epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE OFFICE OF MANAGEMENT AND BUDGET

Request for Information: Privacy Impact Assessments

April 1, 2024

By notice published on January 30, 2024, the Office of Management and Budget (OMB) requested comments regarding Privacy Impact Assessments (PIAs).[1] More specifically, OMB requested input "on how piracy impact assessments (PIAs) may be more effective a mitigating privacy risks, including those that are further exacerbated by artificial intelligence (AI) and other advances in technology and capabilities."[2] The Electronic Privacy Information Center (EPIC) submits these comments to urge OMB to ensure agencies comply with current PIA requirements, improve transparency around PIAs and associated documents, and update guidance around conducting PIAs to make them more detailed and capable of addressing the privacy risks of newer technologies.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[3] EPIC has a particular interest in accountability, civil rights, privacy, and civil liberties with respect to the government's use of personally identifiable information. PIAs play an important role in government accountability and determining the privacy risks of systems that use personally identifiable information (PII). A properly conducted PIA enables an agency to identify privacy risks, determine if and how those risks can be mitigated, and make an informed decision whether the proposed collection or system can be justified in light of its privacy impact. Additionally, a PIA informs the public of data collection or an information system that poses a threat to privacy. PIAs not only help to protect privacy but in doing so inherently help to protect civil rights and civil liberties.

EPIC has a long history of advocating for improvements to PIAs, using the Freedom of Information Act to make PIAs public and trying to force agencies to conduct PIAs. EPIC's work has made clear the shortcomings of PIAs and the consistent failure of agencies to comply with the E-Government Act's PIA requirement.

---

[1] Notice of Request for Information (RFI) on Privacy Impact Assessments, 89 Fed. Reg. 5945 (Jan. 30, 2024), https://www.govinfo.gov/content/pkg/FR-2024-01-30/pdf/2024-01756.pdf.
[2] 89 Fed. Reg. at 5945.
[3] EPIC, *About Us* (2024), https://epic.org/about/.

I. EPIC's work exposing the failure of federal agencies to comply with the PIA requirement

Over the past decade, EPIC has identified numerous instances in which the DHS, FBI, DEA, United States Postal Service, and other agencies have failed to complete required PIAs under the E-Government Act for activities implicating personal data.

In 2015, EPIC sued the FBI over its FOIA request for all unpublished PTAs and PIAs, particularly those related to facial recognition technology, license plate readers, and domestic drone surveillance—documents which had not been publicly updated for years, if at all.[4] EPIC filed the FOIA request because in the past several years prior to EPIC'S request it had come to light that the FBI was using technology in ways that should require a PIA and the agency had indicated it was going to do a number of PIAs that were not publicly available at the time of the request.

For example, in July 2012, the Senate Subcommittee on Privacy, Technology and the Law held a hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties," where the FBI stated they were updating its PIA on facial recognition.[5] In a statement for the record by Jerome Pender, the Deputy Assistant Director of the Information Services Branch for Criminal Justice Information Services Division of the FBI, stated "the 2008 [Interstate Photo System] PIA is currently in the process of being renewed by way of Privacy Threshold Analysis, with an emphasis on facial recognition. An updated PIA is planned and will address all evolutionary changes since the preparation of the 2008 PIA."[6]

Similarly, in June 2013 the Senate Judiciary Committee held a hearing on "Oversight of the Federal Bureau of Investigation."[7] During that hearing, Senator Chuck Grassley asked FBI Director Robert Mueller about the FBI's use drones. Director Mueller responded that the FBI did use drones domestically for surveillance. During that same exchange, Senator Grassley asked about the development of policies, procedures, and operational limits on the FBI's use of drones and the privacy impact on Americans. Director Mueller indicated that the FBI was at the beginning stages and were "exploring not only the use but also the necessary guidelines for that use."[8]

In 2013 through a FOIA request to the FBI, EPIC obtained emails from 2012 that indicated the FBI was required to do a PIA for its license plate reader ("LPR") program and make that PIA

---

[4] EPIC, *EPIC v. FBI – Privacy Assessments* (2017), https://epic.org/documents/epic-v-fbi-privacy-assessments/.
[5] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology, and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012).
[6] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology, and the Law of the S. Comm. on the Judiciary*, 112th Cong. 7 (2012) (statement of Jerome Pender, Deputy Assistant Director, FBI), *available at* https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf.
[7] *Oversight Hearing of the Federal Bureau of Investigation: Hearing Before the Comm. on the Judiciary*, 113th (2013).
[8] *Oversight Hearing of the Federal Bureau of Investigation: Hearing Before the Comm. on the Judiciary*, 113th 13 (2013), https://www.govinfo.gov/content/pkg/CHRG-113shrg88484/pdf/CHRG-113shrg88484.pdf.

publicly available.[9] Additionally, the emails indicated a draft PIA existed for the LPR program.[10] Despite receiving hundreds of pages of documents from the FBI in EPIC's 2015 FOIA lawsuit against the Bureau for all PTAs and PIAs, EPIC did not receive any PIAs for the FBI's use of facial recognition technology, drones, or license plate readers despite evidence that such documents should have been completed.

In 2015 EPIC also filed a lawsuit against the DEA over its FOIA request for all unpublished PTAs and PIAs, particularly those related to the Hemisphere telephone record collection program, National License Plate Reader Program, and DEA Internet Connectivity Endeavor data aggregation and sharing program—programs for which there was no publicly available PTA or PIA documentation.[11] At the time of the 2015 EPIC FOIA request, some of the information known about Hemisphere program was that it was funded by the DEA and the White House's Office of National Drug Control Policy, and since at least 2007 the program had allowed the DEA and other law enforcement agencies to access billions of phone records of AT&T customers as well as other non-customers whose communications were routed through an AT&T switch.[12]

On May 21, 2012, the U.S. House of Representatives Subcommittee on Border and Maritime Security held a field hearing on "Stopping the Flow of Illicit Drugs In Arizona By Leveraging State, Local And Federal Information Sharing."[13] At the hearing, Douglas W. Coleman, Special Agent in Charge, Phoenix Field Division of the DEA, was one of the witnesses. In his statement for the record, Mr. Coleman indicated that "[i]n December 2008, DEA launched a National License Plate Reader (LPR) Initiative in direct response to the smuggling of illicit drug monies out of the United States, primarily via the U.S.-Mexico border."[14] According to Mr. Coleman's statement for the record, the DEA's LPR program monitors and targets vehicles, uses existing database technology, and promotes information sharing.[15] In 2015 the DEA's LPR program came under scrutiny by U.S. news media.[16] Additionally, in January 2015 then Chairman Chuck Grassley and Rank Member

---

[9] Jeramie D. Scott, *License Plate Readers – Will the FBI Ever Address Their Privacy Implications* (Jan. 28, 2014), https://blog.epic.org/2014/01/28/license-plate-readers-will-the-fbi-ever-address-their-privacy-implications/.
[10] *Id.*
[11] EPIC, *EPIC v. DEA – Privacy Impact Assessments* (2016), https://epic.org/documents/epic-v-dea-privacy-impact-assessments/.
[12] Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. Times, Sept. 2, 2013, https://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html; Mike Levine, *DEA Puts Phone Company Inside Government Offices*, ABC News, Sept 1, 2013, https://abcnews.go.com/blogs/headlines/2013/09/dea-program-puts-phone-company-inside-government-offices.
[13] *Stopping the Flow of Illicit Drugs In Arizona By Leveraging State, Local And Federal Information Sharing: Hearing Before the Subcomm. on Border & Maritime Security of the House Comm. on Homeland Security*, 112th Cong. (2012).
[14] *Stopping the Flow of Illicit Drugs In Arizona By Leveraging State, Local And Federal Information Sharing: Hearing Before the Subcomm. on Border & Maritime Security of the House Comm. on Homeland Security*, 112th Cong. (2012) (statement for the record of Douglas W. Coleman, DEA special agent), https://www.justice.gov/d9/testimonies/witnesses/attachments/05/21/12//05-21-12-dea-coleman.pdf.
[15] *Id.*
[16] *See, e.g.*, Devlin Barrett, *U.S. Spies on Millions of Drivers*, Wall St. J. (Jan. 26, 2015), https://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779.

Patrick Leahy of the Senate Judiciary Committee sent a letter to Attorney General Eric Holder regarding the privacy concerns related to the government's use of LPRs.[17]

During the same May 2012 field hearing, Mr. Coleman's statement for the record identified another program entitled the DEA Internet Connectivity Endeavor (DICE) that "… enables any participating federal, state, local and tribal law enforcement agency to de-conflict investigative information, such as phone numbers, email addresses, bank accounts, plane tail numbers and license plates, to identify investigative overlaps."[18] DICE provided access to information collected through the LPR program (among other information) and allows the accessibility of such data through the Internet.[19] DICE reportedly contained approximately a billions records, including phone log data, at the time.[20] Despite the DEA programs described above and EPIC's FOIA lawsuit, the DEA did not produce a single PTA or PIA relevant to those programs.

In addition to EPIC's work to uncover whether PIAs have been conducted for various information systems and if so to make them public, EPIC has also filed lawsuits to compel agencies to produce required PIAs under the E-Government Act. In 2017, EPIC sued the now-defunct Presidential Advisory Commission on Election Integrity for failing to conduct a PIA before seeking citizens' personal voting information, eventually securing the deletion of the unlawfully collected data.[21] In 2018, EPIC sued the Department of Commerce and U.S. Census Bureau to compel the agencies to complete a PIA for the census's addition of a citizenship question—a question which was later dropped.[22] In 2021, EPIC sued the U.S. Postal Inspection Service under the E-Government Act for failing to produce a PIA for its Internet Covert Operations Program, highlighting the Service's surveillance of protesters and other individuals using facial recognition and social media monitoring services.[23]

Despite some positive results EPIC has had bringing lawsuits against agencies for the failure to conduct a PIA, enforcement by civil society is not a reliable means to force the completion of a PIA. Indeed, courts have generally not ruled in EPIC's favor regarding its standing to compel an agency to conduct a PIA. Furthermore, it is clear from EPIC's experience that the failure of agencies to conduct a PIA is not isolated to a few incidents but a widespread occurrence that goes beyond EPIC's means to rectify even if lawsuits could reliably force agencies to conduct PIAs.

---

[17] Letter from Senators Patrick Leahy and Charles Grassley to Attorney General Eric Holder on DEA License Plate Reader Privacy Concerns (Jan. 28, 2015), https://www.grassley.senate.gov/news/news-releases/grassley-leahy-raise-privacy-concerns-about-dea-license-plate-tracking-system.

[18] *Stopping the Flow of Illicit Drugs In Arizona By Leveraging State, Local And Federal Information Sharing: Hearing Before the Subcomm. on Border & Maritime Security of the House Comm. on Homeland Security*, 112th Cong. (2012) (statement for the record of Douglas W. Coleman, DEA special agent), https://www.justice.gov/d9/testimonies/witnesses/attachments/05/21/12//05-21-12-dea-coleman.pdf.

[19] *Id.*

[20] John Shiffman, *How DEA program differs from recent NSA revelations*, Reuters (Aug. 5, 2013), https://www.reuters.com/article/idUSBRE9740AI/.

[21] EPIC, *EPIC v. Presidential Election Commission* (2018), https://epic.org/documents/epic-v-presidential-election-commission/.

[22] EPIC, *EPIC v. Commerce (Census Privacy)* (2019), https://epic.org/documents/epic-v-commerce-census-privacy/.

[23] EPIC, *EPIC v. U.S. Postal Service* (2022), https://epic.org/documents/epic-v-u-s-postal-service/.

II. Role of PIAs in addressing and mitigating privacy risks

The E-Government Act of 2002 established Privacy Impact Assessments as an important step agencies must take before engaging in activities that risk Americans' privacy and civil rights. But PIAs are not currently doing the job they are meant to do. PIAs should require a thorough evaluation of the potential harms of an information collection system that helps an agency decide *whether* to implement that system. Now, agencies treat PIAs as a box checking exercise to complete *after* information collection systems are in place, removing the decision-making value of the document. PIAs often omit important information that could help the public better understand the risks of federal systems—that is, if the agency conducts and publishes the PIA at all. To address the deficiencies in PIAs across the government, OMB should update its guidance to require that agencies:

1) Conduct PIAs as required and publish them promptly;

2) Conduct PIAs before systems are in place so that PIAs are pre-decisional documents, not post-hoc rationalizations;

3) Produce PIAs that are sufficiently detailed to give the public a full accounting of agency activities and the risks they create; and

4) Fully disclose and evaluate the risks created by using third-party technology and third-party data.

Only if the deficiencies in current implementation of PIAs are addressed can PIAs be, as OMB put it, "one of the most valuable tools Federal agencies use to ensure compliance with applicable privacy requirements and manage privacy risks."[24]

a) Agencies must conduct PIAs on all information collection systems in a timely manner.

The most basic requirement of Section 208 of the E-Government Act is unfortunately one of the most frequently flouted. Agencies regularly fail to complete PIAs at all, or do so on a timeline of decades instead of weeks and months. Failure to produce PIAs usually leaves agencies without any analysis of the privacy impacts and potential flaws in their systems, and it always leaves the public without critical information. For agencies that don't want to comply with the spirit of the E-Government Act, the current guidance offers loopholes that agencies can lean on to excuse blatant non-compliance.

The U.S. Postal Inspection Service's (USPIS) failure to complete a PIA for a controversial secret intelligence program leveraging advanced technology illustrates the harms that can propagate when agencies choose not to comply with the E-Government Act. USPIS is a law enforcement agency housed within the Postal Service, tasked with enforcing mail fraud and protecting postal

[24] Appendix II to Circular A-130, *Responsibilities for Managing Personally Identifiable Information*, 10, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

workers.[25] In 2021, EPIC sued the U.S. Postal Inspection Service under the E-Government Act for failing to produce a PIA for its Internet Covert Operations Program (iCOP).[26]

This program runs a bevy of cutting-edge information collection systems, including "'cryptocurrency tracking, open source intelligence and social media analysis, geospatial mapping, and data visualization, and USPS backend and network data exploitation'" alongside Clearview AI's facial recognition software, and specialized social media software for creating fake online identities.[27] iCOP operates with little functional oversight, and virtually no transparency. In 2020-21, the iCOP program tasked its analysts with tracking and collecting online evidence of both left-wing and right-wing protests.[28] Lacking even the oversight and transparency requirements of DHS, the iCOP was able to secretly perform controversial and First Amendment infringing surveillance and then distribute the intelligence it gathered across both federal and local law enforcement agencies. Without a PIA to FOIA, there was functionally no way to discover the program until its existence was leaked to a journalist.

Outside of our litigation work, EPIC regularly calls out agencies for PIAs that are conducted and published long after harmful mass surveillance systems are put in place, or updated so infrequently that document no longer serves to meaningfully inform the public about what an agency is doing. In one egregious example, DHS subcomponent Immigrations and Customs Enforcement (ICE) ran the notorious Alternatives to Detention/ISAP program for nearly 20 years without conducting a PIA, despite using the most invasive forms of surveillance technology like GPS ankle monitors and facial recognition equipped smartphone apps.[29] ICE claimed to be in compliance with the E-Government Act by grandfathering the rapidly expanding ISAP program under an existing System of Records and PIA for the ENFORCE system.[30] But the agency has faced no consequences

---

[25] 39 C.F.R § 233.1 - Arrest and investigative powers of Postal Inspectors (2007), https://www.ecfr.gov/current/title-39/chapter-I/subchapter-D/part-233/section-233.1.
[26] EPIC, *EPIC v. U.S. Postal Service* (2022), https://epic.org/documents/epic-v-u-s-postal-service/.
[27] Joseph Cox, *Here's How the Post Office's Internet Cops Describe Themselves*, Vice (Aug. 31, 2021), https://www.vice.com/en/article/m7enk3/us-postal-inspection-service-icop-presentation (quoting an internal USPIS training presentation); Jana Winter, *Facial recognition, fake identities and digital surveillance tools: Inside the post office's covert internet operations program*, Yahoo! News (May 18, 2021), https://news.yahoo.com/facial-recognition-fake-identities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program-214234762.html.
[28] Jana Winter, The Postal Service is running a 'covert operations program' that monitors Americans' social media posts, Yahoo! News (Apr. 21, 2021), https://news.yahoo.com/the-postal-service-is-running-a-running-a-covert-operations-program-that-monitors-americans-social-media-posts-160022919.html.
[29] Jake Wiener, *New ICE Privacy Impact Assessment Shows All the Ways the Agency Fails to Protect Immigrants' Privacy*, EPIC (Apr. 20, 2023), https://epic.org/new-ice-privacy-impact-assessment-shows-all-the-way-the-agency-fails-to-protect-immigrants-privacy/; American Immigration Council *DHS Publishes Privacy Document About ATDs and the Data They Collect – Two Decades Late* (Apr. 23, 2023), https://immigrationimpact.com/2023/04/06/dhs-publishes-privacy-document-alternatives-to-detention/; *for information on the ATD program see*: Audrey Singer, *Immigration: Alternatives to Detention (ATD) Programs*, Cong. Research Serv. (Jul. 8, 2019), https://crsreports.congress.gov/product/pdf/r/r45804; American Immigration Council, *Alternatives to Immigration Detention: An Overview* (Jul. 11, 2023), https://www.americanimmigrationcouncil.org/research/alternatives-immigration-detention-overview.
[30] Privacy Act of 1974; Department of Homeland Security United States Immigration Customs and Enforcement-011 Criminal Arrest Records and Immigration Enforcement Records System of Records, 81

for delaying a real analysis of the privacy harms of surveilling immigrants for two decades, nor for failing to meaningfully account for those harms. Similarly, DHS' Office of Inspector General found that three agencies failed to implement PIAs before collecting sensitive geolocation data, in one of the most egregious privacy failures in recent agency history.[31] Although agencies regularly shirk their responsibilities to conduct PIAs at all, when it comes to preventing harmful agency actions a late PIA is little better than a nonexistent PIA.

b) PIAs should be pre-decisional, not an exercise in post-hoc justifications and box-checking.

PIAs are modelled after Environmental Impact Assessments (EIS) required by the National Environment Policy Act of 1970,[32] but agencies regularly fail to use PIAs in the in the same way that EISs are used. By federal law, any federal agency must complete an EIS and consider viable alternatives before breaking ground on a new project that might have significant environmental impact.[33] The E-Government Act of 2002 is clear that agencies "shall" conduct a Privacy Impact Assessment "before developing or procuring information technology … or initiating a new collection of information …"[34] But even by agencies' own accounting, most do not meet this requirement.

Agencies fail to complete PIAs on time even though the same agencies recognize that PIAs are helpful. A GAO report on compliance with privacy protections found that only 6 of the 24 agencies surveyed "always" initiated PIAs early enough in the system development process to impact the design or outcome of the system.[35] Only half of agencies claimed to be able to regularly hold staff accountable for failing to conduct a PIA in a timely manner, and one agency even claimed it could never hold staff accountable for the failure.[36] And this issue is not new, the GAO found as far back as 2007 that DHS was not completing and publishing PIAs in a timely manner, reducing the decision-making impacts and transparency effects of PIAs.[37] Neither internal oversight nor external pressure from organizations like EPIC has worked to compel agencies to conduct timely PIAs.

A loose requirement that PIAs be pre-decisional is likely part of the problem. OMB can do more to make it clear to agencies that PIAs must be completed before any covered system is implemented. For agencies, this means clearer guidance that if there is no PIA in place, then the system cannot be activated, full stop.

Fed. Reg. 72080 at 72081-3 (Oct. 19, 2016), https://www.federalregister.gov/documents/2016/10/19/2016-25197/privacy-act-of-1974-department-of-homeland-security-united-states-immigration-customs-and.

[31] Joseph V. Cuffari, OIG-23-61 CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data (REDACTED), DHS OIG (Sept. 28, 2023), https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-61-Sep23-Redacted.pdf.

[32] Pub. L. 91–190, 42 U.S.C. § 4321 *et seq*. (*hereinafter NEPA*).

[33] NEPA Title I.

[34] § 208 (b)(1)(A) E-Government Act, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).

[35] GAO-22-105065 Federal Agency Privacy Programs, Gov't Accountability Off. at 42 (Sept. 2022), https://www.gao.gov/assets/gao-22-105065.pdf.

[36] Gov't Accountability Off., GAO-22-105065 Federal Agency Privacy Programs at 43 (Sept. 2022), https://www.gao.gov/assets/gao-22-105065.pdf.

[37] Gov't Accountability Off. GAO-07-522 DHS Privacy Office at 25-30 (Apr. 2007), https://www.gao.gov/assets/gao-07-522.pdf.

PIAs simply cannot be meaningful if they are completed after-the-fact because the system is already in place, and likely already in use. When PIAs identify systemic problems with the information being collected or the technology being used, it is hard for agencies to reverse course and re-engineer existing systems. It also becomes much harder to police compliance after
In particular, OMB should narrow or eliminate the guidance allowing agencies to post-pone completing a PIA when the technology has been assessed by another PIA or pertains only to internal agency data.[38] As described above, agencies regularly misuse these loopholes to effectively grandfather in new systems that may behave differently from legacy systems, or may collect and analyze different data that creates different privacy risks.

c) *PIAs must be more detailed to ensure that agencies make full and accurate evaluations of privacy harms.*

Most PIAs that agencies currently publish do not provide enough detail for the public to fully understand federal agency systems, nor for the agencies themselves to make a meaningful accounting of potential privacy harms. As a result, the public is unaware of significant risks created by agency action, and agencies are failing to implement low or no-cost privacy protections. The worst results of these oversights are massive data breaches, infringements on individuals' civil rights, and errors leading to wrongful denials of benefits or wrongful arrests alongside reputational and other privacy harms.[39] OMB can do more in its guidance to direct agencies to fully consider the consequences of data breaches, unauthorized access to sensitive systems, and the downstream impacts of systems that are interconnected.

PIAs regularly fail to account for the potential harms of data breaches by implementing weak data minimization requirements. Data minimization is one of the most effective privacy protections because information that is not collected cannot be breached or abused.[40] Very few PIAs undertake a meaningful analysis of the necessity of collecting voluminous amounts of information and tend to defer to agency claims that limiting collection is harmful or impractical. For example, in ICE's ATD PIA from 2023, the agency claims that it is fully implementing data minimization practices despite collecting, retaining, and giving agency employees and contractors full access to immigrants historical geolocation data.[41] But such access is fully unnecessary for tracking down immigrants when they skip court, or for other legitimate enforcement reasons.[42] Agencies similarly are often cavalier about collecting Social Security Numbers (SSN) despite repeated guidance from GAO and

[38] Joshua B. Bolten, M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Off. of Management & Budget § II(B)(c) (Sept. 26, 2003), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/#5.
[39] Danielle Keaks Citron & Daniel J. Solove, *Privacy Harms*, 102 Boston U. L. Rev. 793 (2022), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
[40] *See generally*, EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/.
[41] Immigr. & CustoDHS/ICE/PIA-062 Alternatives to Detention (ATD) Program, ICE (Mar. 17, 2023), https://www.dhs.gov/publication/dhsicepia-062-alternatives-detention-atd-program.
[42] Jake Wiener, New ICE Privacy Impact Assessment Shows All the Ways the Agency Fails to Protect Immigrants' Privacy, EPIC (Apr. 20, 2023), https://epic.org/new-ice-privacy-impact-assessment-shows-all-the-way-the-agency-fails-to-protect-immigrants-privacy/.

OMB that agencies should avoid collecting and storing SSNs where possible.[43] And data minimization routines rarely ask whether retention schedules are necessary. ICE's privacy assessment for facial recognition services for example greenlights a 20 year retention schedule for all data without accounting for the potential damage that could be caused by retaining a false match for an extended period of time.[44]

While agencies are generally good about chronicling what broad types of information is collected, they generally fail on the details and under-report how much data is being collected or how that data is linked with other data. A 2023 DHS OIG report found that CBP had failed to account for how commercially obtained phone geolocation data could be used to identify and track individuals, meaning that the agency was vastly under-reporting the potential risks of its actions.[45] And ICE did little better in accounting for the potential for abuse of its advanced surveillance technologies last year, failing to identify areas where the agency needed to obtain a warrant to use cell-site simulators and otherwise under-describing both the technology ICE has access to and the impact of that tech.[46]

A particular area of concern is agencies failure to account for networked systems and data flows. PIAs tend to capture a single system, and do not often account for just how much data flows between systems.[47] This means that PIAs are often insubstantial checks on agency data transfers, as chronicled in EPIC's 2022 report, DHS' Data Reservoir: ICE and CBP's Capture and Circulation of Location Information.[48] By maintaining discrete PIAs for various location data systems, ICE and CBP are able to skirt effective oversight for just how much location data the agencies buy, and who gets access to it. And the concerns with purchased data only get worse from there. The FBI similarly redacts what systems its facial recognition product FACE is attached to, denying the public the ability to understand how many law enforcment agencies can access the system.[49]

---

[43] OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007), https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-16.pdf; GAO-17-553, Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display (Jul. 25, 2017), https://www.gao.gov/products/gao-17-553.

[44] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the ICE Use of Facial Recognition Services, DHS/ICE/PIA-054 (May 13, 2020), https://www.dhs.gov/publication/dhsicepia-054-ice-use-facial-recognition-services.

[45] Joseph V. Cuffari, OIG-23-61 CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data (REDACTED), DHS OIG at 6-8 (Sept. 28, 2023), https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-61-Sep23-Redacted.pdf.

[46] Kiran Wattamwar, *ICE's Privacy Impact Assessment on Surveillance Technologies is an Exercise in Disregarding Reality*, EPIC (Oct. 5, 2023), https://epic.org/ices-privacy-impact-assessment-on-surveillance-technologies-is-an-exercise-in-disregarding-reality/.

[47] *Government Databases*, EPIC (*last accessed* Mar. 28, 2024), https://epic.org/issues/surveillance-oversight/government-databases/.

[48] Dana Khabbaz, *DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information*, EPIC (Aug. 2022), https://epic.org/documents/dhss-data-reservoir-ice-and-cbps-capture-and-circulation-of-location-information/.

[49] Ernest J. Babcock, Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, FBI (May 1, 2015), https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-

d) Agencies must fully disclose and account for third party data and third party systems.

PIAs often do not name the vendors responsible for providing purchased data, data analysis, or off-the-shelf technology. This practice prevents the public from getting a fulsome view of how data is being analyzed and transferred, who has access to sensitive information, and precisely how proprietary technology works. The vendor matters because the accuracy and security of surveillance products varies widely by vendor. There may be a significant different between using a data broker Lexis Nexis for identity verification and using a more bespoke or lower-tech identity verification provider. OMB should set up specific rules for disclosing information about third party vendors. In particular:

1) Agencies should identify the vendor selling any purchased data;
2) Agencies should identify the vendor selling surveillance technologies or surveillance services; and
3) Agencies should account for the risk that a vendor will get unauthorized access to sensitive data.

PIAs generally do not name the vendor responsible for providing technology or services to the federal government. In extreme cases, like ICE's ATD program, the failure to identify known contractors crosses the border into farce. The ATD PIA refers to a "ATD Servicer" repeatedly, failing to disclose that the servicer is prison-surveillance giant BI Industries.[50] But BI's particular history and corporate structure are highly relevant when assessing the risks of unauthorized use of data, failure to delete data, and other abuses. Agencies that use facial recognition systems similarly fail to disclose the vendor of the system, which has a substantial impact on the accuracy of facial recognition algorithm provided.[51] ICE's PIA for facial recognition services fails to name the facial recognition vendors it contracts with, leaving out any analysis of the wide disparity between a particularly bad actor like Clearview AI and a still-harmful but more limited facial recognition database.[52]

A PIA simply cannot be effective, either as a means for analyzing privacy risks, or as a means for informing the public, without considering the specific vendor and product being used. And even a PIA conducted early cannot be used as a way to engage multiple stakeholders if it lacks the information necessary for impacted communities and experts to determine how harmful a system

information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.

[50] Jake Wiener, New ICE Privacy Impact Assessment Shows All the Ways the Agency Fails to Protect Immigrants' Privacy, EPIC (Apr. 20, 2023), https://epic.org/new-ice-privacy-impact-assessment-shows-all-the-way-the-agency-fails-to-protect-immigrants-privacy/.

[51] Patrick Grother, Mei Ngan, & Kayee Hanaoka, Face Recognition Vender Test Part 3: Demographic Effects, NIST (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; Patrick Grother, Mei Ngan, & Kayee Hanaoka, *Face Recognition Technology Evaluation (FRTE) Part 2: Identification*, NIST 5 (Feb. 2022), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

[52] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the ICE Use of Facial Recognition Services, DHS/ICE/PIA-054 (May 13, 2020), https://www.dhs.gov/publication/dhsicepia-054-ice-use-facial-recognition-services.

might be. When it comes to third party vendors and third party systems, more disclosure is needed across the board.

III. Role of PIAs in facilitating transparency

EPIC regularly uses PIAs and Privacy Threshold Assessments (PTAs) to learn more about federal agency activities, and to inform the public about the systems federal agencies use. PIAs are a particularly important tool to facilitate greater transparency through well-crafted FOIA requests. But PIAs often fall short when they are not published and easily searchable, fail to contain sufficient detail, are not written with enough context for an average person, and fail to consult stakeholders outside the agency. To improve the transparency function of PIAs, OMB's new guidance should:

1) Set up a single centralized and searchable database for PIAs, or at a minimum require agencies to publish PIAs detailed, searchable agency databases; and
2) Require agencies to complete Privacy Threshold Assessments and proactively publish them.

a) *PIAs are a key tool for non-profits and citizens to inform the public about the risks of federal information collection systems.*

EPIC regularly relies on PIAs in our role as a public interest research center to understand the existence and impact of government systems. PIAs often disclose the existence of an important and potentially harmful system, provide information to craft narrow and effective FOIA requests, and allow for analysis of otherwise opaque federal programs. EPIC regularly refers to PIAs in all aspects of our work, particularly in comments to federal agencies,[53] advocacy before Congress,[54] and analysis we publish to inform the public.[55]

---

[53] *See e.g.*, EPIC Comments to GSA on Modified System of Records Notice for Login.gov (Dec. 21, 2022), https://epic.org/documents/epic-comments-modified-system-of-records-notice-for-login-gov/; EPIC, Consumer Federation of America, and Center for Digital Democracy Comments to OSTP on Public and Private Sector Uses of Biometric Technologies (Jan. 15, 2022), https://epic.org/documents/epic-comments-to-ostp-on-public-and-private-sector-uses-of-biometric-technologies/; EPIC Comments to DHS: Advance Collection of Photos at the Border, USCBP-2021-0038 (Nov. 29, 2021), https://epic.org/documents/epic-comments-to-dhs-advance-collection-of-photos-at-the-border/.

[54] Statement of Jeramie Scott at EPIC to House Committee on Homeland Security Subcommittee on Border Security, Facilitation, & Operations Hearing on "Assessing CBP's Use of Facial Recognition Technology" (July 27, 2022), https://epic.org/wp-content/uploads/2022/07/Testimony-Scott-CBP-FRT-Use-2022.07.27.pdf.

[55] Maria Villegas Bravo, *DHS Disregards Internal Policies and Avoids Fourth Amendment Protections to Track Your Location*, EPIC (Feb. 8, 2024), https://epic.org/dhs-disregards-internal-policies-and-avoids-fourth-amendment-protections-to-track-your-location/; Kiran Wattamwar, *ICE's Privacy Impact Assessment on Surveillance Technologies is an Exercise in Disregarding Reality*, EPIC (Oct. 5, 2023), https://epic.org/ices-privacy-impact-assessment-on-surveillance-technologies-is-an-exercise-in-disregarding-reality/; Jake Wiener, *New ICE Privacy Impact Assessment Shows All the Ways the Agency Fails to Protect Immigrants' Privacy*, EPIC (Apr. 20, 2023), https://epic.org/new-ice-privacy-impact-assessment-shows-all-the-way-the-agency-fails-to-protect-immigrants-privacy/.

PIAs are also a crucial tool in crafting narrow FOIA requests that can uncover further information about federal agency activities. EPIC attorneys regularly consult PIAs when drafting FOIA requests and cite specifically to PIAs in the body of the request. We use PIAs to direct FOIA officers to the proper resources, provide keywords for more efficient searching, and save time by only consulting with the relevant sub-components of an agency. PIAs actually reduce FOIA office workloads by allowing the public to craft narrowly tailored FOIAs that do not require searching voluminous amounts of extraneous documents.

EPIC relied heavily on Immigrations and Customs Enforcement's (ICE) PIA on the agency's use of facial recognition services in drafting a highly impactful FOIA request that uncovered a number of new documents detailing how the agency uses controversial facial recognition technology.[56] ICE's 2020 PIA detailed the different sources for facial recognition technology that ICE agents could access, identified the forthcoming existence of training materials, and revealed that ICE was using commercial vendors to obtain facial recognition technology.[57] EPIC eventually litigated the FOIA request after ICE was unresponsive, resulting in thousands of pages of new documents that help the public understand how ICE was using facial recognition technology during times of significant public concern.[58]

b) *Agencies fail to publish PIAs in an easily useable manner.*

Across the federal government, agencies are not doing enough to make PIAs easily available to the public. At best, agencies publish their PIAs on webpages that are difficult to search and lack key details like the type of data or system involved.[59] The Department of Veterans Affairs (VA) maintains a fairly detailed and searchable list of PIAs, but buries this webpage behind several layers of click-throughs from the agency's main webpage labelled "Privacy Impact Assessment (PIA) Repository".[60] A diligent user can find the VA's PIA page, but the experience is unnecessarily complicated.

More often, agencies publish their PIAs in disorganized lists with little if any information beyond the name of the system.[61] For example, the Department of Justice maintains a scattershot

---

[56] *EPIC v. ICE (Facial Recognition Services)*, EPIC, https://epic.org/documents/epic-v-ice-facial-recognition-services/ (2024).
[57] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the ICE Use of Facial Recognition Services, DHS/ICE/PIA-054 (May 13, 2020), https://www.dhs.gov/publication/dhsicepia-054-ice-use-facial-recognition-services.
[58] *EPIC v. ICE (Facial Recognition Services)*, EPIC, https://epic.org/documents/epic-v-ice-facial-recognition-services/ (2024).
[59] *See e.g.*, *Privacy Impact Assessments (PIA) Collection*, Dep't of Homeland Sec., https://www.dhs.gov/publications-library/collections/privacy-impact-assessments-%28pia%29 (2024); *Privacy Impact Assessment (PIA) Reports*, U.S. Consumer Product Safety Commission, https://www.cpsc.gov/About-CPSC/Agency-Reports/PIA-Reports (2024).
[60] *Privacy Impact Assessment (PIA) Repository*, Dep't of Veterans Affairs
[61] *See e.g.*, *Department of Justice/FBI Privacy Impact Assessments (PIAs)*, Fed. Bureau of Investigation, https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments, (2024); *Privacy Act Information*, Federal Communications Commission, https://www.fcc.gov/managing-director/privacy-transparency/privacy-act-information#pia (2024).

PIA webpage that directly houses some PIAs in PDF form for some agency subcomponents, links directly to the PIA page for other subcomponents like the FBI, and links to the general privacy webpage for still others like the Bureau of Prisons.[62] The FCC and many other agencies maintain similarly deficient PIA webpages. Across the DOJ, subcomponents fail to list when PIAs were conducted alongside the name of the system, making it difficult to know which PIAs are for new systems, which are for legacy systems, and which may be completely outdated. The ordinary citizen coming across DOJ's FOIA page would have no way to figure out which PIAs cover systems that impact their lives, and which cover only internal-facing systems of data on federal employees.

At worst, some agencies don't publish their PIAs at all, providing a list of documents that can be obtained through FOIA requests. The U.S. Postal Service simply provides a downloadable list of its' PIAs (labelled Business Impact Assessments) and directs interested citizens to submit a FOIA request for the PIA in question. [63] It is not clear how often the Postal Service updates their downloadable list of PIAs, making it difficult to determine which systems are still active. The FOIA process is an unnecessarily slow and labor-intensive way to access what should be publicly available documents. OMB should not allow agencies to skirt compliance with the E-Government Act by putting a wall of FOIA procedures between the public and PIAs.

PIAs should be proactively disclosed through a centralized and searchable database that is run by the OMB, similar to regulations.gov. This approach would have myriad benefits. Currently, some federal agencies provide their own databases of PIAs, but centralization would encourage uniform publication of PIAs by all federal agencies.[64] Management by OMB would ensure oversight by a third-party agency. Centralization would encourage economies of scale and thus lead to a more functional and searchable database. Creating a robust database of PIAs would bring more than mere convenience: it would enable the PIA provision of the E-Government Act to fulfill Congress's goals of encouraging agency accountability, public transparency, and public trust. With regulations.gov as a model, OMB could spin up a centralized website that made it easier for agencies to publish PIAs and easier for the public to find them.

In the alternative, agencies should maintain an updated PIA webpage with PIAs available as PDFs. This webpage should be searchable, and PDFs should be able to be filtered by sub-agency, topic, and date of publication. A good example of such a webpage is the Consumer Product Safety Commission's Privacy Impact Assessments repository.[65] OMB should go further than the Consumer Product Safety Commission though and direct agencies to tag PIAs with keywords to allow the public to find the relevant PIAs based on basic types of information collected, e.g. social security number or fingerprints, as well as any advanced technologies the system uses like AI or facial recognition.

---

[62] *DOJ Privacy Impact Assessments*, Dep't of Justice, https://www.justice.gov/opcl/doj-privacy-impact-assessments (2024).
[63] *Privacy Impact Assessments (PIA)*, U.S. Postal Service, https://about.usps.com/who/legal/privacy-policy/privacy-impact-assessments.htm (2024).
[64] *Privacy Impact Assessments (PIA) Collection*, Dep't of Homeland Sec., https://www.dhs.gov/publications-library/collections/privacy-impact-assessments-%28pia%29 (2022); Privacy Impact Assessment (PIA) Reports, U.S. Consumer Product Safety Commission, https://www.cpsc.gov/About-CPSC/Agency-Reports/PIA-Reports (2021).
[65] *Privacy Impact Assessment (PIA) Reports*, U.S. Consumer Product Safety Commission, https://www.cpsc.gov/About-CPSC/Agency-Reports/PIA-Reports (2024)

c) *PTAs should be mandatory for all agencies and published in a timely manner alongside PIAs.*

OMB should direct agencies to follow DHS' model and conduct Privacy Threshold Assessments as a useful exercise for agencies and a transparency tool for the public. The DHS is required to assess and mitigate the privacy risks of the information technology systems and technologies they use through a four-part cycle, beginning with conducting a Privacy Threshold Analysis (PTA).[66] Depending on the results of the PTA, the DHS Privacy Office will reach a conclusion about whether the system or program requires additional privacy compliance documentation, like a Privacy Impact Assessment (PIA).[67] As such, these privacy assessments are crucial for the public to assess how new technologies intrude on the lives of ordinary people. However, the requisite PTAs for many DHS programs have not been released. Without published PTAs, it's nearly impossible for organizations like EPIC to check agencies' work and ensure that PIAs are conducted when necessary.

OMB should direct DHS and other agencies to proactively and consistently disclose PTAs soon after they are completed. PTAs identify privacy concerns and determine whether further privacy assessments are required. The results of PTAs therefore determine whether the public is entitled to disclosure about potentially privacy-threatening programs. Withholding PTAs from the public eye obscures one of the most important steps in the process of implementing or updating system and programs. This secrecy undermines the purpose of Section 208 of the E-Government Act, which is to ensure that "privacy considerations and protections are incorporated into all activities of the Department."[68]

IV. Privacy risks associated with advances in technology and data capabilities

Advancing technology and data capabilities have increased the privacy risks associated with the government's use of information systems and privacy impact assessments have largely not kept up. The increasing use of AI and AI-enabled systems implicate privacy in new ways because they 1) are trained on large amounts of personal data from commercial databases and public records and 2) make inferences and assumptions and produce outputs based on persona data that go beyond the risks associated with collection and dissemination of personal data.[69] These systems are used for

---

[66] *Privacy Compliance Process,* Dep't of Homeland Sec., https://www.dhs.gov/compliance#:~:text=Privacy%20Threshold%20Analysis%20(PTA),-The%20first%20step&text=The%20DHS%20Privacy%20Office%20reviews,or%20when%20changes%2Fupdates%20occur (last updated Jan. 13, 2022).

[67] *Privacy Compliance Process,* Dep't of Homeland Sec., https://www.dhs.gov/compliance#:~:text=Privacy%20Threshold%20Analysis%20(PTA),-The%20first%20step&text=The%20DHS%20Privacy%20Office%20reviews,or%20when%20changes%2Fupdates%20occur (last updated Jan. 13, 2022).

[68] *Privacy Policy Guidance and Memorandum,* Dep't of Homeland Sec., https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-02_0.pdf (last accessed July 11, 2022).

[69] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793, 830–60 (2022) (typologizing different privacy harms); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable*

things like risk scoring, eligibility screening, fraud detection, and predictive policing. The use of commercially available information (CAI) tends to exacerbate privacy risks associated with data collection and undermines constitutional protections that would not allow government agencies to collect the same data directly without a warrant.

AI systems implicate privacy in a number of ways, and it starts with the model training and development. AI systems used by federal agencies are likely to be trained on commercial data that can include consumer data and public records. Since AI systems reflect the data they are trained on, procuring an AI system trained on personal information from commercial data and public records is a data collection of that training data. Allowing these types of AI systems to operate on agency records produce inferences that wouldn't otherwise occur. The accurate inferences may reveal private information about someone without their consent[70] and incorrect inferences can restrict or undermine someone's access to services and opportunities.[71] Additionally, the data collection that occurs to train AI systems can contain historical bias that will then be reflected in AI decisions—perpetuating harmful biases and disproportionately impacting historically marginalized groups.[72]

When the government procures an AI system from a private vendor, it is often the case that the vendor will be the one maintaining the system.[73] Consequently, to operate these systems a government agency will need to transmit government data that includes PII to a vendor through the vendor's web portal. AI vendors may not properly separate government data from its own commercial and proprietary data—commingling sensitive data from the government with commercial datasets that are resold or otherwise transmitted to third parties.

The ways in which PII might be exposed go beyond the government handing it over to an AI vendor. PII can also be exposed through data leaks and security vulnerabilities. An agency might not intend to use an AI system to share PII, but some systems—especially large-language models (LLMs)—may unintentionally leak PII during use. ChatGPT, for example, has exposed people's personal information.[74] Data leaks can also occur when an AI developer fails to secure PII in the training data. Microsoft, for example, accidentally leaked 38TB of data that included passwords and

---

Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, Colum. Bus. Rev., 2019, at 22–28 (exploring overlap between data inferences and personal data).

[70] *See* Citron & Solove, *supra* note 23, at 831–33, 853 (discussing physical harm and lack of control); Wachter & Mittelstadt, *supra* note 23, at 12–19 (discussing automated methods for inferring intimate details about someone's identity and life).

[71] *See* Citron & Solove, *supra* note 23, at 817, 839–41 (discussing reputational harms caused by inaccuracies); Wachter & Mittelstadt, *supra* note 23, at 57 (discussing right to rectify inaccurate inferences).

[72] Grant Fergusson, Outsourced and Automated: How AI Companies Have Taken Over Government Decision-Making, Electronic Privacy Information Center (Sept. 2023), https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf.

[73] *See* EPIC, Screened & Scored in the District of Columbia at 24-25 (Nov. 2022) (describing one such arrangement with Thomson Reuters), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf; Grant Fergusson, *Public Benefits, Private Vendors: How Private Companies Help Run Our Welfare Programs*, EPIC Blog (Jan. 26, 2023), https://epic.org/public-benefits-private-vendors-how-private-companies-help-run-our-welfare-programs/.

[74] Jordan Pearson, *ChatGPT Can Reveal Personal Information From Real People, Google Researchers Show*, Vice (Nov. 29, 2023), https://www.vice.com/en/article/88xe75/chatgpt-can-reveal-personal-information-from-real-people-google-researchers-show.

encryption keys while uploading open-source LLM training data set to Github.[75] In addition to unintended data leaks, many AI systems are vulnerable to jailbreaking. This is particularly true for generative AI where, despite guardrails on generative AI systems to restrict what the system can output, hackers have easily circumvented these guardrails and tricked generative AI systems into outputting PII.[76]

The use of AI requires updated guidance by OMB. First and foremost, OMB should specify that the procurement and use of AI requires a PIA to be conducted. As described above, the procurement and/or use of AI constitutes a new data collection that create some unique privacy risks that PIAs should address. Additionally, OMB should consider incorporating NIST guidance on AI risk management into its PIA guidance. For example, testing AI systems for validity and reliability—and documenting AI system limitations—before they are deployed.[77] Lastly, OMB should mandate specific PIA requirements for AI systems, including: 1) Reporting additional information about the procurement and use of AI systems; 2) Conducting regular AI testing and evaluation processes to identify any errors, biases, vulnerabilities, or privacy risks within AI systems; and 3) Setting interagency privacy risk tolerance threshold based on the NIST AI RMF. For additional details about EPIC's recommendations to integrate AI requirements into PIAs, see EPIC's August 8, 2023 memorandum to OMB attached here as Appendix 1.

Of course, it's not just AI systems that pose a threat to privacy in ways that PIAs, as currently conducted, are ill-equipped to handle. The purposeful collection of massive amounts of personal and sensitive data into commercial databases available for purchase by government agencies and other entities presents its own challenges to privacy. Commercially available information (CAI) includes large amounts of sensitive data that government agencies do not have the resources to collect on their own and could not collect in the first place without a warrant or some other court order. Consequently, CAI not only comes with the traditional privacy concerns associated with the government using PII, it also undermines Constitutional protections that would prevent government agencies from collecting certain data in the first place. In particular, the availability of CAI acts as an end run around the Fourth Amendment, allowing government agencies to purchase data they would otherwise not be able to obtain unless they could justify a warrant for it. This undermines a foundational aspect of our Constitution that protects our privacy and civil liberties. CAI could potentially have a chilling effect on our First Amendment protected rights of religion and association because of the prevalence of location data in CAI that could easily be used to determine who goes to particular places of worship or who associates with who. This may be the case even if government agencies do not use CAI in this way given the public understanding of its availability to the government and knowing the fact that CAI is already used to get around Fourth Amendment requirements.

Additionally, the indiscriminate nature of the data collection related to CAI risks amplifying data quality issues. The scale of the collection poses risk related to data access and abuse. The scaled

[75] David Barry, *Microsoft's AI Data Leak Isn't the Last One We'll See*, Reworked (Sept. 29, 2023), https://www.reworked.co/information-management/microsofts-ai-data-leak-isnt-the-last-one-well-see/.
[76] Mehul Srivastava and Cristina Criddle, *Nvidia's AI software tricked into leaking data* Financial Times (June 9, 2023), https://www.ft.com/content/5aceb7a6-9d5a-4f1f-af3d-1ef0129b0934.
[77] NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 29 (2023).

combined with the indiscriminate nature of the collection risks overcollection. These risks will all likely translate to government agencies who buy large amounts of CAI.

Similar to AI systems, OMB should make clear that the potential purchase of CAI requires a PIA. This should not be left up to interpretation as some agencies have already tried to avoid any privacy compliance when it comes to using CAI.[78] Additionally, OMB needs to make clear that agencies need to consider and address the privacy risks associated with the use of CAI regardless if it directly contains PII. Datasets with sensitive information, even if it is not traditional standalone PII, can easily be used to identify someone. Lastly, PIAs assessing CAI should directly address whether the agency could directly collect the information without a warrant or other court order. If an agency cannot collect it directly itself without a warrant then the agency should not purchase the data to avoid a warrant requirement.

V. Conclusion

Privacy impact assessments have the potential to be a powerful tool of transparency that can anticipate and prevent problems and protect our privacy. But they must be conducted in a timely and thoughtful manner that grapples with the growing privacy risks created by advancing technologies. To do that, EPIC urges OMB to implement recommendations described in this comment. For any further questions please contact EPIC Senior Counsel Jeramie Scott at jscott@epic.org.

A summary of EPIC's recommendations is provided below:

- Recommendations to improve PIAs generally:
  - Conduct PIAs as required and publish them promptly;
  - Conduct PIAs before systems are in place so that PIAs are pre-decisional documents, not post-hoc rationalizations;
  - Produce PIAs that are sufficiently detailed to give the public a full accounting of agency activities and the risks they create; and
  - Fully disclose and evaluate the risks created by using third-party technology and third-party data.

- Recommendations to improve transparency:
  - Set up a single centralized and searchable database for PIAs, or at a minimum require agencies to publish PIAs detailed, searchable agency databases; and
  - Require agencies to complete Privacy Threshold Assessments and proactively publish them.

- Recommendations to improve how PIAs address AI systems:
  - Specify that procurement and use of AI require a PIA to be conducted;

[78] *See* DHS Office of Inspector General, CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data [REDACTED] (Sept. 2023), https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-61-Sep23-Redacted.pdf ; *See also* Maria Villegas Bravo, Blogpost: DHS Disregards Internal Policies and Avoids Fourth Amendment Protections to Track Your Location (Feb. 8, 2024), https://epic.org/dhs-disregards-internal-policies-and-avoids-fourth-amendment-protections-to-track-your-location/.

    - Incorporate relevant NIST guidance on AI risk management into PIA guidance; and
    - Mandate specific PIA requirements for AI systems that include reporting additional information, regular testing and evaluation, and setting privacy risk tolerance threshold based on NIST AI RMF.

- Recommendations to improve how PIAs assess commercially available information:
    - Specify that purchasing CAI requires a PIA first;
    - Make clear that a CAI PIA should be conducted even if there is no traditional PII present in the data; and
    - PIAs for CAI should address whether a warrant or other court order would be required for an agency to directly collect the information and prevent end runs around the Fourth Amendment.

APPENDIX I

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

MEMORANDUM

To: Executive Office of the President, Office of the Vice President, Office of Management and Budget
From: Electronic Privacy Information Center (EPIC)
Date: August 8, 2023
Re: **Integrating AI Requirements Into Section 208 Privacy Impact Assessments**

I. Summary

This memorandum proposes that the White House Office of Management and Budget (OMB) update its Privacy Impact Assessment guidance under Section 208 of the E-Government Act of 2002[1] to include AI impact requirements. This updated OMB guidance would align with a May 4, 2023, statement from the White House announcing new initiatives for regulating how federal agencies use emerging AI tools, including new OMB policy guidance on the U.S. government's use of AI systems.[2] This memo proceeds as follows:

1. **AI Impacts are Privacy Impacts.** Section II of this memo explains that AI systems implicate the same privacy and data collection concerns at the core of Section 208. AI systems process and use personal data, so AI impact requirements are natural extensions of existing Privacy Impact Assessment requirements.

2. **Section 208 Encompasses the Procurement and Use of AI Systems.** Sections III and IV describe the contours of OMB's statutory authority, including current Privacy Impact Assessment requirements. Crucially, the "information technology" covered by Section 208 encompasses government AI systems, so the OMB is empowered to incorporate AI impact requirements within its Privacy Impact Assessment guidance.

3. **AI Impact Requirements Align with the Biden-Harris Administration's Broader Policy Goals.** Section V describes recent White House efforts to prioritize responsible AI development and use, highlighting ways in which AI impact requirements in Privacy Impact Assessments would mirror recommendations by the Biden-Harris Administration and the National Institute of Standards and Technology.

---

[1] 44 U.S.C. § 3501 note.
[2] Press Release, White House, FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety (May 4, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/.

4. **AI Impact Requirements Could Include Increased Reporting Requirements, Regular AI System Audits to Identify Privacy Risks, and Setting an Interagency Risk Tolerance Threshold to Manage Risky AI Systems.** Because the OMB has discretion over the exact content of Privacy Impact Assessments, Section VI proposes that the OMB clarify that Section 208 covers AI systems, incorporate NIST's recent AI Risk Management Framework, and pursue specific AI reporting and testing requirements when updating its Privacy Impact Assessment guidance under Section 208.

II. Government AI Use Implicates Personal Privacy Concerns

The impacts of government AI use and those of government personal data collection are not wholly distinct. Rather, many forms of AI systems used by government—including automated decision-making systems—rely on personal data in ways that implicate the same privacy concerns as those protected by Privacy Impact Assessments under Section 208 of the E-Government Act.

First, many AI systems used by government agencies rely on datasets that include personally identifiable information.[3] To develop these AI systems—which encompass everything from eligibility screening algorithms[4] and fraud detection systems[5] to police face surveillance systems[6] and beyond—AI companies train their AI models on scores of personal data taken from commercial databases and public records. When government agencies use AI systems, they once again feed personal data from government or commercial databases into these systems to produce outputs like risk scores, eligibility determinations, and identification determinations—outputs that depend on the storage, processing, and use of personal data. In sum, AI systems are valuable because they can analyze and make predictions about people based on available data, not simply in their ability to automate a process.[7]

Second, the inferences, assumptions, and outputs that AI systems produce based on personal data may produce privacy harms *beyond* those attributable to the collection and dissemination of personal data.[8] When AI inferences are accurate, for example, they reveal private information about someone without their consent—information that may be misused by

[3] *See, e.g.*, EPIC, Screened & Scored in the District of Columbia 4–6, 8, 15, 20–25 (2022) [hereinafter "Screened & Scored Report"].
[4] *Id.* at 27–28.
[5] Screened & Scored Report at 24–25.
[6] *See Face Surveillance and Biometrics*, EPIC, https://epic.org/issues/surveillance-oversight/face-surveillance/ (last visited July 31, 2023).
[7] *See* Daniel Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 Nw. U. L. Rev. __ (forthcoming 2024).
[8] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793, 830–60 (2022) (typologizing different privacy harms); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, Colum. Bus. Rev., 2019, at 22–28 (exploring overlap between data inferences and personal data).

those who can access it.[9] When AI inferences are wrong, they perpetuate errors in automated decisions that can restrict or undermine someone's access to services and opportunities like jobs or public benefits.[10] In either case, government agencies' use of AI inferences may weave historical biases about race, economic status, gender, and ability into life-altering government decisions.

Lastly, government AI systems may disclose personal information to third parties while processing data. Many government AI systems are not built internally, but rather procured from private vendors who develop and maintain the technologies.[11] The personal data that government agencies feed into these AI systems does not always stay within the government. Rather, AI vendors who maintain these systems often require that the personal data within an agency's possession be shared, combined with a vendor's proprietary data, or compared to public and commercial databases.[12] To use many AI systems, then, government agencies are *required* to disseminate personal and government data to private vendors.[13]

Ultimately, AI systems not only rely on the collection, use, and dissemination of personal data, but also perpetuate any errors or biases found in that data. Their procurement and use directly implicates the same privacy concerns at the core of Section 208 of the E-Government Act.[14]

III. Section 208 of the E-Government Act of 2002 Requires Federal Agencies to Regularly Conduct Privacy Impact Assessments

In an effort to protect the privacy of personal information collected, maintained, and disseminated by federal agencies, Congress passed Section 208 of the E-Government Act in 2002.[15] Under Section 208(b)(1), every federal agency is required to conduct, review, and (if feasible) publish a Privacy Impact Assessment *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.[16] These Privacy Impact Assessments must include, at minimum:

1. What information that will be collected;
2. The reason for collection;

---

[9] *See* Citron & Solove, *supra* note 8, at 831–33, 853 (discussing physical harm and lack of control); Wachter & Mittelstadt, *supra* note 8, at 12–19 (discussing automated methods for inferring intimate details about someone's identity and life).
[10] *See* Citron & Solove, *supra* note 8, at 817, 839–41 (discussing reputational harms caused by inaccuracies); Wachter & Mittelstadt, *supra* note 8, at 57 (discussing right to rectify inaccurate inferences).
[11] *See* Grant Fergusson, *Public Benefits, Private Vendors: How Private Companies Help Run Our Welfare Programs*, EPIC Blog (Jan. 26, 2023), https://epic.org/public-benefits-private-vendors-how-private-companies-help-run-our-welfare-programs/.
[12] *See id.*; Screened & Scored Report at 24–25 (describing one such arrangement with Thomson Reuters).
[13] *See* 44 U.S.C. § 3501 note at 208(b)(1)(A) (mandating Privacy Impact Assessments when an agency procures or uses information technology that disseminates personal information).
[14] *Id.* at 208(a).
[15] *Id.*
[16] *Id.* at 208(b)(1)(A)–(B).

3. The agency's intended use of the information;
4. Information about who the information will be shared with;
5. Information about the "notice or opportunities for consent [that] would be provided to individuals regarding what information is collected and how that information is shared;"
6. How the information will be secured; and
7. "[W]hether a system of records is being created under [the Privacy Act, 5 U.S.C. § 552a]."[17]

Although Section 208 dictates that Privacy Impact Assessments must include these minimum requirements, the OMB is also directed to provide guidance on the specific contours of Privacy Impact Assessments, including guidance requiring agencies to include other information within their Privacy Impact Assessments[18] and guidance that requires agencies to conduct Privacy Impact Assessments on already existing information systems or ongoing information collection efforts.[19]

IV. The Text of Section 208 Permits the OMB to Incorporate AI Impact Requirements Within its Privacy Impact Assessment Guidance

Section 208 requires the OMB to issue guidance specifying the contents of Privacy Impact Assessments. But while Section 208's statutory language dictates *minimum* requirements for Privacy Impact Assessments, it grants the OMB broad authority to determine the *exact* contents of Privacy Impact Assessments. The OMB is directed to ensure that all Privacy Impact Assessments address a minimum set of questions about the information collection or technology listed above,[20] and the guidance must "ensure that a Privacy Impact Assessment is commensurate with the size of the information system being assessed, the sensitivity of the information that is in an identifiable form in that system, and the risk of harm form unauthorized release of that information."[21] Beyond these directions, the OMB is granted broad discretion over the substance and form of Privacy Impact Assessments.[22] The only strict limitation on the OMB's guidance relates to the timing of Privacy Impact Assessments: agencies can only be required to complete a Privacy Impact Assessment while (1) "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form,"[23] (2) "initiating a new collection of information,"[24] or (3) continuing to collect personally identifiable information or use existing information technology.[25]

The term, "information technology," used in Section 208 can encompass AI systems. The definition of the term in Section 208, as incorporated within OMB guidance, is borrowed from the Clinger-Cohen Act of 1996, which defines "information technology" as:

[17] *Id.* at 208(b)(2)(B).
[18] *Id.* at 208(b)(2)(B).
[19] *Id.* at 208(b)(3).
[20] *Id.* at 208(b)(2)(B)(ii).
[21] *Id.* at 208(b)(2)(B)(i).
[22] *Id.* at 208(b)(3).
[23] *Id.* at 208(b)(1)(A)(i).
[24] *Id.* at 208(b)(1)(A)(ii)
[25] *Id.* at 208(b)(3)(C).

> "[A]ny equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, movement, control, display, switching, interchange, transmission, or reception of data or information by [an] executive agency... [including] computers, ancillary equipment… software, firmware[,] and similar procedures, services (including support services), and related resources."[26]

No matter their form, the value of AI systems is in their use as tools to collect, maintain, process, analyze, or otherwise manipulate data. Most government AI systems operate as software, AI-enabled equipment, or AI services provided by vendors. Therefore, when an AI system is procured or used to process, store, or analyze personal data, it would fall cleanly within the definition of "information technology" covered under Section 208's Privacy Impact Assessment requirement.

A government agency's use of existing AI systems in new, distinct efforts to collect, store, process, or disseminate personal data can trigger Section 208's Privacy Impact Assessment requirement as well. As described above, agencies are required to complete a Privacy Impact Assessment not only when developing or procuring new information technology, but also when applying information technology to a new or ongoing collection of information. Although the term, "collection of information," is not defined in either Section 208 or the Clinger-Cohen Act, the inclusion of the phrase "ongoing collections of information"[27] within Section 208 suggests that a "collection of information" describes a distinct *effort* to collect data for a specific purpose, rather than each discrete *instance* of data collection. Further, the separation between Section 208(b)(1)(A)(i), which covers the development and procurement of information technology, and Section 208(b)(1)(A)(ii), which covers the initiation of new collections of information, suggests that a new collection of information need not be accompanied by the development or procurement of new information technology to trigger a Privacy Impact Assessment. In fact, Section 208(b)(3) grants the OMB discretion to impose Privacy Impact Assessments for existing information technologies *regardless* of how they are used. When agencies use existing AI systems to collect, store, process, use, or disseminate personal data, the OMB has clear statutory authority to require Privacy Impact Assessments.

Additionally, OMB guidance incorporating AI impact requirements within Privacy Impact Assessments can apply retroactively to AI systems already procured and used by federal agencies. Under Section 208(b)(3)(C) of the E-Government Act, the Director of the OMB is *mandated* to require that federal agencies "conduct Privacy Impact Assessments of existing information systems or ongoing collections of information that is in an identifiable form" if the Director determines that such an assessment would be appropriate.[28] Assuming that AI systems fall within Section 208's definition of "information technology" and new efforts to collect, store, process, or disseminate personal data using AI systems falls within the definition of "collection of information," then the Section 208(b)(3)(C) appears to permit the OMB to require agencies to

[26] 40 U.S.C. § 11101(6); *see also* OMB Circular No. A-130.
[27] Section 208(b)(3)(C).
[28] *Id.*

conduct new Privacy Impact Assessments—including AI impact requirements—for their existing AI systems and any ongoing collections of information that involve AI systems.

Finally, current OMB guidance around Privacy Impact Assessments is compatible with AI impact requirements. The most recent OMB guidance concerning Privacy Impact Assessments, OMB Circular No. A-130, defines "Privacy Impact Assessment" as encompassing determinations of the "risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system" as well as evaluations of "protections and alternate processes for handling information to mitigate potential privacy concerns."[29] The Privacy Impact Assessment should include both an analysis of these requirements and a "formal document detailing the process and the outcome of the analysis."[30]

Because the electronic information systems used to collect, use, process, and disseminate data within OMB Circular A-130 includes information technology under Section 208—and because information technology appears to include A.I. software and vendor services—existing OMB guidance is compatible with a requirement to assess the risks and effects of A.I. systems used by federal agencies to collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information. In fact, many of the specific requirements outlined in OMB Circular A-130 align with existing proposals for AI risk management frameworks. [31] Even the format of these Privacy Impact Assessments—including both a substantive analysis and an accounting of the process and outcome of the analysis—aligns with several reporting and transparency recommendations within existing AI risk management proposals.[32] Together, the text of Section 208 and the text of existing OMB guidance provides a strong basis for including AI impact requirements within Privacy Impact Assessments.

V. Incorporating AI Impact Requirements within Privacy Impact Assessments Aligns with the Biden-Harris Administration's National AI Strategy

Over the past year, the Biden-Harris Administration has taken several steps to incorporate greater AI oversight into the federal government. For example, in October 2022, the White House Office of Science and Technology Policy (OSTP) published its Blueprint for an AI Bill of Rights, which established five guiding principles for AI development and use: safe and effective

[29] OMB Circular No. A-130 at 34. The term, "electronic information system," used in this OMB Circular is derived from the definition of "information system" in 44 U.S.C. § 3502, described as "a discrete set of information resources [including information technology] organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." 44 U.S.C. § 3502(8).
[30] *Id.*
[31] *See, e.g.*, NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) 7–9, 21–33 (2023) (discussing risk prioritization and proposing various steps to measure and manage AI risks) [hereinafter "NIST AI RMF"]; IEEE SA, Standard for the Procurement of Artificial Intelligence and Automated Decision Systems, P3119 (forthcoming 2024) (providing rubric for assessing different AI solutions throughout government procurement and use lifecycle); *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at 12–16, COM (2021) 206 final (Apr. 21, 2021) (summarizing AI risk assessment and reporting requirements under the E.U. Artificial Intelligence Act).
[32] *Id.*

systems; algorithmic discrimination protections; data privacy; notice and explanation; and human alternatives, consideration, and fallback.[33] For each principle, the OSTP included several AI assessment measures that could be incorporated within Privacy Impact Assessments as well. These measures include but are not limited to:

1. Pre-deployment testing to mitigate AI risks, including those that stem from the improper collection, use, or dissemination of personal data;[34]
2. Independent evaluations of each AI system's safety and effectiveness for its intended use(s), which the results of any evaluations made public whenever possible;[35]
3. Proactive equity assessments of AI systems, including assessments of the representativeness of data used to train the system;[36] and
4. Extending privacy protections for personal data to related inferences made by AI systems.[37]

In May 2023, the Biden-Harris Administration expanded its efforts to advance responsible AI use by announcing an updated roadmap for AI research and development, as well as an OSTP-led effort to identify national AI priorities.[38] As part of its updated roadmap, the Administration included several strategies for mitigating privacy harms within AI systems that mirror the privacy concerns at the core of Section 208's Privacy Impact Assessments. These strategies include but are not limited to:

1. Developing approaches to mitigate the ethical, legal, and social risks of AI systems, including by advancing AI explainability efforts and investing in privacy-enhancing technologies like homomorphic encryption, differential privacy, and secure multiparty computation;[39]
2. Developing shared public datasets to train and test AI systems without revealing confidential or otherwise personally identifiable information;[40]
3. Developing standards for auditing and monitoring AI systems, including audits for privacy risks;[41] and

[33] OSTP, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People 5–7 (2022).
[34] *Id.* at 5, 15–16.
[35] *Id.* at 5, 15, 20.
[36] *Id.* at 5, 23, 26.
[37] *Id.* at 6, 30.
[38] Press Release, White House, FACT SHEET: Biden-Harris Administration Takes New Steps to Advance Responsible Artificial Intelligence Research, Development, and Deployment (May 23, 2023), https://www.whitehouse.gov/ostp/news-updates/2023/05/23/fact-sheet-biden-harris-administration-takes-new-steps-to-advance-responsible-artificial-intelligence-research-development-and-deployment/.
[39] Select Comm. on A.I., Nat'l Sci. & Tech. Council, National Artificial Intelligence Research and Development Strategic Plan 2023 Update vii, 12–14 (2023).
[40] *Id.* at 18–20.
[41] *Id.* at 26.

4. When needed, providing private individuals or entities with access to data through secure government platforms.[42]

Several of these AI risk management strategies were reflected in the White House's July 2023 announcement that it had secured voluntary AI commitments from seven leading AI companies, including commitments to independently test AI systems for cybersecurity and privacy risks and publicly report the capabilities, limitations, and proper uses of AI systems.[43] However, more can be done to extend the Biden-Harris Administration's efforts to government AI use—and the OMB is well-positioned to implement the Biden-Harris Administration's national AI priorities.

Many of the AI oversight policies championed by the Biden-Harris Administration already mirror existing OMB guidance. Under OMB Circular A-130, for example, agencies are required to, *inter alia*, (1) develop a plan for replacing or retiring information systems that can be appropriately secured against privacy risks; (2) "regularly review and address risk regarding process, people, and technology; (3) "limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of [personally identifiable information] to that which is legally authorized, relevant, and reasonably deemed necessary;" and (4) "protect information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information."[44] While some of the Administration's AI policy priorities will require additional government efforts, several policy provisions concerning the testing, evaluation, and reporting of AI systems can be incorporated into Privacy Impact Assessments under Section 208. Incorporating AI impact requirements within Privacy Impact Assessments would not extend OMB guidance beyond what Section 208 allows, but rather align OMB guidance with broader governmental priorities around privacy and AI systems.

VI. AI Impact Requirements Could Include Increased Reporting Requirements, Regular AI System Audits to Identify Privacy Risks, and Setting an Interagency Risk Tolerance Threshold to Manage Risky AI Systems

The text of Section 208 empowers the OMB to incorporate AI impact requirements into its guidance surrounding Privacy Impact Assessments. However, the OMB has discretion to determine the exact shape and extent of these requirements. This section suggests three steps that OMB could take to incorporate AI impact requirements within the OMB's Privacy Impact Assessment guidance.

First, OMB should issue explicit guidance to agencies clarifying that existing Privacy Impact Assessment requirements extend to the procurement and use of AI systems. Under

[42] *Id.* at 19.
[43] Press Release, White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.
[44] OMB Circular No. A-130 at 6, 17–18.

Section 208 and OMB Circular A-130, an agency is required to conduct a Privacy Impact Assessment whenever it "develops, procures, or uses information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of [personally identifiable information]."[45] These Privacy Impact Assessments must analyze how personal data is handled, determine the privacy risks associated with an information system or activity, evaluate ways to mitigate privacy risks, and detail the process and outcomes of each analysis.[46] Moreover, each Privacy Impact Assessment is meant to be "living document that agencies are required to update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology."[47] By clearly stating that the procurement and use of AI systems that collect, process, use, or disseminate personal data falls within the scope of an agency's Privacy Impact Assessment obligations under Section 208, the OMB can capture several AI impact requirements automatically, such as analyses of how an AI system uses personal data, determinations of the privacy risks associated with an AI system, and evaluations of the ways to mitigate an AI system's privacy risks.

Second, OMB could incorporate NIST guidance on AI risk management into its Privacy Impact Assessment guidance. OMB Circular A-130 already leverages NIST standards like the Federal Information Processing Standards (FIPS) and NIST Special Publications from the 500, 800, and 1800 series.[48] By incorporating assessment, documentation, and reporting recommendations from NIST's AI Risk Management Framework (AI RMF)[49] into its Privacy Impact Assessment guidance, for example, OMB can rapidly incorporate specific AI impact requirements into Privacy Impact Assessments without extending beyond its statutory authority under Section 208. Examples of NIST AI RMF recommendations that could be incorporated within Privacy Impact Assessments include but are not limited to:

- Establishing processes and procedures for decommissioning AI systems safely and in a manner that does not increase risks or decrease the agency's trustworthiness;[50]
- Documenting information about an AI system's knowledge limits and how system output may be utilized and overseen by humans;[51]
- Documenting AI training and testing datasets, evaluation metrics, and other testing procedures;[52]
- Testing AI systems for validity and reliability—and documenting AI system limitations—before they are deployed;[53]

[45] *Id.* at 74–75 (Appendix II).
[46] *Id.*
[47] *Id.*
[48] *Id.* at 6.
[49] NIST AI RMF at 21–34.
[50] *Id.* at 23.
[51] *Id.* at 26.
[52] *Id.* at 29.
[53] *Id.*

- Regularly evaluating AI systems for privacy and safety risks based on a predetermined agency risk tolerance;[54]
- Incorporating resource constraints into AI system management determinations such that agencies do not procure or use AI systems they cannot adequately oversee;[55] and
- Communicating AI privacy incidents and errors to relevant authorities and affected communities.[56]

NIST's AI RMF is the result of a Congressional mandate, several years of careful consideration, and consultations with a wide range of stakeholders. The OMB can and should incorporate key recommendations from the AI RMF into its Privacy Impact Assessment guidance to align its efforts with existing standards and broader government efforts to oversee AI use.

Third, in line with both White House and NIST guidance on AI, the OMB could mandate specific AI impact requirements within Privacy Impact Assessments that are tailored to the statutory contours of Section 208 of the E-Government Act. At minimum, EPIC recommends incorporating three such requirements:

1. Reporting additional information about the procurement and use of AI systems, including:
    a. The intended purpose and proposed use of an AI system;
    b. What decision(s) the AI system is making or supporting;
    c. The role that the AI system plays in making the decision;
    d. The AI system's intended benefits and research supporting the benefits;
    e. The AI system's capabilities, including capabilities outside the scope of its intended use, as well as uses for which it is not appropriate;
    f. An assessment of the relative benefits, costs, and risks to the public given the system's purpose, capabilities, and probable use cases;
    g. The inputs and logic of the AI system;
    h. The data or inputs used to train and test the AI system;
    i. Any testing and evaluation methods the agency intends to use, including the frequency of testing and any results or findings produced.

2. Conducting regular AI testing and evaluation processes to identify any errors, biases, vulnerabilities, or privacy risks within AI systems, including, where applicable, evaluations of the representativeness of training data, the validity of AI system outputs across different use contexts, and any changes in AI system outputs that may indicate a degradation in the accuracy or reliability of the AI system.

3. Setting an interagency privacy risk tolerance threshold based on the NIST AI RMF and updated to reflect ongoing agency testing and evaluation of AI systems, such that

[54] *See id.* at 30.
[55] *Id.* at 32.
[56] *Id.* at 33.

agencies would be prohibited from using AI systems that exhibit an excessive level of risk to the data security or privacy of individuals. EPIC has previously identified at least two AI systems—emotion recognition systems and one-to-many facial recognition systems—as exhibiting excessive levels of risk to individuals' privacy.[57]

VII. Conclusion

Section 208 is one of only one of many tools necessary to ensure responsible and effective government use of AI systems. AI impact assessments and reporting requirements are an effective way to mitigate AI risks, but they are not a full regulatory solution to the ongoing and emerging risks that AI systems bring. Formal restrictions, federal procurement guidelines, and explicit prohibitions on high-risk AI systems and use cases are also necessary to ensure the AI systems that federal agencies procure and use are trustworthy and effective.

[57] *See, e.g.*, EPIC, Comments on FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 98–108, 87 Fed. Reg. 51273 (Nov. 21, 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.