Comments of the World Privacy Forum
to
the Office of Management and Budget regarding Request for Information regarding Executive Branch Agency Handling of Commercially Available Information Containing Personally Identifiable Information

Submitted via regulations.gov

Keven Herms
Office of Management and Budget
1600 Pennsylvania Ave NW
Washington DC 20500

16 December 2024

The World Privacy Forum welcomes the opportunity to comment on the Office of Management and Budget's *Request for Information on Executive Branch Agency Handling of Commercially Available Information Containing Personally Identifiable Information*. The notice appeared in the Federal Register on October 16, 2024, 89 Fed. Reg. 83517, 89 FR 83517 https://www.federalregister.gov/documents/2024/10/16/2024-23773/request-for-information-executive-branch-agency-handling-of-commercially-available-information. This RFI is part of OMB's implementation of Executive Order 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* [1] pursuant to OMB's statutory authorities to set policies for Executive Branch agencies' management of information resources, including CAI containing PII. In our preparation of these comments, we also took into consideration the *Intelligence Community Policy Framework for Commercially Available Information*, published in May 2024.[2]

The World Privacy Forum is a non-partisan 501(c)(3) public interest research group focused on conducting research, analysis, and education in the area of privacy and complex data ecosystems and their governance, including in the areas of identity, AI, health, and others. WPF works extensively on privacy and data governance across multiple jurisdictions, including the U.S. For more than 20 years WPF has written in-depth, influential research regarding systemic data issues. This work includes early

[1] Exec. Order 14110, 88 FR 75191, Nov. 1, 2023.

[2] *Intelligence Community Policy Framework for Commercially Available Information*, ODNI. May 2024. https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf .

groundbreaking work regarding data brokers and commercially available information and broader datasets which includes reports, consumer-facing resources, and Congressional testimony. *The Scoring of America*, an early and influential report on machine learning and consumer scores, included deeply researched background on databroker activities. Most recently, WPF participated in the OMB 2023 Data Broker Roundtable,[3] and contributed to recent proposals regarding data brokers from CFPB. In other work, WPF co-chairs the UN Statistics Data Governance and Legal Frameworks working group, and is co-chair of the WHO Research, Academia, and Technical Constituency. WPF researchers participate in the OECD.AI AI Expert Groups, and is also a member of the U.S. NIST AI Safety Institute Coalition (AISIC), among other activities. WPF research on complex data ecosystems governance has been presented at the National Academies of Science, the Mongolian Academies of Science, and the Royal Academies of Science. See our reports and other data at World Privacy Forum: https://www.worldprivacyforum.org.

In general, we believe that there is more than enough information on the public record – and otherwise available to OMB – to support the case that private sector data is a major resource used by federal agencies and worthy of more oversight. We note that OMB has led recent work into data brokers and their practices, and has been involved in analyzing the risks these practices involve. For these reasons, WPF is refraining from a lengthy recital of data broker harms, which we believe to be well-documented at this point. We incorporate several key resources articulating these harms by reference.[4]

We further believe that there is currently insufficient disclosure about the use of private sector personal information resources, and that agencies use those resources to make significant decisions about individuals, and that there is a general lack of due process with respect to those decisions. Further, we have seen over the years of our work that the quality of commercially available information is highly variable, which has resulted and can result in substandard decisions and unfairness to individuals. The use of Artificial Intelligence (AI) processes has exacerbated many of the problems already present, and has added additional challenges.

We note that the assignment at hand is to address OMB's specific queries regarding the implementation of section 9(a)(i) and (ii) of Executive Order 14110 which instructs OMB to "…evaluate and take steps to identify CAI procured by agencies, particularly CAI that contains PII" and to "evaluate . . . agency standards and procedures associated with the [handling] of CAI that contains [PII]." For this reason, in these comments, we have focused on several key queries and offer suggestions for practical, implementable solutions to some of the specific challenges that OMB has posed in its RFI. We also address issues that extend beyond PII in our discussion of AI and CAI.

---

[3] *Readout of White House Roundtable on Protecting Americans from Harmful Data Broker Practices*, White House (Aug. 16, 2023), https://www.whitehouse.gov/ briefing-room/ statements-releases/ 2023/ 08/ 16/ readout-of-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/ .

[4] *Readout of White House Roundtable on Protecting Americans from Harmful Data Broker Practices*, White House (Aug. 16, 2023), https://www.whitehouse.gov/ briefing-room/ statements-releases/ 2023/ 08/ 16/ readout-of-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/ . , Consumer Financial Protection Bureau, NPRM, Protecting Americans from Harmful Data Broker Practices (Regulation V), https://www.consumerfinance.gov/rules-policy/rules-under-development/protecting-americans-from-harmful-data-broker-practices-regulation-v/ , Federal Trade Commission, Data Brokers: A Call For Transparency and Accountability https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 , Pam Dixon and Robert Gellman, *The Scoring of America*, World Privacy Forum, April 2014. https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/ .

I. Artificial Intelligence: How does AI potentially exacerbate privacy risks associated with agency handling of CAI containing PII?

The use of Artificial Intelligence (AI) and machine learning, hereafter referred to simply as "AI," is a highly complex field of knowledge and practice. Here, we refer you to two broad areas of challenges.

A. Issues regarding how privacy changes in the AI environment including complex issues related to non-personal data and privacy

An important foundational issue in this topic area is that privacy changes in an AI environment, and it changes in several fundamental ways.[5] First, Fair Information Practices becomes too narrow to address the full range of privacy and data governance and other issues that AI brings with it. To take one example — bias, including bias stemming from historic data that is accurate but discriminatory, or bias stemming from an algorithm that has lost appropriate fit for its intended purpose, or bias arising from systemic use of data that is outright inaccurate …. these are but a few of the many bias-related issues that can crop up related to CAI and PII. These issues are broader than FIPs.

OMB's Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (March 28, 2024)[6] implementing Executive Order 14110 on AI, recognized these broader issues such as bias appropriately, and in our analysis, addressed them in appropriate and forward-looking, practical administrative and procedural proposals. We urge OMB to utilize the approaches it has already articulated in its existing AI guidance to address CAI issues as they interact with AI systems. For example, requiring vendors to produce robust and detailed AI Impact Assessments, as a start, is an important recommendation, as is the inclusion of analysis of safety and rights impacts of CAI ***either containing PII or applicable to individuals.***

Our specific recommendations in this category of AI intersecting with CAI include:

Better PIAs: Formal impact assessments can be useful to address many different policy concerns. Everyone seems aware of the overlaps between some AI assessments and some privacy assessments. In a WPF report, Robert Gellman proposed revising the Privacy Act of 1974 in very specific ways regarding the existing privacy impact assessment requirement. We will not repeat all of the details here. We refer you to pages 115-123 of the report.[7]
We summarize here, however, by noting that the report emphasized the need for an ongoing PIA process and just not a flat, one-time, one-size-fits-all assessment. This need will be just

---

[5] We incorporate by reference in this discussion the OMB M-24-10, in particular the sections discussing rights impacting AI and safety impacting AI, and the mitigations that OMB considered appropriate to the known or potential harms of AI. We supplement this with the data and recommendations in the report the *Scoring of America.*This report investigated and benchmarked the intersection of public data, CAI, and AI and privacy, and was the first major report that looked at this specific intersection. The report was published in 2014. While it has definitely aged, the principles of fairness and the various problems we identified and many recommendations remain the same. OMB M-24-10 updates the remedies we considered in our early report.

[6] Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence,* OMB, March 28, 2024. https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf .

[7] Robert Gellman, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974,* May 2021. https://www.worldprivacyforum.org/2021/05/from-the-filing-cabinet-to-the-cloud-updating-the-privacy-act-of-1974/ .

as true for an AI assessment as it is for a privacy assessment.

We state expressly that:

- Some AI and CAI assessments will require more attention, more consultation, and a long time than others;
- Some AI and CAI assessments will require regular reviews over time because consequences are not static and because agency programs change over time; and
- Some AI and CAI assessments will require lesser efforts because the risks are smaller.
- Responsible agency personnel should be allowed to make determinations about which activities need more assessment than others. OMB may be able to propose standards for making these distinctions.

We specifically recommend that:

A. OMB expand existing requirements to describe CAI as a new category of sources of information in a Privacy Act system of records.

B. Each PIA expressly state if any PII processing activity covered by the PIA involves (or does not involve) the use of CAI, whether the use of AI is accomplished directly by the agency or indirectly by agency contractors or data vendors;

C. Each PII processing activity covered by an existing PIA be revised before the agency adds any new use of CAI to the activity, whether the use of AI is accomplished directly by the agency or indirectly by agency contractors or data vendors;

D. Each system of records notice should state whether the notice covers (or does not cover) any processing of PII that involves the use of CAI; and that if any processing that involves AI that is added to an activity covered by a SORN is added to the SORN in the usual fashion so that the public will have notice and the opportunity to comment.

Transparency is another issue to consider in the analysis of AI and CAI administrative and procedural controls. While the Privacy Act considers transparency to be tied to PII and SORNs and Routine Uses (RU),[8] transparency in AI can be elusive under these tools, and a SORN or RU will likely be deficient as a full standard for creating necessary transparency. This happens due to certain properties and actions of AI systems.

This gets into one of the issues at the core of the problem that OMB will need to address: which is that while the Executive Order that the OMB is implementing discusses **PII** specifically, some of the very significant privacy problems and transparency problems and bias problems in AI systems comes from data that is considered by modern privacy-focused legal definitions to be ***non-personal data***. And non-personal data is not directly covered in the Executive Order. By strict definition, many problems inherent in AI and CAI will likely not be directly covered by OMB's implementation due to this problem. We discuss certain aspects of this problem in the next section.

---

[8] Robert Gellman, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974,* May 2021. https://www.worldprivacyforum.org/2021/05/from-the-filing-cabinet-to-the-cloud-updating-the-privacy-act-of-1974/ .

B. Specific Examples of Issues Related to Deidentification, CAI, and AI, and PII

A significant challenge regarding implementing CAI only in the context of PII is this: when PII is deidentified, it becomes *non-personal data*. It therefore escapes much regulatory guidance, and even legal controls. There are many examples of how this can impact people. To use an example from the U.S. government, in 2015, the National Institutes of Health (NIH) launched a precision medicine initiative that sought to collect 1 million biospecimens for study.[9] [10] The NIH consulted with U.S. tribal stakeholders for its biobank project, and it wrote a report about this engagement in 2023. [11] [12]NIH found that existing privacy protections that depend on deidentification do not always apply across all contexts.

Specifically, genetic identification of groups of people is possible within deidentified datasets, depending on context. In the NIH study, the NIH admits that there is a risk of identifiability of individual specimens back to a particular tribal group, and NIH acknowledges that existing Common Rule protections do not address this risk. This is acknowledged in the statement: "The program acknowledges that it is requesting broad consent from participants according to the conceptual interpretation, rather than the specific regulatory provision in the 2018 Common Rule." [13] Broad consent as defined here is a particularly challenging policy issue that poses difficult risks in the context of AI.

We already know that the right to privacy is going to very challenging to effectuate in an environment that is saturated with AI processing of biobank data samples. But the challenges extend well beyond this example. To put the problem very simply: deidentified data in large data samples of CAI can be utilized to determine group membership and meaningful details of some individuals. A variation of this deidentification problem in AI is that fully deidentified data may still be applied to an individual in a biased or discriminatory way, and the end results of this kind of analysis may vary significantly depending on data accuracy, quality, fit, and additional considerations.

For example, CAI can be based on hundreds to millions of data points about people and groups of people and patterns and neighborhoods, among other data. For example, a data vendor who supplies the U.S. government with for example some type of a fraud risk score applicable to individuals may have been utilizing a compound AI system composed of so much data, so many algorithms, and so many baked in scores, so as to render transparency entirely unavailable. It would be truly impossible in a SORN or RU to fully articulate if the data in this case supported a fraud score that was accurate, what PII was initially used prior to aggregation, and many other questions about the data and the analysis.

---

[9] *All of Us Research Program,* National Institutes of Health. https://allofus.nih.gov/about/faq.

[10] Robert Gellman and Pam Dixon, *Privacy, the Precision Medicine Initiative, & the All of Us Research Program: Will Any Legal Protections Apply?* World Privacy Forum, March 16, 2017. https://www.worldprivacyforum.org/2017/03/report-privacy-the-precision-medicine-initiative-and-all-of-us-research-program-will-any-legal-protections-apply/ .

[11] *All of Us Tribal Engagement*, NIH. https://allofus.nih.gov/about/diversity-and-inclusion/tribal-engagement. See also more recent consultations: https://allofus.nih.gov/news-events/announcements/all-us-research-program-host-information-sessions-tribal-communities .

[12] *All of Us Research Program Tribal Consultation Final Report March 2021*, National Institutes of Health. March 2021.https://allofus.nih.gov/all-us -research-program-tribal-consultation-final-report .

[13] *All of Us Research Program Tribal Consultation Final Report March 2021*, National Institutes of Health. March 2021.https://allofus.nih.gov/all-us -research-program-tribal-consultation-final-report .

To solve for the deidentification problems in CAI, OMB could support the creation of Voluntary Consensus Standards as a way to set appropriate guardrails in place regarding various risk points in the AI lifecycle. See the discussion in II, Marketplace Standards, in this document. Although our primary discussion of VCS is regarding CAI that contains PII, the issues regarding CAI that has utilized AI systems to deidentify and compound data that was originally PII could also be addressed, in part, through standards for transparency and / or accuracy requirements, among other requirements. We urge OMB to consider this issue and how it might be resolved through a standards approach.

II. Marketplace Standards: Using Voluntary Consensus Standards as a key way to address privacy risks, create transparency, and create processes consistent across agencies

We would like to suggest a general approach to developing standards for commercially available information (CAI) containing personal data or personally identifiable data (PII) that does not require new legislation or regulation to be effective. The federal government is a major purchaser of commercial databases and data compilations. So are state and local governments. "Data compilations" in today's world means that CAI may take the form of database subscriptions and APIs with substantive data feeds.

We note that many purchasers of CAI do not always insist that the data they are procuring can be proven to be **accurate**, **timely**, or **complete** to a **particular standard**. Agencies that rely on third party data largely have a sufficient defense on those rare occasions when consumers are able to raise meaningful challenges. Otherwise, buyers — government and commercial — can say that "close enough" is sufficient.

The marketplace power of the federal government – whether or not combined with state and local governments – is enormous. The commercial sales of private sector data have long been supported by the US government.[14] Because of this economic power, Federal, state, and local governments together can demand that commercial database vendors must meet specified standards for accuracy, currency, quality, due process, and otherwise. Faced with the loss of all or most government business, vendors would be under enormous financial pressure to comply.

A. Creating new applicable standards

OMB should enlist the cooperation of state and local governments that are interested in having better quality data for their decision making. We do not know of a firm standard for CAI accuracy, or other specific quality measures that would be applicable today across the U.S. government. This is something that can and should be remedied.

We suggest that OMB should convene -- or invite another agency or group of agencies to convene-- consumer representatives, other public sector purchasers of commercial databases, and the vendors themselves to develop standards for consumer data sold commercially. We suggest that this take place

---

[14] Robert Gellman and Pam Dixon, *Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens*,World Privacy Forum October 2013. https://www.worldprivacyforum.org/2013/10/report-data-brokers-and-the-federal-government-a-new-front-in-the-battle-for-privacy-opens/ See also, for example, Politico regarding a 2021 contract: https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600 . See also bipartisan House Energy and Commerce investigation into data brokers: https://democrats-energycommerce.house.gov/newsroom/press-releases/ec-leaders-continue-bipartisan-investigation-into-data-brokers-potential .

under the auspices and rules of OMB Circular No. A-119, Voluntary Consensus Standards.[15] Use of the voluntary consensus standards process would ensure that openness, balance of interest, due process, and appeals process, and consensus (as defined in the Circular) would be present. We recognize the RFI we are responding to pertains to Executive Agencies. The standard could be developed by Executive Agencies, or potentially a larger array of agency stakeholders, including the FTC and the CFPB. This would require interagency agreement and discussion.

B. More about Voluntary Consensus Standards

Voluntary consensus standards are a well-defined term of art, and law. A voluntary consensus standard or VCS is one that is developed or adopted by Standards Developing Organizations (SDOs) according to consensus principles as defined in the OMB Circular A-119. Consensus standards contribute to regulatory quality because consensus-based SDOs must demonstrate adherence to the tenets of transparency, openness to participation by interested stakeholders, balance of representation, and due process, among other principles.[16]

In the United States, there are two critical definitional groundings for VCS:

1. The OMB Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities,[17] (The National Technology Transfer and Advancement Act (NTTAA) codifies OMB Circular A-119.)

2. The ANSI Essential Requirements: Due Process requirements for American National Standards.

In 1996, the National Technology Transfer and Advancement Act (NTTAA) (Pub. L. No. 104-113), codified OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.[18] The NTTAA and OMB Circular A-119 established that Federal government agencies were to use voluntary consensus standards in lieu of government-unique standards except where voluntary consensus standards are inconsistent with law or otherwise impractical.[19] The ANSI Essential Requirements set forth in detail the definitions and processes that comprise a "due process" standards setting body, and procedures.

---

[15] OMB Circular A-119, *Federal Participation in the Development and Use of voluntary Consensus Standards and in Conformity Assessment Activities*, 2016 Revision, 81 FR 4673 pages 4673-4674. Available at: https://www.federalregister.gov/documents/2016/01/27/2016-01606/revision-of-omb-circular-no-a-119-federal-participation-in-the-development-and-use-of-voluntary.

[16] *ANSI Essential Requirements: Due process requirements for American National Standards*, ANSI. https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures%2C%20Guides%2C%20and%20Forms/ANSI-Essential-Requirements-2018.pdf. *See also*: U.S. Food and Drug Administration, Standards and Conformity Assessment Program, Available at: https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/standards-and-conformity-assessment-program-medical-devices#intro.

[17] National Technology Transfer and Advancement Act (NTTAA) (Pub. L. No. 104-113).

[18] OMB Circular A-119, *Federal Participation in the Development and Use of voluntary Consensus Standards and in Conformity Assessment Activities*, 2016 Revision, 81 FR 4673 pages 4673-4674. Available at: https://www.nist.gov/sites/default/files/revised_circular_a-119_as_of_01-22-2016.pdf.

[19] ANSI essential requirements can also fully apply to standards governing, for example, the FBI, CIA, and NSA in areas such as the voluntary sharing of information by businesses with law enforcement.

The most current definition of a standards body that creates voluntary consensus guidelines is as follows, as found in the 2016 revision of OMB Circular A-119:

"Voluntary consensus standards body" is a type of association, organization, or technical society that plans, develops, establishes, or coordinates voluntary consensus standards using a voluntary consensus standards development process that includes the following attributes or elements:

i. Openness: The procedures or processes used are open to interested parties. Such parties are provided meaningful opportunities to participate in standards development on a non-discriminatory basis. The procedures or processes for participating in standards development and for developing the standard are transparent.
ii. Balance: The standards development process should be balanced. Specifically, there should be meaningful involvement from a broad range of parties, with no single interest dominating the decision-making.
iii. Due process: Due process shall include documented and publicly available policies and procedures, adequate notice of meetings and standards development, sufficient time to review drafts and prepare views and objections, access to views and objections of other participants, and a fair and impartial process for resolving conflicting views.
iv. Appeals process: An appeals process shall be available for the impartial handling of procedural appeals.
v. Consensus: Consensus is defined as general agreement, but not necessarily unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes.

The idea of Federal agencies providing a safe harbor for business in the privacy sphere has continued to arise; but all Federal agencies must comply with the rules enshrined in the OMB Circular. Circular A-119 applies to all US Federal "agencies and agency representatives who use standards or conformity assessment and/or participate in the development of standards." "Agency" means any executive department, independent commission, board, bureau, office, government-owned or controlled corporation, or other establishment of the Federal government. It also includes any regulatory commission or board, except for independent regulatory commissions insofar as they are subject to separate statutory requirements regarding the use of voluntary consensus standards. It does not include the Legislative or Judicial branches of the Federal government. [20]

The OMB Circular states that all Federal agencies must use voluntary consensus standards (in lieu of government-unique standards) in procurement and regulatory activities, except "where inconsistent with law or otherwise impractical." Again, legislative and judicial branches of the federal government are not subject to OMB Circular A-119. However, the Circular does apply to all federal agencies, including law enforcement, national security, and other regulatory agencies such as the FBI, CIA, and NSA, HHS, the FTC, the FDA, and others. What is remarkable is not that such standards exist, but that in many if not most multistakeholder and legislative discussions around privacy, it has not been well-understood that they exist.

The term "voluntary consensus standards," as already discussed, has a specific meaning that is already defined in law. VCS activities are already in practical use and have been for decades. The U.S. Food and Drug Administration for example has been using voluntary consensus standards that comply with due

[20] ANSI essential requirements can also fully apply to standards governing, for example, the FBI, CIA, and NSA in areas such as the voluntary sharing of information by businesses with law enforcement.

process requirements as articulated in the Office of Management and Budget (OMB) Circular A-119 for more than 20 years, which has resulted in more than 1,000 recognized standards applicable to medical devices.[21]

As part of this proposed solution, we further suggest that should standards be developed, that an independent organization funded by the CAI vendors oversee compliance and consider consumer complaints. We repeat that this all can be accomplished without new laws or regulations. Buyers – such as the Federal government -- can demand demonstrable compliance with a new set of VCS standards. There are plenty of commercial and technical standards of all sorts that succeed with this type of approach. We have already mentioned the FDA VCS standards. There are additional ones, such as the numerous VCS that the Environmental Protection Agency participates in,[22] among other standards at other agencies.[23]

Within the framework of due process guarantees set out in OMB Circular A-119, federal regulators today already have the power to recognize compliance with voluntary consensus standards as evidence of compliance with the law for specific, limited regulatory purposes. Federal regulators may only use voluntary consensus standards to create such safe harbors if the standards can be shown to have been developed through processes whose openness, balance, consensus, inclusion, transparency and accountability have been independently verified.

When the interface between federal legislation and voluntary consensus standards is working correctly, then the private sector (inclusive of all relevant stakeholders) takes the lead in developing appropriate, context-specific standards for solving policy problems. Next, regulators take the lead in assessing whether those standards meet the openness and other requirements of the standard, and meet the needs of the American public.

III. Enhancing Existing Agency Obligations

Federal agencies have obligations under various laws and constitutional requirements to meet reasonable requirements when using CAI containing PII to make decisions about individuals. In particular, the Privacy Act of 1974 imposes a series of due process requirements for agency activities involving personal information. We suggest some ways to enhance those requirements.

Because OMB has the responsibility to oversee and guide implementation of the Privacy Act of 1974 by federal agencies, OMB can use existing authority to require agencies to do better when using CAI containing PII. In this section, we limit our discussion to CAI specifically containing PII. (We again note per our previous discussion that AI processes introduce meaningful challenges for very large tranches of data that do not technically contain PII as defined in the relevant Executive Order.)

Here are some examples of proposed guidance for data containing PII:

---

[21] *U.S. Food and Drug Administration Recognized Consensus Standards*, U.S. Food and Drug Administration. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.

[22] *EPA Participation in VCS and Other Private Sector Standards,* US Environmental Protection Agency https://www.epa.gov/vcs/epa-participation-vcs-and-other-private-sector-standards . From this page: "As of January 2024, over 150 EPA staff are participating in the development of VCS and other private sector standards…" (Retrieved December 2024).

[23] See *Use of Standards by U.S. Federal Agencies,* National Institute of Standards, https://www.nist.gov/standardsgov/use-standards-us-federal-agencies.

A. Better disclosure

OMB should require all agencies to disclose in Privacy Act system of records notices how each system obtains CAI containing PII and how the system uses the information to affect individuals. The disclosure requirement should insist on detailed disclosure of the specific fields of data obtained and precisely how the agency uses the information. No general description of a source should be allowed. For example, it should not be sufficient to identify a "consumer reporting agency report" as a source, or, "third party dataset of mobile user data." Specificity will go a long way toward creating much-needed transparency.

B. Internal sharing

Under the Privacy Act of 1974, information maintained in a system of records can be shared with others in the agency *who have a need for the record in the performance of their duties*. This broad and general standard includes no procedures or oversight. We suggest that OMB require each agency that routinely shares CAI containing PII to:

1. publicly disclose the sharing in a system of records notice; and

2. require that the sharing be reviewed and approved on a regular basis by the agency Privacy Act Officer.

3. In instances where the CAI may be highly opaque or aggregated, there should be a mechanism within an AI Impact Assessment and oversight from an Agency AI Officer to determine if the CAI meets AI trustworthiness standards and goals. [24]

C. Routine uses

All routine uses that involve the disclosure of CAI containing PII should expressly state that the disclosure in question includes CAI containing PII and should describe specifically what the agency discloses.

D. Due Process

Whenever an agency makes a decision about an individual that involves the use of CAI containing PII, the agency should be required to record that it used the information, exactly what information it used, and the name of the vendor that provided the information. This information should be available to individuals requesting their records under the Privacy Act of 1974.

IV. Conclusion

WPF thanks the OMB for its thoughtful RFI and its efforts regarding CAI and PII. We believe that there are meaningful possibilities of addressing some of the challenges. Regarding CAI and AI, we believe those challenges are more difficult to solve due in part to definitional issues around privacy and non-

---

[24] We note that AI governance tools are often used to make these determinations of fairness, bias, transparency, and so forth in complex AI Systems. In 2023, WPF published an extensive analysis and Index of such tools in its report, Kate Kaye and Pam Dixon, *Risky Analysis: Assessing and Improving AI Governance Tools An international review of AI Governance Tools and suggestions for pathways forward ,* World Privacy Forum, 15 December 2023. https://www.worldprivacyforum.org/2023/12/new-report-risky-analysis-assessing-and-improving-ai-governance-tools/ .

personal data. These definitional challenges exist even within the Executive Order. We encourage OMB to consider the risks inherent in aggregate data compilation and uses that are non-transparent, and note that when aggregate data is applied directly to individuals, additional risk mitigations need to apply, even if the actual aggregate data (or CAI) itself does not contain PII.

We remain attentive to any questions you may have and would welcome the opportunity to discuss these issues further.

Respectfully submitted,

Pam Dixon
Founder and Executive Director,
World Privacy Forum