosure of "investigatory records compiled for law enforcement purposes, . . . to the extent that the production of such records would . . . interfere with enforcement proceedings." See generally *Federal Bureau of Investigation v. Abramson*, 456 U.S. 615 (1982).

<sup>12</sup> Similarly, in *Scherer v. Brennan*, 379 F.2d 609, 611 (7th Cir.), cert. denied, 389 U.S. 1021 (1967), the Seventh Circuit held that Treasury Department agents were acting within the scope of their duty to protect the person of the President when they monitored the activities of an individual who they believed might pose a threat to the President, even though he was not the subject of an arrest warrant or under investigation for any prior criminal activity. The agents were thus held to be immune from suit for any damages to the subject that might have resulted from their surveillance. Cf. *Galella v. Onassis*, 487 F.2d 986, 993 (2d Cir. 1973) (USSS charged "with guarding against and preventing any activity by any individual which could create a risk to the safety and well being of" protectees).

them,<sup>13</sup> it authorizes an agency head to exempt from this requirement any files “maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056.” 5 U.S.C. § 552a(k)(3). Speaking against an amendment which would have deleted this exemption from the Act, Representative Moorhead recognized that “[t]he list of the protective service by the Secret Service has gotten too broad,” but added that the “list also contains the names of people who are a real threat” and “that an amendment which completely eliminates the secrecy of the legitimate protective right of the Secret Service just goes too far.” 120 Cong. Rec. 36966 (1974). Similarly, the House Committee Report on the Act noted that “[a]ccess to Secret Service intelligence files on certain individuals would vitiate a critical part of Secret Service work which was specifically recommended by the Warren Commission [the Commission to Investigate the Assassination of President Kennedy].” H.R. Rep. No. 1416, 93rd Cong., 2d Sess. 19 (1974). The Warren Commission had recommended that the USSS expand its activities beyond the investigation of “persons communicating actual threats to the President,” or persons expressing “some manifestation of animus against a Government official.” The President’s Commission on the Assassination of President Kennedy (Warren Commission Report) at 461–62 (1964). In its view, such a limitation was “unduly restrictive.” *Id.* at 462. “A basic element of Presidential protection,” it advised, “is the identification and elimination of possible sources of danger to the President before the danger becomes actual.” *Id.* at 429.<sup>14</sup> In passing the exemption for the USSS protective files, therefore, Congress apparently recognized that the USSS would be engaged in the prophylactic investigation and surveillance of a variety of individuals, including many who are not the subject of an arrest warrant or suspected of any prior criminal activity.<sup>15</sup>

Accordingly, we believe that the USSS has the authority to monitor the activities of individuals who are not the subject of an outstanding arrest warrant or being investigated for the commission of prior crimes, so long as the USSS

---

<sup>13</sup> The Act generally covers any “system of records” “maintained” by an agency on an individual “Maintain” is defined to include “maintain, collect, use or disseminate” 5 U.S.C. § 552a(a)(3). A “system of records” is defined as a “group of any records under the control of any agency from which information is retrieved by the name of the individual,” or by some other symbol 5 U.S.C. § 552a(a)(5). The USSS protective files are a “system of records” within the meaning of the Act. *See* 46 Fed. Reg. 16643 (1981).

<sup>14</sup> The Warren Commission apparently assumed that the USSS has the authority to undertake such investigation under § 3056. Although the Commission criticized the prior lack of preventive investigation, and strongly recommended that the USSS and FBI expand such activity in the future, it did not suggest that any new statutory authority was necessary for such investigation. The only recommendations made by the Commission with respect to the authority of the USSS under § 3056 were that Congress should make assaults or attempted assaults on the President or his successor a federal crime, and grant its agents the authority to make arrests without a warrant. Warren Commission Report at 454–56. Congress adopted these recommendations by amending § 3056 in Pub. L. No. 89–218, 79 Stat. 890 (1965), to give the USSS the authority to make arrests without a warrant, and by enacting 18 U.S.C. § 1751 to make an assault on the President (-elect), Vice President (-elect), or the President’s successor a federal crime.

<sup>15</sup> In adopting this provision, Congress also failed to rely on a more general exemption from the Privacy Act requirements for files “maintained” “for the purpose of a criminal investigation” by an agency or component thereof “which performs as its principal function any activity pertaining to the enforcement of criminal laws.” 5 U.S.C. § 552a(j)(2)(B). This may suggest that Congress believed investigations undertaken by the USSS might be somewhat broader than traditional “criminal investigations.” *Cf.* 120 Cong. Rec. 36966 (1974) (remarks of Rep. Erlenborn) (supporting USSS exemption even though it “falls under the same general category of law enforcement where we already have an exemption”).

reasonably believes that the individuals might pose a threat to the physical safety of protectees.<sup>16</sup>

### III. Authority of USSS to Enter Information About USSS-Monitored Subjects into the NCIC

Having determined that the USSS has the authority to collect information about, and maintain files on, individuals who are not the subject of an arrest warrant, we next consider whether it may disclose the proposed information about these individuals to the FBI, and whether the FBI may in turn disclose it to other agencies, by creating the proposed new file in the NCIC. These disclosures raise two issues: first, whether the USSS has the statutory authority to disseminate this information to the FBI, or the FBI, in turn, to other agencies; and second, even if they do, whether the Privacy Act prohibits such disseminations.

#### A. *Statutory Authority of the USSS and FBI to Disseminate Information on USSS-Monitored Subjects to Agencies with Access to the NCIC*

The USSS clearly has the authority to transmit information on individuals it believes may threaten a protectee to the FBI in order to facilitate protection of protectees. Such authority is implicit in its power under § 3056 and explicit in its authority under the Presidential Protection Assistance Act of 1976, Pub. L. No. 94-524, § 6, 90 Stat. 2475, as amended, *reprinted in* 18 U.S.C. § 3056 note, to seek the assistance of other federal agencies in its protective responsibilities. We also believe that the FBI has the authority to disseminate this information to law enforcement agencies in the circumstances you have proposed, although this conclusion requires a more detailed explanation.

Section 534, Title 28 (1976), authorizes the Department of Justice to collect and disseminate various types of "records." It states in pertinent part:

The Attorney General shall—

- (1) acquire, collect, classify, and preserve identification, criminal identification, crime, and other records; and
- (2) exchange these records with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions.

By authorizing the collection and dissemination of "identification, criminal identification, crime, and other records," the language of this provision appears

---

<sup>16</sup> We note that the Privacy Act generally requires that an agency "maintain no record describing how any individual exercises rights guaranteed by the First Amendment" 5 U.S.C. § 552a(e)(7). This restriction, however, would not limit surveillance of individuals or maintenance of files for the protection of protectees. The Act provides an exception to this prohibition for surveillance which is "pertinent to and within the scope of an authorized law enforcement activity." The Attorney General has previously determined that USSS and FBI protective investigations undertaken pursuant to § 3056 constitute a "law enforcement activity." See Memorandum from Edward H. Levi, Attorney General, to Clarence M. Kelley, Director, FBI, "Gathering and Reporting Data Regarding Civil Disturbances." p. 2 (Mar. 4, 1976). We see no reason to reconsider this conclusion.

to support the Attorney General's power to collect and disseminate a wide variety of criminal investigatory information, including the proposed entry on USSS-monitored subjects.<sup>17</sup>

Some question about this interpretation, however, is raised by the D.C. Circuit decision in *Menard v. Saxbe*, 498 F.2d 1017 (D.C. Cir. 1974), which interpreted the Attorney General's authority under § 534 very narrowly. In *Menard*, the plaintiff had brought suit to expunge an FBI record of his "detention" by California State Police.<sup>18</sup> In granting him relief, the court held that the FBI lacked statutory authority under § 534 to retain a record of a detention in the arrest file for dissemination to law enforcement agencies. It appeared to reason that the Department only had authority to disseminate "criminal records," *i.e.*, criminal matters of record, such as arrests or convictions, and not criminal investigatory information. Since a record of a "detention" was, in its view, a type of investigatory information, the FBI had no authority to maintain the record in a file for dissemination.

The court based its narrow reading of § 534 on the brief congressional debate attendant to its "original enactment." The Chairman of the House Judiciary Committee had described the practice of the Identification Bureau during this debate as follows:

There are two classes of information that [are] gathered. One is criminal records, and another is the information that is gathered about criminals that is not a matter of record. That they do not give out, but the criminal records they do give out. That information is gathered for the department itself and its agents, in order that they more effectually do their work.

72 Cong. Rec. 1989 (1930) (remarks of Rep. Graham). Thus, according to the court, Congress did not intend to authorize the dissemination of investigatory information, such as the plaintiff's detention record, which was not a "matter of record." 498 F.2d at 1028-29 n.42.

The *Menard* decision should undoubtedly be read narrowly. As a practical matter, the FBI disseminates criminal investigatory information in many cases to other federal and state agencies. *See, e.g.*, 46 Fed. Reg. 60311, 60321 (1981) (describing dissemination of criminal investigatory information in FBI Central Records System). The court in *Menard*, however, was concerned principally with the FBI's dissemination of inaccurate or misleading information from its files, such as a record of a "detention" in an arrest file, where that information would be used for employment decisions. In its opinion, the court specifically found that the retention of plaintiffs' file was "not consistent with the FBI's duty,

---

<sup>17</sup> The Attorney General has delegated his authority under § 534 to the Director of the FBI. *See* 28 C.F.R. § 0.85 (1981)

<sup>18</sup> After the plaintiff was arrested by California police, the police were unable to connect him with any felony or misdemeanor, and therefore they classified his custody as a detention pursuant to California law. Nevertheless, this incident was initially entered into the FBI criminal identification files as an arrest. After plaintiff brought suit, the FBI amended the entry in its arrest file to show that the plaintiff had been "detained" under California law. 498 F.2d at 1019-20



corollary to its function of keeping identification records, to take appropriate measures to assure that this function is discharged responsibly and that the records are reliably informative.” *Id.* at 1027–28. A subsequent District of Columbia decision emphasized this aspect of the decision. *See Tarlton v. Saxbe*, 507 F.2d 1116, 1121 & n.7 (D.C. Cir. 1974). Thus, the decision should probably be read as only prohibiting the NCIC from disseminating inaccurate records in this context, and not from disseminating accurate investigatory information to other law enforcement agencies.

Indeed, even if *Menard* were read to prohibit the dissemination of general criminal investigatory information, we believe that this limitation would not apply to the Attorney General’s dissemination of information to assist in the protection of the President and other protectees. There is no doubt, for example, that the USSS and the FBI may contact local law enforcement officials in the area where the President or another protectee is traveling in order to provide background information on USSS-monitored subjects. Such authority flows directly from the USSS’s ability to protect such figures pursuant to 18 U.S.C. § 3056 and to obtain assistance in this effort from other executive agencies. *See* Presidential Protection Assistance Act of 1976, § 6, *reprinted in* notes to 18 U.S.C. § 3056. For similar reasons, we believe that both the USSS and the FBI have implied authority to disseminate generally some limited background information in order to monitor the subject’s activities. This authority would not only permit the disclosure of identifying information about the subject, but also USSS evaluations. These descriptions would assist police in handling the subject and ultimately contribute indirectly to the USSS protection of protectees.

Even if *Menard* could not be distinguished, however, we believe that 28 U.S.C. § 534 clearly authorizes the Attorney General to disseminate criminal investigatory information. Our conclusion that other courts should not and will not adopt *Menard’s* analysis of § 534, at least with respect to the entry on USSS-monitored subjects, is based on three weaknesses in the *Menard* analysis.

First, the legislative history of § 534 does not support the court’s narrow interpretation. The court relied on the congressional debates during the enactment of a predecessor statute, 5 U.S.C. § 340 (1964), *repealed by* Pub. L. No. 89–554, § 8(a), 80 Stat. 632, 648 (1966), which had authorized dissemination of only “criminal identification and other crime records.” In 1966, however, Congress had combined § 340 with 5 U.S.C. § 300 (1964), *repealed by* Pub. L. No. 89–554, § 8(a), 80 Stat. 632, 648 (1966), to form present § 534. Section 300 had authorized the Attorney General to appoint officials to exchange “identification and other records.”<sup>19</sup> Section 534, which combines both provisions, not only authorizes the dissemination of “criminal identification” and “crime records,” but also “identification” and “other records.” Accordingly, Congress’ narrow intent in passing 5 U.S.C. § 340 (1964), on which the court in *Menard* relied, does not limit the dissemination of records under the broader language of 28

---

<sup>19</sup> Section 300 was based on the Department of Justice Appropriation Act, 1965, Pub. L. No. 88–527, 78 Stat. 71 § 201 (1964). Similar provisions authorizing the exchange of “identification and other records” had been passed every year since 1932. *See, e.g.*, ch. 361, 47 Stat. 488 (1932).

U.S.C. § 534.<sup>20</sup> Moreover, while the separate legislative history of 5 U.S.C. § 300 (1964), does not clarify the meaning of “other records,” there is no indication that Congress intended to give it the restrictive interpretation which the court in *Menard* gave to 5 U.S.C. § 340 (1964).

Second, *Menard's* interpretation of the language of the statute is illogical. The court apparently did not challenge the obvious authority of the Attorney General to gather and maintain records on criminal investigations. See 498 U.S. at 1029. Thus, the definition of records for purposes of acquisition and storage of information covers records of criminal investigations. The court adopted a narrower interpretation of records, however, with respect to the dissemination of criminal information. In such cases, “records” were defined as matters of official record. This bifurcated definition of record obviously finds no support in the text of § 534. The section authorizes the exchange of “these records,” meaning the same “records” which the Attorney General is permitted to “acquire, collect, classify, and preserve.” Therefore, unless the provision is interpreted to prohibit the Attorney General from maintaining investigatory records, a position that not even the court in *Menard* was willing to adopt, the language of § 534 and its legislative history authorize the dissemination of some types of investigatory information, including, we believe, the entry on USSS-monitored subjects.

Third, the Court in *Menard* partly based its narrow reading of § 534 on the view that dissemination of criminal investigation information would create a constitutional problem which should be avoided through narrow statutory construction. See 498 F.2d at 1029. After *Menard* was decided, however, the Supreme Court in *Paul v. Davis*, 424 U.S. 693 (1976), held that no liberty or privacy interest was implicated by the dissemination of criminal justice information unconnected with any tangible property interests such as employment. Thus, there is no justification for interpreting § 534 so as to avoid constitutional problems with respect to the dissemination of investigatory information only for law enforcement purposes.

In light of all of these factors, we believe that federal courts should not and will not adopt *Menard's* narrow interpretation of § 534 in this context. Section 534, in our view, authorizes the dissemination of investigatory information for law enforcement purposes, including the USSS entry on USSS-monitored subjects.

### *B. The Privacy Act*

Although the USSS and FBI have the authority to disseminate this information, this disclosure must still satisfy the requirements of the Privacy Act. The USSS files are a “system of records” within the meaning of the Privacy Act.<sup>21</sup>

<sup>20</sup> The Court in *Menard* ignored the more expansive language of 28 U.S.C. § 534 because the 1966 amendments specifically stated that they were not intended to change the substantive meaning of the predecessor statutes. See 498 F.2d at 1028–29 n.42, citing Pub. L. No. 89–554, § 7a, 80 Stat. 611, 631 (1966). However, if § 300 authorized the dissemination of investigatory records before it was combined with § 340, then the court's exclusive reliance on the language and history of § 340 was misplaced.

<sup>21</sup> “System of records” is defined as “any records under the control of any agency for which information is retrieved by the name of the individual or by some identifying” symbol. 5 U.S.C. § 552a(5). The USSS's Privacy Act notice on its protective files recognizes that they constitute a “system of records.” See 48 Fed. Reg. 16643 (1981).

The Act prohibits an agency from “disclosing” to another agency any record which is contained in a “system of records” unless the subject of the record gives his consent or one of several other exceptions are met. The only exemption that might permit the transmission of information on USSS-monitored subjects is that exemption which authorizes disclosure for a “routine use” of the information, 5 U.S.C. § 552a(b)(3), *i.e.*, “use [of the record] for a purpose which is compatible with the purpose for which it was collected.” 5 U.S.C. § 552a(a)(7).<sup>22</sup> Thus, dissemination of the records from the USSS to the NCIC, and from the NCIC to the various participating law enforcement agencies, must each come within this exception to satisfy the requirements of the Act.

The precise meaning and outer limits of the “routine use” exception have not been clearly delineated. In adopting this admittedly “ambiguous” language, 120 Cong. Rec. 36957 (1974) (remarks of Reps. Ichord and Erlenborn), it was recognized that “[i]t would be an impossible legislative task to attempt to set forth all of the appropriate uses of Federal records about an identifiable individual.” 120 Cong. Rec. 36967 (1974) (remarks of Rep. Moorhead). It is clear, for example, that the exemption may cover the dissemination of information even though it is used for a purpose different from the one for which it was collected. *See, e.g.*, 120 Cong. Rec. 36967 (1974) (remarks of Rep. Moorhead); 120 Cong. Rec. 40406 (1974) (remarks of Sen. Ervin); OMB Circular No. A-108 (1975), 40 Fed. Reg. 28953 (1974); *United States v. Collins*, 596 F.2d 166 (6th Cir. 1979) (per curiam); *Burley v. United States Drug Enforcement Administration*, 443 F. Supp. 619, 623 (M.D. Tenn. 1977). The “routine use” exemption may also permit dissemination of information for a particular purpose even though the dissemination occurs infrequently. *See* 120 Cong. Rec. 36967 (1974) (remarks of Rep. Moorhead).

Because of the difficulty in defining legislatively the limits of the routine use exception, Congress chose to prevent irregular disclosures under this exemption primarily by requiring agencies to promulgate the regulations setting forth the “routine uses” of their own information. Under 5 U.S.C. § 552a(e)(4) & (11), agencies must publish the routine uses of information in the *Federal Register* 30 days before dissemination for notice and comment. This “public scrutiny” was intended to “caution . . . agencies to think out in advance what uses it will make of information,” 120 Cong. Rec. 40406 (1974) (remarks of Sen. Ervin) and provide a “check” against “potential bureaucratic abuses.” 120 Cong. Rec.

---

<sup>22</sup> The Privacy Act also exempts disclosure to any government agency “for a civil or criminal law enforcement activity,” but only “if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.” 5 U.S.C. § 552a(b)(7) Because requesting agencies in the NCIC do not make written requests for information, this exception would not exempt the exchange of information through the NCIC.

The other exceptions also do not cover the exchange of information through the NCIC. They exempt the disclosure of information to employees of the agency that maintains the record; to the Bureau of the Census for Census purposes; to the National Archives if the information is of historical value; to either House of Congress; to a committee of Congress if within its jurisdiction, to the Comptroller General if pursuant to its GAO duties, to a court of competent jurisdiction if pursuant to court order, to a recipient who gives adequate assurances that the information will be used for statistical purposes and the information is transmitted so as not to be personally identifiable, to a person who can show “compelling circumstances” affecting the health or safety of the subject of the file; and pursuant to the Freedom of Information Act. 5 U.S.C. § 552a(b).

36655 (1974) (remarks of Rep. Moorhead). The only cases to date in which courts have disallowed disclosures of information sought to be transmitted under this exception have arisen where the agency failed to satisfy the procedural requirements of public notice and comment. *See, e.g., Parks v. United States Internal Revenue Service*, 618 F.2d 677 (10th Cir. 1980).

Assuming the USSS and FBI satisfy these procedural requirements of public notice and comment, we believe that the transmission of the proposed information on USSS-monitored subjects into the NCIC, and from the NCIC to other federal and state agencies, would come within the “routine use” exception. The proposal involves the transmission of two types of information. First, the names of and identifying information about these individuals would be disclosed to a participating agency in order to obtain current information from that agency about the subject. In such cases, the information on the subject is being disclosed for the same purpose for which it was originally collected—protection of protectees—and therefore is clearly a “routine use.”

Second, certain evaluative descriptions, such as “potentially dangerous to a protectee,” “mentally unstable,” or “armed and dangerous,” are disclosed, according to your letter, essentially to assist law enforcement personnel in their own dealings with the subject. *See* Opinion Request, p. 3. So long as law enforcement personnel are obtaining the information to further a criminal investigation or an arrest, and the information may be of assistance in this effort, this use would appear to be “compatible” with the use for which the information has been collected. The information is being used to assess the subject with regard to the possible commission of a crime and his danger to police officers. Moreover, this disclosure may also assist in the protection of the President and other protectees by making local law enforcement personnel aware of possible threats to protectees and the specific danger they pose.<sup>23</sup>

We caution, however, that disclosure of the information for the purpose of making non-law enforcement decisions, such as licensing or employment, which are unrelated to criminal investigation, would present different issues. Such use might well not satisfy the underlying intent of the routine use exemption in many cases. The purpose of the “routine use” exception is “to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency’s reasons for using and interpreting the material.” 120 Cong. Rec. 40406 (1974) (remarks of Sen. Ervin) (“Analysis of House and Senate Compromise Amendments to the Federal Privacy Act”). Designation of certain individuals as dangerous to protectees or “mentally unstable,” as the above discussion has suggested, may often be based on necessarily tentative, highly prejudicial and conclusory judgments. While such evaluations may be valuable to law enforcement investigation, they may be

---

<sup>23</sup> We note, however, that this issue will probably be litigated if individuals in the file believe that they have been subjected to police harassment as a result of this designation. Accordingly, we recommend, as discussed in greater detail below, that adequate precautions be taken to assure that designations are accurate, timely, and no more derogatory than is necessary to provide needed information. It is also extremely important, as the proposed entry provides, to warn local officials *not* to arrest the subject based on the NCIC entry.

unduly prejudicial when used for purposes such as employment or licensing, which are unrelated to criminal investigation. Employment personnel clearly “may not be as sensitive to the [USSS’s] reasons for using and interpreting the material.”<sup>24</sup>

This possibility is underscored by the legislative history of 5 U.S.C. § 552a(k)(3), which permits USSS protective files to be exempted from the access requirements of the Act. In speaking against a proposed amendment that would have deleted this exemption, Representative Erlenborn conceded that “real harm” could result from the dissemination of USSS investigatory information “to some other agency where the person would be harmed in his application for employment or some other right or privilege under the laws of the United States.” 120 Cong. Rec. 36966 (1974). He recommended that the exemption for USSS protective files should be passed only because the “prohibition of transfer to other agencies,” except for routine uses, would still apply to USSS files. *Id.* Thus, Congress may have exempted USSS protective files from the access requirements of the Act with the understanding that the restrictions on dissemination of these files to other agencies would be carefully scrutinized.

Dissemination of this information for non-law enforcement purposes could also create serious constitutional problems. In *Paul v. Davis*, 424 U.S. 693 (1976), the Supreme Court held that no liberty or privacy interest of the plaintiff was violated by a police department’s dissemination of a flyer identifying him as an “active shoplifter.” The Court reasoned that defamation, “standing alone,” does not deprive an individual of any liberty interest protected by the procedural guarantees of the Fifth and Fourteenth Amendments. 424 U.S. at 709. The Court suggested in dicta, however, that imposition by the government of a stigma plus a loss in government employment might trigger a liberty interest. Other cases have similarly suggested that a stigmatizing government disclosure coupled with the loss of employment or property interest might trigger due process protection. See *Owen v. City of Independence, Mo.*, 445 U.S. 622, 633 n.13 (1980); *Board of Regents v. Roth*, 408 U.S. 564, 573 (1972). Although we need not reach the question of whether and when dissemination of information on USSS-monitored subjects for non-law enforcement purposes would be impermissible, in light of these decisions and the legislative history of the Privacy Act,<sup>25</sup> we strongly

---

<sup>24</sup> We note that one court has held that the disclosure of drug investigation records about a state pharmacist to a state licensing board constituted a routine use. See *Burley v. United States Drug Enforcement Administration*, 443 F Supp 619, 623–24 (M D Tenn 1977). In contrast to the general and conclusory designation of individuals as a “threat to a protectee” or “mentally unstable,” however, drug investigation information is directly relevant to the licensing decision of such boards. Moreover, as the court noted, 21 U.S.C. § 873 specifically authorizes the Attorney General to disclose drug investigation information to state officials.

<sup>25</sup> Dissemination for non-criminal investigation purposes could also restrict the flexibility of the USSS in gathering information about USSS-monitored subjects. The Privacy Act requires federal agencies to “collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual’s rights, benefits, and privileges under Federal programs.” 5 U.S.C. § 552a(e)(2). Dissemination of information on USSS-monitored subjects in a way that would result “in adverse determinations about an individual’s rights, benefits, and privileges under Federal programs” would therefore require the USSS to collect information on USSS-monitored subjects “as much as practicable” from the subjects themselves, unless the information were construed to come within the law enforcement exemption to this requirement. See 5 U.S.C. § 552a(j)(2)(B).

recommend that care be taken to assure that dissemination of this information is strictly limited to law enforcement purposes.<sup>26</sup>

#### IV. Maintaining the Accuracy of Information on USSS-Monitored Subjects

Finally, we note that even though the NCIC has the authority to disseminate this information to law enforcement agencies, § 534 and the Privacy Act, 5 U.S.C. § 552a(e)(6), require that reasonable efforts be made to assure that the information is accurate and relevant to its use for law enforcement purposes. In *Tarlton v. Saxbe*, 507 F.2d at 1125, the D.C. Circuit “interpret[ed] § 534 in a manner designed to prevent government dissemination of inaccurate criminal information without reasonable precautions to ensure accuracy.” See also *Pruett v. Levi*, 622 F.2d 256, 257 (6th Cir. 1980); *United States v. Doe*, 556 F.2d 391, 393 (6th Cir. 1977); *Menard v. Saxbe*, 498 F.2d at 1026. *Tarleton* recognized, however, that this “duty must be accommodated to the particular role the FBI plays in the collection and dissemination of criminal information in the Federal system, the FBI’s capacity to take reasonable measures to ensure accuracy and the practicalities of judicial administration and executive efficiency.” *Id.* at 1126. Similarly, the Privacy Act, 5 U.S.C. § 552a(e)(6), provides that “prior to disseminating any record about an individual to any person other than an agency . . . , [an agency must] make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes.” Since state law enforcement agencies with access to the NCIC are not agencies within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1),<sup>27</sup> the FBI should satisfy this standard if the records are to be introduced into the NCIC for general dissemination.<sup>28</sup>

Because we are not sufficiently familiar with the process by which individuals receive designations such as “dangerous” to a protectee or “mentally unstable,” we believe that it would be inappropriate for us at this time to express an opinion on what procedural safeguards should be provided. We emphasize that some periodic reassessment of these designations, as your proposal indicates will be undertaken, would probably be necessary. We also believe that the entry on USSS-monitored subjects should clearly note, as the current proposal provides, that the individual should not be arrested as a result of the entry.<sup>29</sup> *Cf. Testa v.*

---

<sup>26</sup> We note that information on USSS-monitored subjects in the NCIC file would remain exempt under 5 U.S.C. § 552a(k)(3) from the access requirements of the Privacy Act. This provision permits the head of an agency to exempt files which are “maintained in connection with providing protective services pursuant to section 3056 . . . .” Although the new NCIC files on USSS-monitored subjects are not maintained “by” the USSS, they are maintained “in connection with” providing protective services under § 3056.

<sup>27</sup> Agency means “agency as defined in § 552(e) of Title 5,” which does not include state institutions.

<sup>28</sup> Section 552a(e)(5) also requires that an agency “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” Because dissemination of these files through the NCIC is clearly covered by 5 U.S.C. § 552a(e)(6), we need not decide whether inclusion of an individual in the file on USSS-monitored subjects for law enforcement purposes is a “determination” within the meaning of the section.

<sup>29</sup> See note 3, *supra*.

*Winqvist*, 451 F. Supp. 388, 394–95 (D.R.I. 1978) (operator of criminal history computer system may be held liable for knowing dissemination of inaccurate information which leads to unconstitutional arrest). If you would like us to look into this issue after being briefed in more detail about the investigation process, we will be happy to do so.<sup>30</sup>

### **Conclusion**

We believe that the USSS has the authority to monitor the activities of individuals who are not the subject of an arrest warrant so long as the USSS reasonably believes they may pose a threat to protectees. We also believe that the USSS can introduce the proposed information about USSS-monitored subjects into the NCIC. We emphasize, however, that care should be taken to assure that evaluative information about such individuals is periodically reevaluated and not disseminated from the NCIC for non-law enforcement purposes.

THEODORE B. OLSON  
*Assistant Attorney General*  
*Office of Legal Counsel*

---

<sup>30</sup> Finally, we note that establishment of the new file in the NCIC would require amendment of the present regulations on the operation of the NCIC, *see* 28 C.F.R. §§ 20.1–20.38 (1981), as well as a new Privacy Act disclosure statement for both the USSS and NCIC. *See* 5 U.S.C. § 552a(e)(4) & (11)