April 1, 2024

COMMENTS IN RESPONSE TO US OFFICE OF MANAGEMENT & BUDGET REQUEST FOR INFORMATION ON PRIVACY IMPACT ASSESSMENTS*

The Association for Computing Machinery (ACM), founded in 1947 as a non-profit and non-lobbying organization, is the world's largest and longest-established society of individual professionals involved in virtually every aspect of computing. Our over 50,000 members in the United States and 100,000 worldwide serve in government, industry, academia, and civil society organizations. Many have pioneered and continue to pursue work on the cutting edge of computing, including artificial intelligence.

Through its U.S. Technology Policy Committee (USTPC), ACM strives to provide apolitical technical expertise and analysis to Congress, the Executive Branch, and policymakers throughout government to inform technology policy. USTPC hopes its response helps OMB harmonize the privacy impact assessment (PIA) process across the federal government, increase its utility, improve its value as a tool that helps identify privacy risks, and determine appropriate measures to address/mitigate risks.

To that end, USTPC is pleased to offer the following responses to select inquiries in the Office of Management and Budget's Request for Information regarding Privacy Impact Assessments:[1]

Role of PIAs in Addressing and Mitigating Privacy Risks

1. A wide range of privacy risks are associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII). What improvements to OMB guidance on PIAs as analytical tools and notices to the public would assist agencies in identifying, addressing, and mitigating these risks, including when an agency:

a. Develops, procures, or uses information technology to handle PII;

It would be helpful if OMB provided default terms and definitions for concepts used in PIAs, such as standard prose and machine-readable constructs, to standardize needed concepts and avoid confusing diversity.

---

* These comments were principally drafted for USTPC by Vice Chair Jody Westby, Privacy Subcommittee Chair Brian Dean, and Committee members Jean Camp, Peter Neumann, Neeti Pokhriyal, and Arnon Rosenthal. Also contributing were Technology Policy Council (TPC) Interim Chair Jim Hendler, TPC Past Chair Lorraine Kisselburgh, and USTPC members David Bauman, Vaibhav Garg, Santos Jha, Ali Obaidi, and Sai Teja Makani.

[1] *Request for Information: Privacy Impact Assessments*, 89 FR 5945-47 (January 30, 2024). For ease of reference, section headings and questions answered are copied herein in boldfaced italics and retain their original numbers as published in the Federal Register. Questions not responded to have been omitted.

It also would be helpful to clarify how best to express common privacy controls and metrics, and whether deviation from a control requires justification. Tools need a consistent means of measuring, with well-documented standards and best practices. While explainability should not be confined to a template, ways of reporting results should be standardized where feasible. In addition, it is important that tools be used in accordance with all laws, regulations, and policies (including OMB M-10-06) pertaining to privacy, accessibility, information security, and records management.[2]

2. What other models or best practices for conducting and documenting PIAs or similar analyses could improve agencies' PIAs?

a. Are there approaches to analyzing and documenting how an entity addresses and mitigates privacy risks used by non-federal government entities, specific sectors or industries, academia, or civil society that OMB should consider?

Today, there is a diverse range of approaches to analyzing and documenting privacy risks within the federal government, state governments, foreign jurisdictions, and the private sector. *USTPC recommends that OMB perform an analysis of these various approaches – and various definitions of personal data – and update current guidance used by government agencies and departments to promote a harmonized approach.*

Since the E-Government Act was passed in 2002, which required PIAs, and OMB's memorandum M-03-22, which set forth guidance for implementing the privacy provisions of the Act, numerous federal agencies have developed guidance on conducting PIAs. A simple Google search revealed major federal agency websites with guidance on PIAs, much of it more than ten years old, such as SEC (2007), DHS (2010), OPM (2010), NIH (2011), DOJ (2012), DOI (2014), DOD (2017), and HUD (2023). During this time, approaches to PIAs have evolved and new requirements, such as incorporating privacy by design, have been adopted. Thus, the federal guidance and templates are out-of-date, inconsistent, and confusing. They do not now provide the public with a uniform approach to federal privacy analysis.

U.S. states also have actively passed privacy legislation over the past decade, much of it mirroring the requirements of the European Union's (EU) General Data Protection Regulation (GDPR). Thirteen states have adopted comprehensive privacy laws with expanded definitions of personal data, and twenty states have similar legislation pending.[3] Eleven of the thirteen comprehensive state privacy laws require PIAs, and 17 of the 20 states with new privacy laws pending require assessments.

The State of California (CA) is often looked to by other states when drafting and enacting privacy laws and regulations. CA requires all state agencies/entities to conduct Privacy Threshold Assessments (PTA) for all proposed and modified information systems (paper and electronic) and PIAs on systems that collect or maintain personal information. A California PTA/ PIA Standard was developed, which is aligned with the National Institute of Standards and Technology (NIST) Special Publication 800-53

[2] "Open Government Directive," Memorandum M-10-06, Office of Management and Budget, Dec. 8, 2009, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-06.pdf.

[3] Andrew Folks, "U.S. State Privacy Legislation Tracker," Int'l Assn. of Privacy Professionals, Mar. 1, 2024, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.[4] The PTA/PIA Form can be filled in electronically on a downloaded Word document.[5] PTA/PIAs are required on all new systems and when changes are proposed to existing systems.[6] The California PTA/PIA requires data classifications and security categorizations. The PTA considers all types of data considered personal information under CA law and requires a PIA if the system collects, uses, maintains, or shares any of the data types.

USTPC also urges OMB to analyze international approaches to PIAs because the EU has been the global leader on privacy protection since 1994, and many comprehensive U.S. state privacy laws are modeled after the GDPR. The GDPR requires a data protection impact assessment (DPIA) when "a type of processing in particular using new technologies, and taking into account the purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons."[7] Regulation (EU) 2018/1725 mirrors the GDPR and applies to the processing of personal data by EU institutions, bodies, offices, and agencies and similarly requires a DPIA.[8] The EU has put out well-written guidance addressing DPIAs that is applicable to both EU public and private sectors and is worthy of U.S. Government consideration.[9]

---

[4] "Security and Privacy Controls for Information Systems and Organizations," 800-53 Rev. 5, National Institute of Standards and Technology, Computer Security Resource Center, Dec. 10, 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[5] PS 022 – SIMM 5310-C: Privacy Threshold Assessment and Privacy Impact Assessment: Procedures and standards update, July 2022, California Dept. of Technology Office of Information Security, https://cdt.ca.gov/policy/announcements/ps-023-simm-5310-c-privacy-threshold-assessment-and-privacy-impact-assessment-updates/.

[6] Privacy Threshold and Privacy Impact Assessments, California Dept. of Adm. Services, State Administrative Manual, Section 5310.8, https://www.dgs.ca.gov/en/Resources/SAM/TOC/5300/5310-8.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons re: the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 35(1), https://gdpr-info.eu/art-35-gdpr/.

[8] Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC," Oct. 2018, https://fusionforenergy.europa.eu/downloads/terms/Regulation_EC_2018_1725.pdf.

[9] "Guidelines on Data Protection Impact Assessment (DPIA)" determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 17/EN WP 248 rev. 01, Adopted Apr. 4, 2017, revised and adopted on Oct. 4, 2017, https://ec.europa.eu/newsroom/article29/items/611236; "Recommendation 01/2019 on the draft list of European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725," European Data Protection Board, Adopted July 10, 2019, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/ recommendation-012019-draft-list-european-data_en; "Guidelines 4/2019 on Article 25 Data Protection by Design and Default, Version 2.0, European Data Protection Board, Oct. 20, 2020,

Other countries also require PIAs (or DPIAs), including Canada, Switzerland, and the United Kingdom. The Electronic Privacy Information Center recently published an excellent comparison of privacy impact assessment requirements in the US and abroad.[10] Bloomberg Law also published a useful table comparing key requirements of the GDPR and U.S. state privacy laws, which includes a comparison of assessment provisions.[11] Another useful compilation of templates for various countries' privacy impact assessments has been compiled by the International Association for Privacy Professionals (IAPP).[12]

The privacy assessment requirements of foreign jurisdictions are important for OMB to consider because numerous U.S. Government contractors must comply with the impact assessment requirements of the E-Government Act, as well as state privacy assessment requirements and the GDPR. Therefore, the U.S. Government should analyze these various approaches, learn from them, and try to amend U.S. PIA guidance in a manner that advances a harmonized approach.

In addition to the various assessment methodologies that have cropped up over the 20-plus years since the E-Government Act was enacted, the definition of what constitutes personal data also has evolved. The updated HUD template, for example, considers 42 data fields as personally identifiable information (PII),[13] whereas OMB Guidance Memorandum M-03-22 defines Information in identifiable form much more narrowly:

> Information in identifiable form – is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).[14]

OMB Circular A-130 also defines this term:

---

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf; "Data Protection Impact Assessment (DPIA): How to conduct a Data Protection Impact Assessment " https://gdpr.eu/data-protection-impact-assessment-template/.

[10] Kara Williams, "Assessing the Assessments: Comparing Risk Assessment Requirements Around the World," Electric Privacy Information Center, Dec. 4, 2023, https://epic.org/impact-comparison/.

[11] "GDPR vs. State Comprehensive Consumer Privacy Laws," https://www.bloomberglaw.com/external/document/XE7S54D0000000/data-collection-management-comparison-table-gdpr-vs-state-compre.

[12] "Data Protection and Privacy Impact Assessments Topics Page: Samples, Templates and Forms," IAPP, https://iapp.org/resources/topics/privacy-impact-assessment-2/.

[13] "Privacy Impact Assessment," Dept. of Housing and Urban Dev., Sept. 19, 2023, https://www.hud.gov/sites/dfiles/OCHCO/documents/PIATemplate.pdf

[14] "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Office of Management and Budget, M-03-22, Sept. 26, 2003, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2003/m03_22.pdf.

> 'Personally identifiable information' 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.[15]

State laws, such as California, protect data that is considered sensitive personal information (SPI) within the protection of the law, such as sexual orientation, racial or ethnic origin, religious or philosophical beliefs, and union membership. A new law effective January 1, 2024, expands SPI in California to include a consumer's citizenship and immigration status.[16] Moreover, the GDPR and state laws expand the definition of personal data and require consideration of whether the data in a particular dataset could be linked with data in another database and thereby enable identification of an individual. We note that OMB A130's definition of "personally identifiable information" also addresses the issue of linkage.

Thus, much of the current guidance by federal agencies and departments on PIAs is out-of-date and does not have a consistent definition of personal data within the scope of more recent, expanded privacy laws. After a full review of foreign, state, and federal guidance on privacy impact assessments, OMB should consider: (1) the data fields considered to be personal data under federal law, (2) the types of processing this data may be subject to; and (3) how to best close gaps in current PIA guidance, including Memorandum M-03-22, and to revise its guidance to promote harmonization among agencies and departments.

b. Are there similar approaches to analyzing and documenting how an entity addresses and mitigates other risks in information governance (e.g., security risks) that OMB should consider from other federal guidance or frameworks?

USTPC recommends that more be done collaboratively by privacy, cybersecurity, and AI experts. Additionally, it is important that safety and security concerns be evaluated to determine when these are separable and can be evaluated independently, and where they are inherently interdependent (as described in the FDA guidelines for health devices). With regard to information governance, it is important that PIAs require that the risks which warrant C-suite/administrator oversight be identified.

3. What guidance should OMB consider providing to agencies to help reduce any duplication that may arise in preparing PIAs along with other assessments focused on managing risks (e.g., security authorization packages or the AI impact assessments proposed in OMB's Draft Memorandum on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence) and to support these assessments' different functions?

It is important that PIAs incorporate privacy considerations associated with the use of AI and emerging technologies so duplication in assessments is avoided, interdependencies are considered, and

---

[15] OMB Circular A-130, "Managing Information as a Strategic Resource," p.33 (July 28, 2016) https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[16] Natasha G. Kohne, Michelle A. Reed, Rachel Claire Kurzweil, Jerry Berger, "California Expands Definition of Sensitive Personal Information Covered Under CCPA." Akin Gump, Oct. 13, 2023, https://www.akingump.com/en/insights/blogs/ag-data-dive/california-expands-definition-of-sensitive-personal-information-covered-under-ccpa.

inconsistencies are minimized to enable a picture of privacy risks. AI systems use data and process it in various ways and the ways in which AI uses training data are ambiguous or unknown. Thus, requiring separate AI and privacy assessments is certain to create duplication of effort and gaps between the assessments.

Avoiding duplication requires structured sharing of sensitive information. Here it is possible to learn from the development of cybersecurity severity ratings, which required an iterative process to develop the current CVE (Common Vulnerabilities and Exposures) ratings used in the National Vulnerability Database (NVD). The stakeholders include the private sector, researchers, and public sector. Further learning from cybersecurity, the current efforts towards transparency of code provided by software bill of materials (SBOMs) may also be applicable to data sources as well. Consider the applicability of the emerging SBOM standards to enhance documentation of data sources, data provenance, and data processing, not only to avoid duplication in identification, but also to better address the interactions of code and data.

Role of PIAs in Facilitating Transparency

5. What improvements to PIAs would help you better understand agencies' assessment of privacy impacts and risk mitigation strategies?

b. What improvement(s) would you recommend to make it easier to read and understand agencies' PIAs?

The agencies within the federal Government have assembled an impressive catalog of PIAs, but it is very difficult to discern what mitigation measures were implemented to counter identified privacy risks, much less obtain any information regarding whether they were effective. PIAs need to be more than a paper exercise that creates a roster of PIAs. At present, there is no follow-up or review process to a PIA that would determine whether any major privacy risks were missed, or if the recommended controls were implemented or effective. Cybersecurity risk assessments are regularly reviewed for this very reason. Privacy assessments should require the same periodic reviews, including an assessment of whether mitigation measures taken were effective.

Privacy Risks Associated with Advances in Technology and Data Capabilities, Including AI

7. AI and AI-enabled systems used by agencies can rely on data that include PII, and agencies may develop those systems or procure them from the private sector.

a. What privacy risks specific to the training, evaluation, or use of AI and AI-enabled systems (e.g., related to AI system inputs and outputs, including inferences and assumptions; obtaining consent to use the data involved in these activities; or AI-facilitated reidentification) should agencies consider when conducting PIAs?

The PIA process is intended to identify potential privacy risks associated with using data with existing, new, and evolving processes and technologies. It records these privacy risks and considers effective controls that may be deployed to manage them. This iterative process can be used for managing privacy risks, including those involved with state-of-the-art technologies, such as AI and other emerging technologies.

While various PIA methodologies and PIA tools have been available for years, it is important that any revised approach to PIAs include consideration of specific privacy risks related to AI, machine learning (ML), and other state-of-the-art technologies. A PIA involving AI or other emerging technologies should include additional considerations to ensure that key risks associated with the data used or processing are taken into account.

Some of the unique privacy risks posed by AI and AI-enabled systems that use PII information can be categorized as follows:

a) Since the behavior of AI-enabled systems might be unpredictable[17] and unexpected, and since they are trained with immense amounts of data scraped from the web, there is a risk that these systems might unintentionally disclose the private and sensitive information of individuals who never provided consent. Additionally, there are risks associated with the lack of reliability, safety, security, and transparency of AI and AI-enabled systems which can compound privacy-related risks.

b) Risks also are posed by lack of transparency related to how data is stored, processed, analyzed, and secured by AI and AI-enabled systems and whether there are mechanisms for defense-in-depth strategies that, for example, assign sensitive stores and compartmentalize different types of sensitive data. This raises not only privacy risks but also serious threats to cybersecurity, data security, and of harm to individuals. Additional privacy and cybersecurity risks also are posed when current AI and AI-enabled systems fail to provide differential access privileges to different types of data. There are also risks (while not unique to AI) of revealing sensitive personal information posed by linking, processing, or integrating disparate sources of non-sensitive information.

c) Conversational Chatbots, other AI systems, and even web browsers keep track of queries, IP addresses, and contextual information to better assist users and are employed for training purposes. Limited testing, validation, and evaluation of AI agents and nascent legal and regulatory considerations both pose the risk that the PII information will be used for training the model. These risks are further compounded by the lack of accuracy, authenticity, and provenance not only of data (collected with consent), but also of derived data and products that do not have appropriate user consent.

These rapidly evolving technologies present new challenges, such as how to properly protect training data, preserve privacy restrictions and the provenance of original data, and impose privacy restrictions for newly created data. AI/ML can source data from many data stores with the potential of violating privacy sharing/usage restrictions applicable to that data, or losing anonymity when combining datasets. The PIA will need to address each of these risks.

Emphasis should be placed on: a) protecting personally identifiable information and privacy sensitive data, including in captured, created, derived, and evolved data sets specific to data subjects; b) downstream manifestations of the data; and c) compliance requirements and contractual terms (including privacy policies); and d) societal expectations regarding protection of the data. The USTPC's

[17] Deep Ganguli, Danny Hernandez, Liane Lovitt, Amanda Askell, Yuntao Bai, Anna Chen, Tom Conerly et al., "Predictability and surprise in large generative models." In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 2022, pp. 1747-1764.

Statement on Preserving Personal Privacy[18] provides guidance for the implementation of appropriate measures and necessary safeguards for effective implementation of privacy controls. Key considerations that may be included in an AI/Emerging Technology section of a PIA include:

- **Privacy by Design:** Privacy by Design is a methodology for proactively embedding privacy into information technology, business practices, and networked infrastructures.[19] PIAs should query whether privacy by design was part of the design, development, implementation, and management of the AI system(s) to be used. The European Data Protection Board's Article 25 Data Protection by Design and by Default[20] document provides guidelines for the implementation of appropriate measures and necessary safeguards for effective implementation of data protection principles and, consequentially, data subjects' rights and freedoms by design and by default. This recognizes a growing demand for provable software privacy claims, systematic methods of privacy due diligence, and greater transparency and accountability in the design and operation of software systems.[21]

- **Security and Safety.** PIAs should consider whether security protections align with existing privacy controls and whether a system has the potential to harm society. AI and emerging technologies may introduce unique and additional safety risks, such as manipulating data to create deepfakes, using datasets to reach invalid conclusions, creating advanced malware, and/or building more effective phishing campaigns. Machine learning models introduce complexity that the PIA should consider. PIAs should incorporate guardrails to protect society as, for example, articulated in the EU's recently adopted comprehensive framework for constraining the risks of AI.[22]

- **Education and Awareness:** PIAs should consider the privacy training required for AI system designers, developers, testers, and users. For example, development teams should consider:
  - the principles of privacy by design, (*i.e.*, proactive measures, privacy by default, privacy embedded into design, full functionality, end-to-end security, visibility and transparency, and respect for user privacy); and
  - the OASIS Privacy by Design Documentation for Software Engineers.[23]

---

[18] Statement on the Importance of Preserving Personal Privacy, US ACM Public Policy Council (March 1, 2018) https://www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf

[19] "Privacy by Design: 7 Foundational Principles," Information and Privacy Commissioner of Ontario, Jan. 2018, https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf.

[20] Supra at footnote 6.

[21] "Privacy by Design Documentation for Software Engineers Version 1.0, OASIS, June 24, 2014, https://docs.oasis-open.org/pbd-se/pbd-se/v1.0/pbd-se-v1.0.html.

[22] Artificial Intelligence Act, European Parliament, Mar. 13, 2024, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html

[23] "Privacy by Design Documentation for Software Engineers Version 1.0," OASIS, Organization for the Advancement of Structured Information Standards (OASIS), June 25, 2014, http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/pbd-se-v1.0.html

Additionally, the business units that own a particular application should have ultimate responsibility for aligning business needs with application development. PIAs should examine how well the system embeds privacy protections in the final product and whether business analysts can determine whether training datasets can be combined without increasing privacy risk.

- **Transparency:** PIAs should examine all data used regardless of its source, including purchased data, how it is processed, how it is protected, with whom it is shared, and for what purpose. AI modeling and its outcomes should be explained, including what controls are used to mitigate the risk of loss of data provenance.

- **Data Protection:** Where limiting personal data collected is not feasible, use sanitization and obfuscation techniques to limit the risk of data leakage. Specifically:
  - **Anonymized Data:** Where feasible use anonymization techniques (*e.g.*, synthetic, generalization, pseudonymization, data perturbation) to protect privacy while still facilitating useful analysis;
  - **Differential Privacy:** Introduce techniques like noise injection to protect individuals' privacy while maintaining statistical accuracy;
  - **Federated Learning:** Train AI/ML models across decentralized devices without centralizing raw data; and
  - **Homomorphic Encryption:** Perform computations on encrypted data without decrypting it.

- **Algorithmic Fairness:** PIAs should encourage appropriate controls to help ensure that AI/ML models do not perpetuate existing biases or infringe on individual privacy rights.

- **Industry Collaboration:** PIAs should incorporate a means to share best practices, research, and lessons learned for improving the PIA and privacy risk ecosystem. PIA development is an evolving process that must change as AI and new technologies evolve and as new business processes are introduced.

b. What guidance updates should OMB consider to improve how agencies address and mitigate the privacy risks that may be associated with their use of AI?

Privacy risks associated with the use of AI must be evaluated, particularly with respect to the types of processing contemplated, the data to be used, and data that may be transferred to an AI database as result of processing. Additionally, PIAs should analyze the unpredictability of how data is used and the security of the data.

8. What role should PIAs play in how agencies identify and report on their use of commercially available information (CAI) that contains PII?

a. What privacy risks specific to CAI should agencies consider when conducting PIAs?

With CAI (or any other data), unexpected privacy risks are possible when it is combined. The government should particularly consider privacy risks to individuals when purchasing or obtaining

commercial data containing personal data as it is currently defined. Location data and communications traffic data are particularly sensitive, as they can provide a roadmap to private details pertaining to individuals, enabling surveillance.[24]

It is important that analysis of privacy risks consider how data in one dataset can be linked with data in another to reveal personal identities and/or details. For example, the risk of disclosure and identifiability rises significantly with just two or three pieces of data combined. Before purchasing such data, federal agencies should be required to conduct a rigorous PIA that takes into consideration the legal restrictions that apply to the government directly accessing/obtaining this data from its source, the privacy policies applicable to the data, and its path from original source to the dataset. Assessments involving CAI should clearly document the expected boundaries of predictability of how the data will be used, and the security of the data so that such information can be updated to improve future estimates and best practices.

b. OMB M–03–22 requires PIAs "when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources," while noting that "[m]erely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement." What guidance updates should OMB consider to improve how agencies address and mitigate the privacy risks that may be associated with their use of CAI that contains PII?

See above.

Other Considerations

10. What else could help promote greater effectiveness and consistency across agencies in how they approach PIAs?

USTPC recommends the creation of one set of PIA guidance applicable to all federal agencies and departments, including implementation guidance. A standard template also is recommended. This would also ensure that changes to the guidance will be applied across the government and reduce the need for each agency to issue updated guidance. OMB also may want to consider whether PIAs should be randomly reviewed by an experienced PIA governance body.

11. What else should OMB consider when evaluating potential updates to its guidance on PIAs?

Broader factors than those covered above impact privacy, and most are not addressed in PIA methodologies. USTPC believes it is important that OMB take these factors into consideration as it contemplates updates to its guidance on PIAs:

- Computer systems and networks are incapable of enforcing requirements for trustworthiness, including security and privacy. Furthermore, the hardware often is not trustworthy, which

[24] Byron Tau, "U.S. Spy Agencies Know Your Secrets. They Bought Them, "*The Wall Street Journal,* Mar. 8, 2024, https://www.wsj.com/politics/national-security/u-s-spy-agencies-know-our-secrets-they-bought-them-791e243f.

implies that operating systems and applications also are not trustworthy, but this does not imply that systematic harm cannot be identified, prevented, and mitigated. OMB should consider such harm mitigation;

- Risks related to privacy are very diverse and not easy to enumerate. This commonly results in a poor definition of requirements related to privacy; and
- Artificial intelligence often is a misunderstood/exaggerated catchphrase for algorithms that lack documentation and are often nonreplicable.