Office of Governmental Liaison and Disclosure
Internal Revenue Service
1111 Constitution Ave., NW
Washington, DC 20224

Proposed Rule, IRS 50.22 Tax Exempt/Government Entities Case Management Records

Comments of the Electronic Privacy Information Center

In response to the Internal Revenue Service's Privacy Act System of Records notice issued on December 7, 2005,[1] the Electronic Privacy Information Center submits these comments. EPIC strongly urges the IRS not to exempt its Tax Exempt/Government Entities Case Management Records ("TE/GE System") from requirements that its information be relevant and necessary for its purpose. EPIC also recommends that the IRS limit the scope of its exemptions from the Privacy Act requirements to provide access and correction rights to individuals.

EPIC is a non-profit public interest research organization founded in 1994 to focus public attention on emerging civil liberties and First Amendment issues and to protect privacy. EPIC has long been involved in the debates surrounding the continuing application and implementation of the Privacy Act of 1974, participating through comments on many agencies' systems of records notices,[2] as well as *amicus* briefs in

[1] Proposed Rule, 70 Fed. Reg. 72876 (Dec. 7, 2005).
[2] *See, e.g.*, Comments of EPIC on Notice to Alert Two Systems of Records, Dec. 8, 2005, *at* http://www.epic.org/privacy/airtravel/profiling/rt120805.pdf; Comments of EPIC on the Terrorist Screening Records System, Sept. 6, 2005, *at* http://www.epic.org/privacy/airtravel/tsrs_comments090605.html; Comments of EPIC on the Computer Assisted Passenger Prescreening System, Sept. 30, 2003, *at* http://www.epic.org/privacy/airtravel/capps-comments.pdf.

cases litigating Privacy Act jurisprudence.[3] EPIC thus has a twofold interest in this system of records, as both a non-profit corporation, and as an organization devoted to preserving the full enforcement of the Privacy Act to personal information collected by federal agencies.

EPIC therefore urges the IRS to not exempt itself from the Privacy Act's requirement that records in a system be "relevant and necessary" to the agency's purpose. 5 U.S.C. § 552a(e)(1). The privacy of personal information for non-profit organizations is particularly important, as the Supreme Court has made clear that this information is protected by the First Amendment right of association. In *NAACP v. Alabama*,[4] the Supreme Court held that organizations have a constitutional right to keep their membership information private. The Court held that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association[.]"[5] The constitutional right to privacy thus requires that great care be taken in preserving the privacy safeguards afforded to organizations by the Privacy Act.

The Privacy Act's "relevant and necessary" requirement is a fundamental and necessary part of the Privacy Act's protections, as it is

> designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary.[6]

Part of the Privacy Act's purpose was to stave off the risk that government databases might become dossiers cataloging the various details of individuals' lives. By limiting

---

[3] *See* Amicus Brief of EPIC, *et al*, *Doe v. Chao*, 540 U.S. 614 (2004), *at* http://www.epic.org/privacy/chao/Doe_amicus.pdf.
[4] 357 U.S. 449 (1958).
[5] *Id.* at 1172.
[6] S. Rep. No. 93-3418, at 47 (1974).

the data kept by an agency to that which is necessary and relevant to the agency's purpose, the Privacy Act limits the extent to which a system of records may invade privacy. Limiting the data to that which is necessary and relevant also reduces the risk of "mission creep," in which a system is pressed into unintended uses. Such mission creep presents additional opportunity for errors, as has been see in the demise of the Transportation Security Administration's second-generation Computer Assisted Passenger Prescreening System (CAPPS II) program.[7]

The IRS claims that, as a system of investigatory records, the TE/GE System must gather data whose relevance may not be known at the time. The IRS also notes that relevance and necessity are questions of judgment and timing. An investigation will likely begin with a broader scope than it ends with, and information at first gathered may later become irrelevant and unnecessary. However, the mere fact that relevance and necessity may change should not be a reason for the IRS to completely absolve itself of its Privacy Act obligations. A blanket exemption from the § 552a(e)(1) requirements would allow the records to contain wholly and blatantly irrelevant and unnecessary information unrelated to any purpose of the IRS. Furthermore, in assessing the necessity and relevance of records kept in a system, the nature of the system would be taken into account. Any facts in the system that might be helpful to the IRS in a particular investigation would hopefully be relevant and necessary to the investigation at some stage, and thus in compliance with the Privacy Act. As investigations proceed to a close, information can be added or removed from the system as it becomes more or less relevant and necessary. Therefore, the IRS should not exempt its TE/GE System from the

[7] Matthew L. Wald and John Schwartz, *Screening Plans Went Beyond Terrorism*, N.Y. Times, Sept. 19, 2004, at A35.

relevance and necessity requirements, as doing so would eliminate a vital privacy safeguard while failing to add any flexibility benefits not already provided by the Act.

EPIC also urges the IRS to limit its exemptions from the Privacy Act's provisions requiring disclosure to individuals of records kept about them[8] and requiring notification of the systems of records and how to access them.[9] The IRS notes that these provisions, if implemented, may put entities on notice that they are being investigated. While EPIC recognizes the need to withhold notice during the period of the investigation, entities should be able to know, after an investigation is completed or made public, the information stored about them in the system. Since the IRS depends, at least in part, upon informants to initiate investigations, tax-exempt organizations may find themselves investigated due to malicious misinformation spread by ideological opponents or other bad actors. Furthermore, many tax-exempt organizations critical of government practices have found themselves under increased scrutiny by the IRS.[10] Access to records of a completed investigation, with appropriate redactions to protect the identities of confidential informants, would provide individuals and entities with the right to address potential inaccuracies and misinformation resulting from such investigations. Such access could also aid the organizations in maintaining compliance with their tax-exempt status, by revealing the basis for the investigation. Providing access to information on

[8] 5 U.S.C. § 552a(c)(3).
[9] 5 U.S.C. § 552a(d) (1), (2), (3), and (4); 5 U.S.C. § 552a (e)(4) (G) and (H); 5 U.S.C. § 552a(f).
[10] *See* Mike Allen, *NAACP Faces IRS Investigation*, Washington Post, Oct. 29, 2004, *available at* http://www.washingtonpost.com/wp-dyn/articles/A7433-2004Oct28.html (noting that both the NAACP and the Christian Coalition have been investigated under allegations of political campaigning).

completed investigations would not undermine the IRS's law enforcement purposes, while protecting the privacy rights of entities and their individual members.

For the foregoing reasons, EPIC urges the IRS not to exempt itself from the relevance and necessity requirements of the Privacy Act, and to limit the scope of its exemptions from the notice and access provisions, by allowing entities to access files kept on them, insofar as the investigations have been completed.

Respectfully Submitted,

Marc Rotenberg
Executive Director
Electronic Privacy Information Center

Sherwin Siy
IPIOP Staff Counsel
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington DC 20002
(202) 483-1140