



WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum to OMB Regarding the proposed revision of Circular A-108 on Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act

Via Regulations.gov

Executive Office of the President,
Office of Management and Budget,
OIRA
725 17th Street, NW
Washington, DC 20503

October 26, 2016

We welcome the opportunity to comment on OMB's redraft of Circular A-108 defining agency responsibilities under the Privacy Act of 1974. The notice seeking comments appeared at 81 Federal Register 69871 (Oct. 7, 2016), <https://www.gpo.gov/fdsys/pkg/FR-2016-10-07/pdf/2016-24239.pdf>.

The World Privacy Forum is a non-profit public interest research and consumer education group. We publish research papers and policy comments focused on privacy and security issues. Much of our work explores technology and health-related privacy issues, biometrics, consent, data analytics, and other rapidly evolving areas of privacy. Our publications and more information about the work of the WPF are at www.worldprivacyforum.org.

In our comments on the proposed circular A-108, located at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/circulars/a108/draft_omb_circular_a_108_10_3_16_clean.pdf, we use the line numbers in the draft to identify the provisions we are addressing in our comments.

I. Timing of a System of Records Notice (lines 243 - 257)

The proposed publication rules for a system of records notice will give rise to unnecessary increases confusion and will have an impact on the public's ability to both understand and comment on system notices. This section of the proposed circular needs to be changed.

In the current proposal, a system notice becomes effective upon publication (with the exception of routine uses, which require a period for public comment), but public comments are still accepted on the system notice after its publication. If an agency receives comments and republishes the notice, the public becomes aware of what happened to the original system notice. If there are no public comments or if the agency chooses not to change the notice, there is no further publication.

Given this set of proposed rules, the public cannot tell whether a system notice is effective as published originally or is undergoing change. This period of limbo can extend for months or longer, and this uncertainty should not be allowed.

OMB should adjust the requirements. Agencies are already required to provide both OMB and the Congress advance notice of a system notice. (See Section 7(b), line 467).

1. OMB should direct agencies to publish system notices and routine uses in the Federal Register at the same time that agencies send the notices to OMB and the Congress.

Subsection (r) of the Act says only that the notice to OMB and the Congress be an “adequate advance” notice. It says nothing about the number of days. OMB can interpret “advance” to be one day before a Federal Register publication. Neither OMB nor congressional review will be undermined if the public receives an earlier notice of Privacy Act activities. This approach makes the first Federal Register publication the equivalent of a request for public comment in advance of a system notice’s effective date.

2. OMB should order agencies to publish a notice stating that a system of records notice or routine use took effect because of a lack of comments or because comments did not require any adjustment. This publication provides formal notice to the public of the status of the system or routine use. If agencies publish in the Federal Register an advance notice as suggested above, a system can take effect upon the publication of the second notice.

None of these changes would interfere with the current procedure for implementing a system earlier with a waiver from OMB.

II. Scope of a SORN (lines 285-323)

The proposed circular language properly suggests that agencies have latitude in defining what constitutes a system of records for purposes of preparing a notice. One of the factors listed in determining the scope of a system is the purpose of the system. The proposed circular suggests that “agencies shall also consider whether different routine uses or security requirements apply to the different groups.” (lines 310-311) We think in determining the scope of a system that there should be greater emphasis on the routine uses.

If all records in a system have the same routine uses, then it is more likely that all the records can be included in a single system if otherwise appropriate. However, where different routine uses apply to different records, there must be a way to segregate application of routine uses. One way

is to not put a record in a system of records if the system allows disclosures that do not apply to that record.

While we do not seek to expand the number of systems of records, we also do not think that routine uses can or should apply to all records in a system if the routine uses do not apply to some records in the system. One alternative is to require that agencies expressly state in a system notice which routine uses apply to which records. Some existing systems do this well. See, e.g., EPA 24, Claims Office Master Files.

The guidance in the circular should be more express with respect to application of routine uses. We suggest language like this:

If all routine uses for a system of records do not apply to all records in the system, an agency should consider changing the scope of the system so that all routine uses apply to all records. In the alternative, if there is a good reason to keep records with different routine uses in the same system, an agency should expressly state in the system notice which routine uses apply to which records.

III. Format and Style of a System of Records Notice (line 278-284)

When an agency changes an existing system notice, the agency can publish for comment only that part of the system notice that is changing. We object to this cut-and-paste method of changing notices. This approach obscures what the agency is doing and makes it much more difficult for the public to understand the nature of the change.

Finding the original notice can be difficult, especially if the original notice predates the electronic availability of the Federal Register. Further, it is possible that there could be a series of changes over time to the system that would require finding more than one previous change to an original system notice and piecing together the changes. Given that agencies are not required to publish a notice stating that it has adopted a system notice or change as originally published, the research required can be especially challenging. We doubt most members of the general public would go to such effort except in rare circumstances.

All of the problems with cut-and-paste changes would disappear if OMB required agencies to republish entire notices when any part of a notice changes. We believe that the cost of this requirement would be minimal, perhaps a few thousand dollars a year government-wide. This one change would create substantial improvement in transparency for the public, and would increase the public's ability to respond to notices.

We applaud the provision at lines 1043-1045 which states that agencies should maintain public availability of all system notices, including this specific requirement:

For any SORNs that are comprised of multiple *Federal Register* notices, an unofficial consolidated version of the SORN that describes the current system of records and allows members of the public to view the SORN in its entirety in a single location.

We do not think this obligation addresses the point we make here about cut-and-paste notices, however, we support it, and encourage OMB to also required agencies to republish entire notices when any part of a notice changes.

IV. Government-Wide System of Records (lines 324-348)

We believe that the proposed language around the use of government-wide systems of records is especially confusing. A researcher can find all system notices adopted by an agency and still be entirely unaware that other agencies have systems that effectively include records that the agency uses. We recognize the value of the government-wide system of records, and we do not propose banning them. Instead, each agency should include in its list of systems of records a statement that there are record systems maintained by other agencies that contain records used by that agency.

We propose that there should also be a current and authoritative list of government-wide systems that each agency can copy and publish or, better still, a centralized current and authoritative list of government-wide systems to which each agency can provide a link.

OMB can maintain the list of government-wide systems itself or assign the responsibility to NARA, the Federal Privacy Council, or another organization. Ideally, the link will be permanent.

We note that some agencies publish their own lists of government-wide systems of record for the convenience of the public. See, e.g., <http://www.fhfa.gov/AboutUs/FOIAPrivacy/Documents/ListofGovernmentWideSystemofRecordsNotices.pdf>.

We appreciate these efforts, but we suggest that there is little reason for agencies to duplicate the same effort, and we suspect that many of these lists are not current. A central list could more easily be kept up-to-date.

V. Linkages Between Systems (lines 317-322)

The proposed circular directs agencies to describe any linkages between different systems of records in the “Supplementary Information” section of the relevant SORNs.

Agencies shall ensure that all SORNs clearly describe any linkages that exist between different systems of records based on the retrieval of the records. For example, if records in multiple systems are linked together through a central indexing or retrieval capability such that an employee or contractor retrieving records from one system would also thereby retrieve and gain access to records in another system, the agency shall explain this linkage in the “Supplementary Information” section of the relevant SORNs.

We support this requirement, but we suggest that it is inadequate. Those who research systems of records using the very useful Privacy Act Issuances maintained by the Federal Register

<https://www.gpo.gov/fdsys/browse/collection.action?collectionCode=PAI>) will not find there the supplementary information included in the original Federal Register publication. The absence of this information in the permanent central set of system notices maintained by the Federal Register means that in order to find the linkages, it is necessary to find each original or changed system notice published by each agency. This is no easy task, and it is a significant barrier to understanding linkages between agency systems of records.

The solution here is to require that each system notice published by the Federal Register in the Privacy Act Issuances and each system notice published by each agency include the Supplementary Information section of the system notice's original publication. This would go a long way toward improving the public's understanding of agency record-keeping practices. If agencies maintain their own independent list of agency systems, the agencies should also be obliged to include the supplementary information from the original system notice publication.

VI. Routine Uses (lines 372-422)

OMB discourages agencies from relying on so-called blanket routine uses applicable to all systems of records:

The Privacy Act requires agencies to describe each routine use of the records contained in the system of records, including the categories of users of the records and the purpose of the use. Agencies may only establish routine uses for a system by explicitly publishing the routine uses in the relevant SORN. Agencies are strongly encouraged to publish all routine uses applicable to a system of records in a single Federal Register notice for that system. However, some agencies choose to publish a separate notice of routine uses that are applicable to many systems of records at the agency, and then incorporate them by reference into the notices for specific systems to which they apply. When incorporating such routine uses by reference, agencies shall ensure that the routine use section of the SORN clearly indicates which of the separately published routine uses apply to the system of records and includes the *Federal Register* citation where they have been published.

We think that blanket routine uses are confusing to the public. Few individuals realize that other routine uses not listed in a system notice apply to that system or know where to find them. Agencies often pay little attention to their own blanket routine uses, and they either apply them when inappropriate or write conflicting/overlapping local routine uses.

Firmer action by OMB is needed here. OMB should ban the use of blanket routine uses and force agencies to specifically and knowingly adopt each routine use proposed for each system. We recognize that banning blanket routine uses immediately would create difficulties so we suggest that OMB allow a generous transition of several years for agencies to comply.

We also suggest that many of the routine uses included in agency blanket routine uses have unnecessary variation across agencies. OMB should direct the Federal Privacy Council or its own new privacy office to undertake standardization work on common routine uses.

The same effort could encourage agencies to stop adopting routine uses inappropriately, especially when agencies use routine uses where relying on the consent of the data subject is a more appropriate way to provide for disclosure. We note that the proposed circular already states (line 394):

Overly broad or ambiguous language would undermine the purpose of the routine use notice requirement and shall be avoided.

We applaud this statement, but we do not think it is sufficient to prod agencies to do better. Without some type of systemic review of existing routine uses within and among agencies, nothing will change.

VII. Privacy Act Exemption Rules (line 854-902)

The circular should expressly state that an agency proposing an exemption for a new system of records must publish the proposed rule and the new system of records notice together in the same issue of the Federal Register. A proposal for an exemption without an accompanying system notice is impossible to evaluate.

If the exemption is for a previously published system, republication of the notice need not be required, but a specific link to a previous (and complete) system notice should be mandatory. Privacy Act exemptions are important, and need heightened treatment.

VIII. Privacy Act Reviews (lines 904-959)

We applaud the requirement (at line 935) that “[a]gencies shall ensure that all SORNs remain accurate, up-to-date, and appropriately scoped.” However, we are concerned that this requirement will not make enough of an impact. We know that agency system notices often lag years behind current practice, and that the process of updating notices can take so long that the revised notices sometimes become outdated before publication. This is a perpetual problem that will not be solved easily, if ever, but certainly not with a one-line statement in the circular.

We urge a requirement that OMB should direct agencies to undertake a **comprehensive review of system notices on a defined schedule** (multiyear for agencies with large numbers of systems) and to publish both the schedule and the results of the review on a public website maintained and overseen by the Federal Privacy Council or the new OMB privacy office. External and regular oversight is necessary to make any comprehensive review a reality.

We suggest that each agency be required to conduct a complete review on a cycle that does not exceed four years. We think that strikes a fair balance between the pace of administrative and technological change on the one hand and the practical realities of conducting reviews.

IX. Date of Last System Notice (lines 440-454, and 531-599, Appendix II, SORN Template, ex.)

This comment is regarding an element that does not exist in the proposed circular language. The standard elements of a system of records notice do not include **the date of the last change of that notice or a reference and link to all previous relevant Federal Register notices**. OMB should direct the Federal Register and agencies to include this information in each system notice in the Federal Register and in the Privacy Act Issuances.

This information will greatly help those who need more information about any given system of record. If OMB had a list of all system notices more than five or ten years old, it could direct agencies to review and republish those notices most likely to be out of date or obsolete. Thus, the information would help OMB carry out its Privacy Act responsibilities and help the public at the same time.

X. Addresses (Method of public response) (lines 1224-1226)

This comment pertains to an element that was not discussed in the proposed circular, namely, publication of the method of response for Privacy Act notices by the public. **The address for public response needs to include an electronic method of submission**. This should be a required element for all Privacy Act notices. Too often SORN notices in particular do not include electronic delivery options. Because delays caused by the postal service security screening requirements, this puts an undue burden on the public and discourages comments.

In order to comment, and have those comments reach an agency on time, a commenter has to either FedEx the comments at their own expense, Fax the comments, or hand deliver the comments. For example, in a recent comment WPF submitted to the US Department of Justice in October 2016 regarding a SORN, there was no electronic method of delivery listed in the SORN. (See The Department of Justice System of Records Notice, FBI Insider Threat Program Records (ITPR),” JUSTICE/FBI-023, CPCLO Order No. 007-2016. The notice appears at 81 Federal Register 64198 (September 19, 2016), <https://www.federalregister.gov/d/2016-22410>. WPF’s comments, which include an objection to the lack of electronic notice, are here: http://www.worldprivacyforum.org/wp-content/uploads/2016/10/WPF_comments_DOJ_InsiderSORN_10_fs.pdf. In September 2016, we had a similar experience with a SORN from the US Postal Service, see Informed Delivery Notification Service, 81 Federal Register 58542. For the DOJ comments, we had to pay for a fax, as we no longer maintain one in-house. For the US Postal Service, we had to pay to FedEx the comments.

We think there is no justification for the exclusion of electronic means of submitting comments on Privacy Act notices. Providing an address for electronic delivery for all Privacy Act notices will encourage the public to respond, will allow for timely responses, and will enable better tracking of incoming comments for the record.

Thank you for the opportunity to comment. Please do not hesitate to contact us with any questions.

Respectfully submitted,

A handwritten signature in cursive script that reads "Pam Dixon".

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org