

Alex Goodenough
Office of Management and Budget
Request for Information: Privacy Impact Assessments
89 Fed. Reg. 5945
Docket number: 2024-01756

April 1, 2024

Coalition Comment of Civil Society Groups:

The undersigned privacy, government accountability, civil liberties, civil rights, racial justice, and human rights groups submit this comment to urge the Office of Management and Budget (OMB) to implement the following recommendations to improve the use of privacy impact assessments (PIAs). The E-Government Act of 2002 requires government agencies to conduct a PIA *before* it either (1) develops or procures information technology that collects, maintains, or disseminates personally identifiable information or (2) initiates a new collection of information.¹ The E-Government Act was enacted with the aim of “promot[ing] better informed decisionmaking by policy makers”; “provid[ing] enhanced access to Government information”; and “mak[ing] the Federal Government more transparent and accountable.”²

Despite the aims and requirements of the E-Government Act, agencies often fail to conduct PIAs at all or conduct PIAs well after the system has been implemented—undermining the purpose and usefulness of the assessments. PIAs have unfortunately become an optional box-checking exercise that fails to live up to its original purpose and falls short in the analysis of the privacy risks of the systems the government uses. This failure will have greater consequences as the government increasingly uses systems that incorporate artificial intelligence. Privacy risks in general, but particularly AI-related privacy risks, often implicate our civil liberties and civil rights.

Black communities, Latino communities, and other communities who have been historically disadvantaged have a particularly strong interest in making sure that privacy impact assessments are done correctly, because they are disproportionately impacted by these harms. AI systems often rely on data sets that contain personally identifiable information and the outputs can be tainted by historical bias, racial bias, or other social biases. The targets of AI systems, particularly surveillance-related systems, are often disproportionately from communities of color and other traditionally marginalized communities. The failure to meaningfully consider the impact of privacy-invasive systems and databases used by the government has eroded our civil liberties and civil rights. These consequences are compounded by the scale at which the federal government implements these systems and the fact that people often do not have a choice about the inclusion

¹ E-Government Act § 208(b)(1)(A).

² E-Government Act §§ 2(b)(7), (9), (11).

of their personal information or if the system is directed at them. In order to better address the privacy risks and the related civil liberties and civil rights risks with the information systems used by government agencies, agencies should implement the following recommendations.

PIAs should be pre-decisional, not an exercise in post-hoc justifications.

The E-Government Act of 2002 established PIAs as both a tool that informs the public about federal activities and one that helps agencies decide whether to implement potentially invasive and harmful systems. PIAs were modeled after Environmental Impact Assessments, which agencies must complete before breaking ground on a project. The E-Government Act of 2002 is clear that agencies must complete a PIA *before* using a new information technology involves personally identifiable information. But federal agencies regularly ignore this requirement, completing PIAs after systems are in place. OMB should clarify in the new guidance that agencies are out of compliance with the E-Government Act if the agencies begin using an information collection system before completing a PIA.

PIAs should be made public in an organized and searchable format.

Currently some federal agencies do the bare minimum by publishing outdated webpages to meet their obligation to make PIAs public. Other agencies don't even go that far, and simply claim that they comply by making PIAs available when requested through the Freedom of Information Act. PIAs are meant to meaningfully inform the public about potentially harmful government activity. But they will not serve that function if the public can't find a document because it's buried in a disorganized list or hidden behind a wall of FOIA procedures. OMB should either 1) create a standalone PIA archive searchable by agency, system name, date, etc. or 2) publish guidance requiring all federal agencies to publish PIAs in an accessible, organized, and searchable manner, such as on regulations.gov.

PIAs must provide sufficient detail about agency information systems to allow a full accounting of the privacy risks.

PIAs often lack important details about the full range of personally identifiable information in an information system or accessible by an information system. Similarly, PIAs often lack a full accounting of the other information systems connected to the system being assessed. OMB should make clear the amount and level of detail that must be disclosed in a PIA, including: 1) All the different types of personally identifiable information associated with the system whether collected, stored, accessed, or otherwise processed by the system; 2) An accounting of any interoperability with other information systems, particularly accounting for data that can be transferred between systems; and 3) An accounting of the entities that have access to the data in a given information system regardless if the access is through the information system itself or through a separate, interoperable system.

PIAs must disclose and evaluate the harms of AI systems.

The OMB should incorporate AI assessment, auditing, and reporting requirements into its guidance on PIAs. Agencies should analyze how an AI system functions, including its risks, uses, purpose, benefits, limitations, and inputs used to train and deploy the system. OMB should mandate that agencies perform pre-deployment testing to identify and mitigate potential AI risks, including harms related to the collection, use, and transfer of personal data. The OMB should require agencies to publicly disclose any harms identified through such assessments and audits, including information about any mitigation measures adopted to address such harms.

Privacy Threshold Analyses should be made publicly available in a timely manner.

A Privacy Threshold Analysis (PTA) or similar document is used by agencies to determine the privacy compliance requirements for the use of personally identifiable information. PTAs determine, for example, if a PIA is required. These documents are generally not made public, despite containing crucial information about the necessary privacy compliance steps needed for a given system. PTAs should be published by default to inform the public of the privacy compliance requirements for a new or modified system. Publication should occur in a timely manner after the PTA determination has been made to allow the public and government watchdogs to hold agencies accountable when they do not meet their privacy compliance obligations.

PIAs must better evaluate the impact of an agency's use of third party services.

Current PIAs consider a very narrow set of potential privacy implications for an agency's use of a third party service and fail to consider the larger implications. PIAs must consider the broader privacy implications of the government's use of third party systems and data. Often third party systems may obtain their data by underhanded means that undermine privacy, use the data in unscrupulous ways, or sell data or access to privacy-invasive systems to disreputable buyers. Agencies should closely scrutinize third party contractors for risks created by poor cybersecurity practices, privacy and disclosure policies, and AI and other advanced surveillance technologies. Furthermore, government agencies should consider and disclose the privacy implications of purchasing data or access to data from a third party when the government itself could not obtain the data directly without further judicial process. Finally, PIAs should identify the third party contractor or specific data sources incorporated into government systems to allow the public a detailed understanding of the privacy risks involved.

PIAs are an important tool of oversight and transparency, but for them to be effective the requirements of the E-Government Act of 2002 must be enforced and OMB must update its guidance. We therefore urge OMB to implement the above recommendations. For any questions about the submission, please contact Jeramie Scott, Director of EPIC's Project on Surveillance Oversight, at scott@epic.org.

Sincerely,

Access Now
Advocacy for Principled Action in Government
Algorithmic Justice League
American Civil Liberties Union
Center for Digital Democracy
Data & Society
Defending Rights & Dissent
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press
Government Information Watch
Japanese American Citizens League - National
Just Futures Law
Kapor Center
Lawyers' Committee for Civil Rights Under Law
The Leadership Conference of Civil and Human Rights
National Consumer Law Center
National Council of Asian Pacific Americans (NCAPA)
National Taxpayers Union
National Workrights Institute
New America's Open Technology Institute
Organization for Identity and Cultural Development (OICD.net)
Project on Government Oversight
Public Knowledge
Restore The Fourth
Surveillance Technology Oversight Project
UnidosUS