Comments of the World Privacy Forum to OMB
Regarding OMB Circular A-130, Managing Information as a Strategic Resource

Sent via email to: a130@omb.eop.gov

OMB Office of the Federal Chief Information Officer
The Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Nov. 16, 2015

We welcome the opportunity to comment on OMB's redraft of Circular A-130, which establishes policies for the management of federal information resources. The issues and functions governed by A-130 have only grown in importance since the last revision. We applaud OMB's initiative in revising and modernizing the Circular.

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.

We use the line numbers in the draft to identify the provisions addressed by our comments. We are pleased to support some provisions, and we urge changes in some provisions. In one instance, we are requesting a change because the proposed language does not comply with the requirements of 44 U.S.C. § 3506(d).

I. Agency Information Strategy (Lines 270-309)

The draft Circular requires each agency to develop and maintain an Agency Information Strategy describing the agency's technology and information resources goals. We support this requirement.

We suggest, however, that the Circular explicitly directs agencies to make the Information Strategy document publicly and readily available. We recognize that there may be a need for confidentiality in the case of activities properly classified pursuant to Executive Order in the interest of national security or foreign policy.

We also think that it would be appropriate for the CIO Council to maintain a central webpage with a link to the Information Strategy for each agency so that the public can find all the documents through a single website.

In addition, we suggest that the Circular (lines 288-293) expressly direct each agency to make public on its website the required "inventory of the agency's major information systems, holdings, and dissemination products; a description of the agency's major information and record locator systems; [and] an inventory of the agency's other information resources."

We do not think that it is enough for an agency to maintain an online resource for persons to obtain public information from the agency, although we support that resource (lines 292-293). To the greatest extent practicable, each agency should maintain *all* available public information on the agency's website so that public requests for agency public information resources will be minimized.

II. Conditions on Use (Lines 573 and 572-574)

One of the privacy safeguards specified in the draft (lines 572-574) obliges each agency to "[l]imit the disclosure of personally identifiable information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists." We support this requirement, but we think that it needs some adjustment.

The Privacy Act of 1974 authorizes each federal agency to share information under appropriate circumstances (most notably via routine uses) with other agencies and, at times, with third parties. The Privacy Act does not expressly authorize an agency to impose conditions on the recipient so that shared information remains confidential and so that the recipient only uses the information appropriately.

This failure of the Act is a significant shortcoming in several ways.

- First, personal information shared may lose the privacy protections that it had in the hands of the originating agency.

- Second, when an agency shares personal information with a second federal agency, the second agency may maintain that personal information in its own system of records that has a different and potentially broader set of routine uses.

- Third, if a federal agency shares information with a state agency or a private party (e.g., a credit bureau), the information passes beyond the reach of the Privacy Act of 1974, and remedies for individuals may no longer exist.

We note these consequences of sharing, while recognizing that some are inevitable. It is rare in American privacy statutes for privacy control to attach to information and apply to downstream users. The Substance Abuse rules (42 C.F.R. Part 2) and, perhaps, the Internal Revenue Code are the only examples we can think of offhand.

Nevertheless, there are ways to impose limits on downstream recipients of PII. The HIPAA health privacy rule imposes limits on business associates and subcontractors of covered entities, although the rule now covers these downstream users directly rather than through contracts as it did previously. Contracts, data use agreements, and memoranda of understanding all provide ways to impose limits when an agency shares personal information with others.

We think that the draft Circular should be more express here.

- First, use of the information is not the only concern. The Circular should say "impose appropriate conditions on use**, disclosure, and other processing**."

- Second, given the lack of downstream controls in the Privacy Act of 1974, OMB should expressly tell agencies that the use of contracts, data use agreements, MOUs, and similar instruments is authorized and recommended in appropriate circumstances.

We do not believe that the Circular needs more detail than that, but the Circular should push agencies to do more and provide general suggestions for how to do it. Thus, the Circular might say "**impose appropriate conditions on use, disclosure, and other processing through contracts, data use agreements, and memoranda of understanding.**

III. Restrictions on reuse of federal information (Lines 682-683)

This provision of the Circular implements 44 U.S.C. § 3506(d), which provides:

> With respect to information dissemination, each agency shall—
> (1) ensure that the public has timely and equitable access to the agency's public information, including ensuring such access through—
> (A) encouraging a diversity of public and private sources for information based on government public information;
> (B) in cases in which the agency provides public information maintained in electronic format, providing timely and equitable access to the underlying data (in whole or in part); and

(C) agency dissemination of public information in an efficient, effective, and economical manner;

(2) regularly solicit and consider public input on the agency's information dissemination activities;

(3) provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and

(4) not, except where specifically authorized by statute—

(A) establish an exclusive, restricted, or other distribution arrangement that interferes with timely and equitable availability of public information to the public;

(B) restrict or regulate the use, resale, or redissemination of public information by the public;

(C) charge fees or royalties for resale or redissemination of public information; or

(D) establish user fees for public information that exceed the cost of dissemination.

The draft Circular does not reflect the restriction in (4)(B), (C), & (D). That provision *expressly bans* agencies from charging fees or restricting reuse, resale, redissemination, unless specifically authorized by statute. The draft only directs agency to "avoid establishing unnecessary restrictions." **The draft must fully reflect the limitations imposed by 44 U.S.C. 3506(d).** Neither OMB nor any agency has the authority to waive or reduce the express statutory limitation.

IV. Personally Identifiable Information (Lines 1054-1056)

The draft includes this definition of PII:

> Personally identifiable information' (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Generally, PII includes information about an individual's identity, but it is not limited to identity information. The draft's focus on identity information is necessary but not sufficient. We think that a broader definition is appropriate and necessary. NIST offered this definition:

> PII is ―any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. *Guide to Protecting the Confidentiality of Personally Identifiable Information* at 2-1, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

The NIST definition covers the notion of PII in a broader way. We think that OMB knows better than to use the definition it has proposed in the draft Circular. Another NIST publication discusses other definitions of PII in existing OMB documents:

> OMB Memorandum 07-16 defines PII as information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Memorandum 10-22 further states that "the definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements. *Security and Privacy Controls for Federal Information Systems and Organizations* at note 119, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

There is no universal definition of PII, and the exact words may not matter a great deal. However, we see no reason to proliferate definitions unnecessarily among OMB documents. We feel strongly that the definition should reference both identity information and the other categories of information such as such as name, social security number, date and place of birth, mother's maiden name, and biometric records.

We recommend that the Circular use the NIST definition or one of the definitions from an existing OMB document.

V. Fair Information Practices (Lines 1200-1242)

The World Privacy Forum strongly supports basing privacy laws and policies on Fair Information Practices, and we are encouraged to see that OMB wants to incorporate FIPs into Circular A-130. However, we have a few problems with the proposed language.

First, the proposed version of what OMB calls FIPPs differs from each of the multiple statements of FIPPs published by federal agencies. The different versions are collected in Robert Gellman, *FAIR INFORMATION PRACTICES: A Brief History*, http://bobgellman.com/rg-docs/rg-FIPshistory.pdf. The proliferation of FIPs versions in one of the few countries where there is no general privacy law implementing FIPs is unnecessary and confusing.

Second, we see no reason for federal agencies to regularly reinvent FIPs and produce yet another version with changes from previous versions that are unexplained and unjustified. Essentially, almost everyone who touches FIPs seems to engage in pointless wordsmithing. This seems to be the case for the draft Circular.

Third, we much prefer the classic version of FIPs used as the basis for most privacy laws around the world, namely the 1980 version from the Organization for Economic Cooperation and Development at

http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

If OMB does not want to rely on this version, then we suggest that it use one of the other federal versions already extant. We are not prepared to endorse for all purposes the Department of Homeland Security version (at http://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf), but it is a better restatement than the one in the draft Circular.

Fourth, we will not go through OMB's the restatement of FIPPs word-for word, but we particularly object to the language on Individual Participation at lines 1229-1232:

> *Individual Participation*. Agencies should involve the individual in the decision-making process regarding the collection, creation, use, dissemination, and maintenance of PII and, to the extent practicable, seek individual consent for these activities. Agencies should also establish procedures to receive and address individuals' privacy-related complaints.

Generally, in statements of FIPs, *individual participation* refers to a data subject's access and correction rights. The OMB version covers those rights elsewhere. Here, however, OMB seems to think that each individual should be involved in each agency's decision-making process regarding the collection, creation, use, dissemination, and maintenance of PII. This is completely unrealistic, both for agencies and for individuals. Agencies do not have the resources to engage in these discussions with individuals, and most individuals have neither the knowledge nor time to participate to the extent that the *individual participation* principle suggests.

Rather than engage each individual in these decisions, it would be appropriate for agencies to engage the *public*, although we see no reason to include that obligation in a statement of FIPs. Public consultation is a core principle of administrative law, and many statutes mandate obtaining public comments.

Further, the provision says that agencies should seek individual consent for all these activities to the extent practicable. That's a lovely thought, but it probably unrealistic. We observe that federal agencies generally bend over backwards to *avoid* seeking individual consent in the one part of the Privacy Act of 1974 where consent is contemplated by the Act. The Act envisions that agencies should seek individual consent for some disclosures. However, it is common for agencies to write routine uses that allow disclosures without consent because agencies do not want to be bothered obtaining consents and dealing with the administrative consequences thereof. While we do not necessarily agree with those choices, we recognize the limitations of seeking consent frequently. OMB should too.

Finally, with respect to the last sentence regarding complaints, we suggest that this language belongs in the accountability section.

VI. SAOP Responsibilities in the Risk Management Framework for Federal Information Systems (Line 1262)

In the table describing responsibilities for the Senior Agency Official for Privacy (SAOP), the draft Circular mentions in several places the notion of a "privacy continuous monitoring strategy." The draft Circular refers elsewhere to continuous monitoring of privacy as well as security. We see substantial value in the language around continuous security monitoring, as there is an established body of research and work in this area.

In the area of privacy, however, there is less research around implementing the idea of "continuous monitoring." It makes implementing this concept more challenging. In practice, experience from forty years of operating under the Privacy Act of 1974 suggests that a continuous monitoring strategy has little chance of success if it is left as simply a broad statement. We recommend that this idea be fleshed out with some practicalities.

We suggest this because history shows that agency compliance with the most basic requirements of the Privacy Act – defining systems of records and maintaining – has been woefully and consistently inadequate. Many existing Systems of Records Notices (SORNs) are out-of-date in significant ways because agencies review SORNs only fitfully. We know of cases where a decade or more passes before some agencies undertake a review and republication of their SORNs. Frankly, OMB tolerates this inattention to the Privacy Act of 1974 by devoting few resources to prodding agencies to do better.

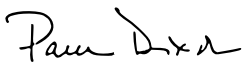
The continuous monitoring directive in its privacy application is much more likely to be meaningful if specifics and a timetable are involved. We would be happy to trade the broad notion of continuous monitoring for a firm, well-understood requirement that agencies review their SORNs every two years and that they conduct a review of general privacy obligations and requirements at the same time. We would also be interested in such things as real-time access monitoring with audit trails, and a set requirement for reviewing such access, where this is appropriate and feasible.

Perhaps the most constructive place to focus is on new activities and on regular, consistent review of privacy on a fixed timetable thereafter. We welcome the focus in the Circular on paying attention to privacy for new systems. For example, the language in lines 2042-2062 that seeks to "ensure that privacy risks are addressed prior to system authorization" is forward-looking and helpful. We support this language. This language envisions a process that will identify the risks and resolve any conflicts and disagreements before final determination. The best time to include privacy considerations is at the start of any information activity, when changes are under consideration, and on a fixed schedule thereafter.

Continuous monitoring will likely not work unless the idea is reigned in to a more practical set of applications. This could be technical, procedural, or otherwise. We encourage OMB to give more specificity and direction regarding this concept. We understand that becoming too technology-specific is problematic, but with less privacy implementations in this area on the books, it would be helpful to agencies to have more flesh on the bones for this concept.

Thank you for your consideration of our comments. We would be happy to answer any questions you might have.

Respectfully submitted,



Pam Dixon
Executive Director,
World Privacy Forum
+1 760-713-4281
www.worldprivacyforum.org