Outside Counsel

Outside Counsel

Privacy Act Governs Release of Agency Records
By Harry A. Valetk
New York Law Journal

It is no secret that the Social Security Administration (SSA) has detailed information on virtually every individual in this country. [1] With this in mind, litigants often serve subpoenas on SSA personnel requesting "any and all" records belonging to their adversary. Presumably, litigants are seduced by the prospect of getting confidential medical records, comprehensive individual earnings reports, and other reliable statistical information maintained by SSA.

However, the Privacy Act prohibits SSA from releasing an account holder's records without that individual's written consent, unless a statutory exception applies. Similarly, SSA's own regulations take many precautions, recognizing that account holder records contain very sensitive information required by statute to establish entitlement to benefits.[2] Unfamiliar with the relevant Privacy Act provisions and SSA's strict privacy safeguards, litigants often waste valuable time and resources serving unenforceable court subpoenas on SSA's personnel.

To better understand the legislative background underlying the need for prior written consent, notwithstanding an order from a state court, this article will review both the relevant sections of the Privacy Act and the case law on a State court's lack of jurisdiction over federal agencies. The article will also discuss appropriate procedures for obtaining an individual's Social Security records by either court order or written consent.

The Privacy Act requires that all federal agencies protect the privacy rights of individuals whose records it may possess. Specifically, the

Privacy Act provides that:

No agency shall disclose any record which is contained in a system of records by any means of communication to any person . . . except pursuant to the written request by, or with the prior written consent of, the individual to whom the records pertains . . . .[3]

Explaining its purpose, Congress declared that:

The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies . . . to (1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies; (2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available . . . without his consent . . . .[4]

Emphasizing the importance of consent, the House Report reveals that:

[t]he consent requirement may well be one of the most important, if not the most important, provisions of the bill. No such transfer could be made unless it was pursuant to a written request by the individual or by his prior written consent. This requirement would apply to all so-called "non-routine" transfers of information.[5]

The Privacy Act lists twelve exceptions to the general "no disclosure without consent" rule. The focus of our discussion here will be the eleventh exception allowing disclosure without consent "pursuant to a court order of competent jurisdiction."[6]

Competent Jurisdiction

A common source of confusion is the statutory definition of a "court order" for Privacy Act purposes. Although the term is not defined by the Privacy Act, the Court of Appeals for the District of Columbia Circuit held that a subpoena routinely issued by a court clerk is not a "court order" within the meaning of the Privacy Act exception because it is not "specifically approved" by a judge. *Doe v. DiGenova*, 779 F.2d 74, 77-85 (D.C.Cir. 1985); *Doe v. Stephens*, 851 F.2d 1457, 1467 (D.C.Cir. 1988) ("[t]o read the 'order of the court' language as permitting disclosure pursuant to a subpoena, would create a gaping hole in the overall scheme of the Privacy Act."). However, even "so ordered" subpoenas fail to satisfy the individual privacy protections available under the Privacy Act, unless issued from a court of competent jurisdiction.[7]

Another popular misconception is that state courts are courts of "competent jurisdiction" under the Privacy Act. In fact, many litigants incorrectly assume that they can obtain agency records without consent by serving a state court subpoena as an order of a court of competent jurisdiction. However, courts have long held that state courts lack authority to compel federal agencies or officials to testify or produce documents under the doctrine of sovereign immunity.[8] See, e.g., *Block v. North Dakota*, 461 U.S. 273, 287 (1983) (holding United States and its agencies are not subject to judicial proceedings unless there is an express waiver of doctrine of sovereign immunity);

Smith v. Cromer, 159 F.3d 875, 882 (4th Cir. 1998) (finding doctrine of sovereign immunity divested state court of jurisdiction to enforce subpoena); *In re Elko County Grand Jury*, 109 F.3d 554, 556 (9th Cir. 1997) (finding state court lacked jurisdiction to compel federal employee to appear and testify before grand jury); *Houston Bus. Journal Inc. v. Office of Comptroller of Currency*, 86 F.3d 1208, 1211-12 (D.C.Cir. 1996) (holding state court, and federal court on removal, lacked jurisdiction to compel production of records); *Edwards v. U.S. Dep't of Justice*, 43 F.3d 312, 317 (7th Cir. 1994) (holding state court lacked jurisdiction to independently compel the testimony or production of documents when contrary to valid agency regulation); *Louisiana v. Sparks*, 978 F.2d 226, 234-26 (5th Cir. 1992) (granting motion to quash state court subpoena on sovereign immunity grounds).

In the context of a subpoena, federal courts have held that State court litigants seeking SSA records without the account holder's consent will not prevail. See e.g., *Mason v. S. Bend Comty. Sch. Corp.*, 990 F.Supp. 1096 (N.D.Ind. 1997) (finding SSA was justified in failing to produce protected records because party requesting documents must show that release without written consent is authorized by law); *Phoenix Ins. Co. v. Phillips*, 2000 WL 680334, 2 (E.D.La. May 24, 2000) (finding subpoena for Social Security records without defendant's consent was improper).

Unlike a State court litigant, however, a federal court litigant may obtain agency records without consent by means of a "so ordered" federal subpoena, even when the United States is not a party. See, e.g., *U.S. Envtl. Prot. Agency v. General Electric Co.*, 197 F.3d 592, 598 (2d Cir. 1999), aff'd on reh'g, 212 F.3d 689 (2000) (finding federal government waives sovereign immunity under Administrative Procedure Act insofar as federal court may require agency to respond to subpoena seeking documents in action to which agency is not a party); *Houston Business Journal*, 86 F.3d at 1212 (holding that in federal court, the federal government waives sovereign immunity and federal agency may not withhold documents from a federal court). But cf., *Edwards*, 43 F.3d at 317 (stating that federal employee cannot be compelled to obey a subpoena - even a federal subpoena - that is against valid agency regulations).

Even when SSA is served with a federal "so ordered" subpoena, it must still comply with the additional restrictions imposed by the Social Security Act and SSA regulations.[9] To ensure full compliance, the Social Security Act imposes fines on SSA employees of up to $10,000, imprisonment not exceeding 5 years, or both for each violation. Specifically, the Social Security Act states that:

No disclosure of any . . . file, record, report, or other paper, or any information, obtained at any time by the Commissioner of Social Security or by any officer or employee of SSA in the course of discharging the duties of the Commissioner under this chapter, and no disclosure of any such file, record, report, or other paper, or information, obtained at any time by any person from the Commissioner or from any officer or employee of the SSA shall be made except as the Commissioner may by regulations prescribe and except as otherwise provided by Federal law. Any person who shall violate any provision of this section shall be deemed guilty of a felony and, upon conviction thereof, shall be punished by a fine not exceeding $10,000 for each occurrence of a violation, or by

imprisonment not exceeding 5 years, or both.[10]

Concerning court orders, SSA's regulations recognize that:

The Privacy Act allows us to disclose information when we receive an order from a court of competent jurisdiction.

However, much of our information is especially sensitive. Participation in Social Security programs is mandatory, and so people cannot limit what information is given to SSA. When information is used in a court proceeding, it usually becomes part of a public record, and its confidentiality cannot be protected.[11]

Conditions of Disclosure

To simultaneously adhere to the Privacy Act's restrictions and comply with a federal court's order, SSA's regulations allow disclosure pursuant to a competent court order only if:

1. another section of this part would specifically allow release;[12]

2. The Commissioner of SSA is a party to the proceeding; or

3. The information is necessary for due process in a criminal proceeding. In other cases, we try to satisfy the needs of courts while preserving the confidentiality of the information. [13]

Courts have held that a proper procedural device for protecting the particularly sensitive information found in an individual's SSA records, while satisfying the needs of the courts, is through a protective order. [14] Addressing this issue, the District of Columbia Circuit Court of Appeals stated that "the fact that a document is subject to the Privacy Act is not . . . irrelevant to the manner in which discovery should proceed. Although discovery standards . . . permit access . . . those same . . . standards give the district court ample discretion to fashion protective orders upon a showing of 'good cause.'" *Laxalt v. McClatchy*, 809 F.2d 885, 889 (D.C.Cir 1987); see also *Boudreaux v. United States*, 1999 WL 499911, at 1-2 (E.D.La July 14, 1999) (ordering in camera review of Privacy Act-protected documents so that legitimacy of agency objections may be determined).

One disadvantage to using protective orders instead of actual consent is that protective orders can be burdensome on both parties.

For example, a typical protective order restricts the manner in which the subpoenaed information can be used and often requires that a copy of the protective order be delivered to every attorney, administrative staff, intern, expert witness, and court reporters employed by the firm or associated with the case.

Most mid-sized firms, for example, with offices and affiliations in other parts of the world, would find that this burdensome task exponentially increases costs and unnecessarily delays disclosure. At the end of the litigation, protective orders generally require the return of all original and photocopied confidential documents disclosed under court order.

Now that we established the importance of getting an account holder's consent, we can discuss the essential information a consent should include.[15] To be effective, a consent need only be:

(a) in writing;

(b) signed and dated by the account holder;

(c) specifically authorize SSA to release records;

(d) specify the information to be disclosed; and

(e) specify to whom the records may be disclosed.[16]

Agency regulations also provide that SSA will verify the account holder's identity and the identity of the individual authorized to receive the information.[17] To comply with this requirement, a consent must include:

1. an account holder's social security number;

2. date of birth; or

3. other personally identifiable information.

Likewise, paying close attention to the date that a consent was executed can mean the difference between a valid consent and an expired one. For example, SSA policy directs that consents to disclose medical records are acceptable only if submitted within 90 days from the date of execution.[18] Consent to release tax information are acceptable only for 60 days.[19] For non-medical records, SSA will accept consents submitted within one year of execution.[20]

However, few realize that SSA will apply these strict time frames only when the individual does not specify a time frame on the consent. Indeed, SSA policy is to honor any time frame for consent which is indicated by the account holder.[21] Litigants swamped with discovery and pre-trial minutiae would find the power to get medical records long after the general 90-day limit for medical records to be very valuable. For best results, consents should be made "valid through the completion of trial."

In cases where an account holder refuses to authorize disclosure, seasoned counsel may petition the court to compel authorization. Under Rule 26(a)(1)(B) of the Federal Rules of Civil Procedure, a party is required to provide to other parties "a copy of . . . all documents, data compilations, and tangible things in the possession, custody, or control of the party that are relevant to disputed facts alleged with particularity in the pleadings."

In one case, a Pennsylvania federal district court ordered a plaintiff alleging civil rights violation by police officers to produce or sign a form authorizing the release of her social security records within 10 days.[22] When plaintiff failed to provide the authorization, the court dismissed her complaint under Rule 37(b)(2)(C) of the Federal Rules

of Civil Procedure.

In a New York State Surrogate Court case, a court ordered the Executor of a Will to execute an authorization which would permit the contestants to obtain copies of the decedent's Social Security checks for the period between 1976 and 1978.[23] Reasoning that because the Social Security documents were material, necessary, and could not be examined without the Executor's authorization, the court concluded that the information was "under the control" of the Executor within the meaning of Civil Practice Law and Rules 3120.24

Conclusion

In sum, before you spend the time and expense of serving an unenforceable subpoena for individual records on SSA personnel, remember that the Privacy Act will likely protect an account holder's records unless that individual authorizes release in writing. If the dynamics of your case make it unlikely that you can voluntarily get written consent, ask the court to compel the account holder to authorize release when such records are relevant to the case. Harry A. Valetk *is an assistant regional counsel for the New York Office of the Regional Chief Counsel, Social Security Administration. The opinions in this article belong to the author and are not those of the administration.*

FootNotes: [1]

The author would like to thank to Sybil L. Burnett for her valuable contributions to this article. [2]

20 C.F.R. §401.105(b). [3]

5 U.S.C. §552a(b). [4]

Id., at (b)(1)-(2). [5]

H.Rep. No. 93-1416 Privacy Act of 1974, 93rd Cong., 2d Sess. 25, at 12 (Oct. 2, 1974). [6]

5 U.S.C. §552a(b)(11). [7]

Id. [8]

14 Wright & Miller, Federal Practice and Procedure, §3655. [9]

42 U.S.C. 1306(a). [10]

42 U.S.C. §1306(a) (emphasis added). [11]

20 C.F.R. §401.180(a) (2000). [12]

For instance, other provisions of SSA's regulations allow for disclosures if required by law, "routine uses," law enforcement purposes, health or safety, statistical and research activities, and Congress, General Accounting Office, Bureau of the Census, National

Archives, and Blood Donor Locator Services. 20 C.F.R. §§401.120, 401.150 - 401.175, 401.200. [13]

20 C.F.R. §401.180(b) (emphasis added). [14]

Fed. R. Civ. P. 26(c). [15]

20 C.F.R. §401.100(a) (2000). [16]

SSA Programs Operations Manuals Systems §03305.001 (2000). [17]

[18]

Id. [19]

Id. [20]

Id. [21]

Id. [22]

Funk v. Disciplinary Bd. of the Commonwealth of Pennsylvania, 1990 WL 82120 (E.D.Pa. June 12, 1990). [23]

In the Matter of the Estate of Chauncey Mann, 99 Misc.2d 758, 760 417 N.Y.S.2d 193 (1979).

Date Received: *May 18, 2001*