Comments of the World Privacy Forum

Regarding

Department of Justice AAG/A Order No. 018-2006, Privacy Act of 1974, System of Records Notice

Via email, postal mail, and facsimile

Mary E. Cahill,
Management and Planning Staff
Justice Management Division
Room 1400, National Place Building
United States Department of Justice
Washington, DC 20530–0001

Re: 71 Federal Register 63354 (October 30, 2006) AAG/A Order No. 018-2006, Privacy Act of 1974; System of Records Notice

November 17, 2006

This is a comment on the Department of Justice's proposal to add a routine use to all departmental Privacy Act of 1974 systems of records. The proposal appears in 71 Federal Register 63354 (October 30, 2006). The notice includes a proposed new routine use that would allow "disclosure to appropriate persons and entities for purposes of response and remedial efforts in the event that there has been a breach" of personal data in departmental systems of records.

The World Privacy Forum is a non-profit, non-partisan public interest research organization. It focuses on in-depth research and analysis of privacy topics. See <http://www.worldprivacyforum.org>. We appreciate the opportunity to comment on this issue. We have a number of substantive concerns about the proposed routine use, which we discuss below.

I. Necessity

It is difficult to evaluate the proposed routine use as published because of the vagueness of the wording of the routine use and the lack of sufficient justification in the published notice. The publication contains only a single paragraph of explanation for applying a routine use to dozens of different systems of records containing substantially different types of records. The types of records include highly sensitive records such as Criminal Division Witness Security File (CRM-

002) to Witness Immunity Records (CRM-022) to the National Instant Criminal Background Check System (NICS, FBI-018). It is difficult to envision who the possible recipients might be and why those recipients are not already covered by existing routine uses.

Any disclosure necessary for a law enforcement investigation or prosecution of a security breach is already covered by the Privacy Act itself, either by existing routine uses, or by subsection (b)(1) of the Act covering disclosures within the Department. If there is a need to share information with contractors hired by the Department to ameliorate the harm from a data breach, routine uses covering contractor disclosures should be adequate. A common routine use for many Privacy Act systems covers disclosure to "contractors, experts, and consultants when necessary to accomplish an agency function related to a system of records."

It is interesting that some, but not all, Department of Justice (DOJ) systems of records have contractor routine uses. If the Department contemplates disclosure of information to anyone not hired by the Department and made subject to contractual limitations on the use of the data, it should include that information in its justification and within the routine use.

If the DOJ needs the routine use to comply with the requirements of the Office of Management and Budget (OMB) Memorandum M-06-19 (reporting security incidents to the Department of Homeland Security), a simple and narrow routine use would be more than sufficient. However, the OMB requirement is that security incidents be reported. Nothing requires the reporting of any personal data that is the subject of a security breach. Even considering mandatory breach reporting requirement, the necessity for the routine use remains in doubt.

II. Vagueness

The proposed routine use appears to allow disclosure of any Privacy Act record in the Department to quite literally anyone in the world, and this is not intended as a glib statement. The actual text says that disclosure is permitted to "appropriate agencies, entities, and persons." The use of the modifier *appropriate* offers no clear limitation. A routine use that potentially allows disclosure to anyone and everyone is simply too vague to meet statutory standards for identifying the potential recipients of Privacy Act information. Indeed, the Privacy Act Overview published by the Department itself cites a case that found the use of *appropriate* as a qualifier to be insufficient in a routine use.[1]

The Department has an obligation to tell the public precisely what individuals and which institutions in what parts of the world might be appropriate recipients under this routine use. Would the Department of Homeland Security be a possible recipient under this routine use? Would commercial data brokers with anti-fraud products or services be a possible recipient under this routine use? Would financial sector companies such as credit bureaus be the recipients under this routine use? The point is that all of these institutions and infinitely more are potential recipients under the proposed routine use as currently drafted. The Department needs to be

[1] See < http://www.usdoj.gov/oip/1974condis.htm#routine>. ('In Krohn v. United States Department of Justice, No. 78-1536, slip op. at 4-7 (D.D.C. Mar. 19, 1984), however, the court invalidated an FBI routine use allowing for "dissemination [of records] during appropriate legal proceedings," finding that such a routine use was impermissibly "vague" and was "capable of being construed so broadly as to encompass all legal proceedings."').

specific and unambiguous in describing who would be eligible to receive personal information from so many different and sensitive systems of records.

The remainder of the routine use seeks to identify the purpose of the disclosure. This part too suffers from vagueness. The first clause allows disclosure when "it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised." The Department needs to make clear precisely who has to suspect or confirm the compromise. Otherwise, speculation in the Washington Post or the suspicions of a GS-5 clerk in the Department could meet the standard. At a minimum, any "suspicions" or "confirmations" should come from a politically accountable appointee within the Department. Beyond this, there needs to be specific and detailed procedural guidelines for determining what should constitute "suspicion."

The second clause allows disclosure when "the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information." Proving an economic or property interest under the Privacy Act of 1974 can be complex and challenging. Suppose that a different interest is affected by a security breach. A security breach might be potentially embarrassing to a data subject or cause harm to reputation. Would that type of harm permit the Department to make a disclosure? It is not clear why non-economic interests of data subjects have been excluded. While we have doubts about the need for the routine use and the disclosures that it seeks to justify, we think that the second prong should not exclude the possibility of "harm to the privacy interests of data subjects."

We have an additional concern about the second clause. It allows disclosure if there is a risk of harm to the integrity of a system maintained by an "entity." It appears that the recipient of data could be a private entity whose database may suffer harm from the security breach. If so, we question the propriety of these disclosures. When and if the Department should undertake to disclose its own Privacy Act information to a private organization to correct or update information of that organization is far from clear. If a security breach could justify information sharing with a private entity, those circumstances should be more clearly and narrowly defined. The open-ended authority of the proposed routine use is troubling.

The third clause has problems as well. It provides for disclosure when "the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm." This clause repeats the vague phrase "agencies, entities, and persons" already the subject of a previous comment. There are additional problems. Disclosures to prevent, minimize, or remedy harm seem justifiable, albeit lacking in any clear standard. However, it is not apparent what is meant by "respond to the suspected or confirmed compromise" that is not already included in preventing, minimizing, and remedying the harm. Would an attempt to hide or shift blame for a security breach qualify as a type of response? The possibility is evidence of the vagueness of the language.

If *respond* has some meaning other than preventing, minimizing, or remedying harm, the Department should be more specific. As it stands, the routine use would allow a disclosure of all Privacy Act information in the Department to anyone in the world if some unstated person has a suspicion of a security breach, the Department determines that there is a risk of harm to some unqualified economic or property interest (regardless of the magnitude of the interest), and the Department wants to "respond." Again, we are not being glib; this is an accurate analysis of the language as currently proposed.

Reserving the right to disclose Privacy Act records to anyone so the Department can make some unspecified "response" is just too vague to provide members of the public with the notice contemplated by Congress when it established the ability to add new disclosures via the routine use provision of the Privacy Act.

III. Overbreadth

The notice is overbroad because it allows the disclosure of any and all records in Privacy Act systems. The routine use makes no attempt to limit the type of records that may be disclosed. If the Department has a copy of an individual's medical record (as part of a health care fraud case), the routine use allows disclosure of the entire medical record without limitation. The routine use also appears to allow the disclosure of classified information, other information restricted by law, identities of undercover agents, home addresses of Department employees, and names of confidential informants.

The categories of records that can be disclosed under the routine use should be qualified. Information that is generally restricted by law or policy should not be eligible for disclosure just because there is *suspicion* of a security breach, and the Department is searching for a *response*. The Department has a responsibility to its employees, its informants, the subjects of incomplete investigations, and any other individuals who might be the subject of a DOJ file to narrow the scope of records that can be disclosed. The limits belong in the routine use itself and should not be left to the discretion of unnamed and possibly low-level Department employees.

IV. Justification

The Department seeks to add the proposed routine use to every existing system of records, but it does not explain why the routine use is necessary or appropriate for any system, let alone each system. For example, the Office of Justice Programs system 001 is an Equipment Inventory system. Is there sufficient personal information about individuals (other than title, office, telephone number) so that an unauthorized disclosure would actually give risk to a realistic concern of identity theft? A one-in-a million chance does not justify a routine use and certainly not one as broad as the proposed routine use. Where is the risk assessment for each system of records that would justify the application of a new routine use?

We believe that it would be appropriate for the Department to prepare a detailed, system-by-system Privacy Impact Assessment for the proposed routine use. The OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (M-03-22) states that "PIAs are required to be performed and updated as necessary where a system change creates new

privacy risks." The addition of a routine use to all DOJ systems of record cries out for a Privacy Impact Assessment and a risk analysis. This would be true even if the proposed routine use were more narrowly written and better justified. Is the proposed routine use necessary and worth the risk entailed by the additional disclosure authority contained in the routine use? A detailed, system-by-system evaluation of risk is needed and necessary.

An additional problem is that the Department has not addressed or justified the obvious alternative to a routine use. Disclosure from a Privacy Act system of records is possible with the consent of the data subject. If a breach includes records on a relatively small number of individuals, obtaining consent is a realistic alternative. It is also a reasonable alternative. An individual who is already the subject of a suspected data breach might be just as unhappy about the disclosure of his or her record to any agency, entity, or person selected by the Department for some unspecified "response." Further disclosures made to supposedly to protect an individual might not be welcome and might only compound the problem. The Department should explain why consent could not be used to justify a disclosure, and the bureaucratic convenience of the Department will not be a sufficient justification for every system of records.

V. Publication and Procedure

Lastly, the notice includes a list of DOJ systems of records. We applaud the Department for including this list and, especially, for including the original date and Federal Register citation for what we presume is the last publication of each system of records notice. However, the list reveals that some systems notices have not been updated for ten, twenty, or in some cases nearly thirty years. Evaluating changes to systems of records as published in the Federal Register is difficult enough without having to wade through decades-old publications. It is also difficult to believe that any government system has remained stable enough over decades and has not required a revision of the system of records notice. We will set aside the issue of out of date systems of records notices for another time. However, the issue of the difficulty for a reasonable person to be able to locate all of the original systems of records notices is highly pertinent to the current issue at hand.

The World Privacy Forum asks that the Department republish all of its up-to-date system of records notices in their entirety immediately and at least every two years thereafter. Further, the World Privacy Forum asks that the publication of any change to an existing system of records include the full text of the existing system notice. A publication limited to the text of the new part of a system of records notice makes it extremely difficult to evaluate the change in context. In some cases, it may be necessary for a commenter to locate and then cut and paste several notices of amendments published at different times – even different decades -- in order to recreate the current text of a notice.

We are aware of the compilation of system notices published online by the Federal Register, but the compilation is almost always out-of-date and is difficult to search online. That means that a member of the public who wants to review a proposed change in context must look through the Federal Register to find or reconstruct a current system notice. In the case of the change that is the subject of this comment, that means researching every one of the dozens of departmental systems of record. That burden is overwhelming, and we did not have the resources to undertake

it while preparing these comments. Failure to provide the public with a complete and current text of a current system notice when a change is proposed does not meet the spirit, if not the letter, of the public notice requirements in the Federal Register Act, the Administrative Procedure Act, and the Privacy Act of 1974.

We observe that the addition of a new routine use to every DOJ system of records is likely to require a change to every DOJ form that collects information from an individual. Subsection (e)(3)(C) requires an individual notice on each form used to collect information of the routine uses which may be made of the information. Revising all forms to include a new routine use is a task likely to take years. Further, the failure to include the information promptly on forms may make it impossible to rely on the routine use or – even worse – may make availability of the routine use inconsistent from system to system and perhaps from record to record.

Finally, we observe that the website of the Office of Information and Privacy at DOJ did not in November 2006 include a link to DOJ system of records notices. The website did not even include a link to the Department's Privacy Act rules. We eventually discovered that the Privacy Act rules are available on the website, but it is necessary to click on a link identified only as DOJ FOIA Regulations. We found a list of Privacy Act systems on the website of the Privacy and Civil Liberties Office, but even there we did not find either the current text of all system notices nor the DOJ Privacy Act rules. The Department needs to do a much better job of informing the public about its Privacy Act operations and providing better search and other tools for those who need more information about DOJ systems of records.

Thank you for the opportunity to comment on the proposed routine use.

Respectfully submitted,

Pam Dixon
Executive Director
World Privacy Forum

cc: Jane Horvath
Chief Privacy and Civil Liberties Officer
950 Pennsylvania Avenue, NW
Room 4217
Washington, DC 20530