

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Administrative Conference of the United States

Disclosure of Agency Legal Materials

87 Fed. Reg. 30,455

July 18, 2022

The Electronic Privacy Information Center (EPIC) submits these comments in response to the request for comment by the Administrative Conference of the United States (ACUS) on Disclosure of Agency Legal Materials.¹ ACUS is “requesting public input on what legal materials agencies must or should make publicly available and how they ought to do so.”² Following the comment process, ACUS plans to have a team of scholars draft a report on the issue, and the agency may propose recommendations to Congress to improve access to agency records.

EPIC has a long history of advocating for open government and transparency,³ and EPIC commends ACUS for seeking to streamline, clarify, and broaden public access to agency legal materials. EPIC frequently uses open records laws to obtain information from the government about surveillance and privacy policy.⁴ Open government laws such as the Freedom of Information Act (FOIA), the Federal Register Act, the Federal Records Act, the E-Government Act, and other agency

¹ 87 Fed. Reg. 30,455, <https://www.federalregister.gov/documents/2022/05/19/2022-10749/disclosure-of-agency-legal-materials-comment-request>.

² *Id.*

³ *Open Government*, EPIC, <https://epic.org/issues/open-government/>, for a list of EPIC’s Freedom of Information Act cases see https://epic.org/?s=&_content-type=foia-cases.

⁴ *Id.*

and program specific open government laws promote government transparency and accountability and enable the public to stay informed about government decisions and actions.

ACUS has an opportunity to strengthen the efficiency, clarity, and scope of open records laws by recommending that the public should have convenient access to a broad range of agency legal materials.

Question 1: What types of agency records should ACUS consider to be “agency legal materials” for purposes of this project?

ACUS should adopt a broad interpretation of the term “agency legal materials.” This term should encompass all records generated by agencies that impose legal obligations, determine rights or interests of parties, provide notice of agencies’ interpretation of the statutes and rules they administer, advise the public of when agencies plan to exercise discretionary powers, and explain other agency legal actions that impact the public. ACUS should interpret the term as broadly as possible so that the public is aware of agencies’ legal decisions and actions. Agencies should not be permitted to make legal decisions or take legal action in secret; thus, ACUS should recommend that all agency legal materials are affirmatively made available to the public.

A broad interpretation of “agency legal materials” is consistent with the purpose of open records laws. The Supreme Court has repeatedly emphasized the value of open records laws, explaining that “[t]he basic purpose of [the] FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.”⁵ The Biden administration has also pledged to make government transparency a top priority.⁶ Agencies should not make legal decisions or take legal actions in secret

⁵ *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978).

⁶ *Press Briefing by Press Secretary Jen Psaki* (Jan. 20, 2021), <https://www.whitehouse.gov/briefing-room/press-briefings/2021/01/20/press-briefing-by-press-secretary-jen-psaki-january-20-2021/>; *Presidential Memorandum on Revitalizing America’s Foreign Policy and National Security Workforce, Institutions, and Partnerships* (Feb. 4, 2021), <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/04/memorandum-revitalizing-americas-foreign-policy-and-national-security-workforce-institutions-and-partnerships>.

because doing so undermines the public’s ability to “know ‘what their Government is up to,’”⁷ which the Supreme Court has said “defines a structural necessity in a real democracy.”⁸

Organizations like EPIC and members of the public rely on open records laws to engage in government oversight and keep the government accountable for its actions. ACUS should recommend that agencies publish a broad range of legal materials in a manner that is easily accessible to the public. Doing so will promote transparency and accountability, which in turn will affirm the legitimacy of agency decisions and decision-making processes.

Question 2: What obstacles have you or others faced in gaining access to agency legal materials?

Significant obstacles stand in the way of EPIC and many others who attempt to gain access to agency legal materials through FOIA requests. The problems with FOIA compliance are numerous and well-documented. In a recent Senate Judiciary Committee hearing on FOIA compliance, there was bipartisan consensus that FOIA is broken.⁹ Specifically, EPIC has encountered three main challenges in accessing agency legal materials: (1) agencies’ failure to produce documents in a timely manner; (2) agencies’ lack of resources to process FOIA requests; and (3) agencies’ overuse of FOIA exemptions and issues with the scope of the search.

I. Agencies do not produce records fast enough to inform public debate.

The primary obstacle EPIC and others face in accessing agency materials is the sheer amount of time it takes for agencies to fulfill FOIA requests. In 2020, agencies took an average of 97 days to process FOIA requests, which is eight days longer than in the previous year.¹⁰ This lack of timely access to records undermines FOIA’s central purpose: to provide the public a way to stay informed

⁷ *NARA v. Favish*, 541 U.S. 157, 171–72 (2004) (quoting *DOJ v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 773 (1989))

⁸ *Id.* at 172.

⁹ Josh Gerstein, ‘*There Is a Big Problem*’: *Senators Unite to Slam FOIA Compliance*, POLITICO (Mar. 29, 2022), <https://www.politico.com/news/2022/03/29/senators-foia-woes-00021324>.

¹⁰ *Freedom of Information Act Requests in FY2020: By the Numbers*, Cong. Res. Serv. (Oct. 26, 2021), <https://crsreports.congress.gov/product/pdf/IF/IF11955> [hereinafter “FOIA by the Numbers”].

about what the government is doing and hold government officials accountable.¹¹ Agencies routinely take months or years to fulfill FOIA requests. For example, EPIC received documents this year in response to a FOIA request it filed with the Coast Guard in 2014. This eight-year wait for documents—which is not out of the ordinary—does not allow the public to stay informed about what their government is doing nor is it in line with Congress’ intent in enacting FOIA.

Delays in completing FOIA requests also contribute to a massive FOIA backlog. This backlog continues to grow year after year. It increased 17.7% to 142,000 backlogged requests from the end of 2019 to the end of 2020.¹² Agencies’ failure to comply with FOIA requirements that they proactively release certain documents also contributes to this backlog.¹³ A 2021 report from the Government Accountability Office found that 25 of 118 agencies completed zero proactive disclosures in 2018 or 2019.¹⁴ Because agencies are failing to proactively release documents, the public must submit FOIA requests to obtain them. These unnecessary requests add to the FOIA backlog and result in longer wait times for other documents, both of which could be lessened by agencies complying with proactive disclosure requirements.

Another issue closely tied to delays in fulfilling FOIA requests is that agencies will attempt to close old outstanding FOIA requests after failing to produce responsive documents. Agencies will often send a letter to requesters who have not yet received documents years after they filed their requests asking whether they are still interested in the documents. These letters—which have no basis in the text of the FOIA—require the requester to send a response within 30 days if they are still interested in the documents; if the requester does not respond, the agency will close out the request

¹¹ *What is FOIA?*, FOIA.gov, <https://www.foia.gov/about.html>.

¹² Office of Info. Pol’y, Dep’t of Justice, *Summary of Annual FOIA Reports for Fiscal Year 2020* at 1, 9, <https://www.justice.gov/oip/page/file/1436261/download> [hereinafter “Summary”].

¹³ 5 U.S.C. § 552(a)(2).

¹⁴ *Freedom of Information Act: Actions Needed to Improve Agency Compliance with Proactive Disclosure Requirements*, Gov’t Accountability Office 1, 17 (Mar. 2021), <https://www.gao.gov/assets/gao-21-254.pdf>.

without having completed the search or released any materials. For example, EPIC received one of these letters in 2018 regarding its request to the Coast Guard, so in addition to having to wait eight years for the requested documents, EPIC also had to take proactive steps to ensure the Coast Guard did not close out the request without producing any documents.¹⁵ This practice shifts the burden back onto the requester, allowing the agencies to close old FOIA requests without having fulfilled their legal obligation to provide materials to the public.

II. Agencies lack funding to fulfill their open records obligations.

The second main obstacle EPIC faces in accessing agency records is that agencies lack the resources to efficiently complete the FOIA requests they receive. Chronic underfunding contributes to the growing backlog of FOIA requests and results in longer wait times to receive requested documents. For example, the Department of Justice is consistently one of agencies that receives the highest number of FOIA requests.¹⁶ Yet in 2019, the DOJ dedicated only three-tenths of 1% of its annual budget to completing FOIA requests.¹⁷ A general sentiment that dealing with FOIA requests is not part of an agency's primary job also contributes to this lack of funding and inattention paid to requests for information.¹⁸

III. Agencies comply with the letter, but not the spirit of the open records law.

Finally, the third obstacle EPIC faces is agencies conducting insufficient searches to locate the requested materials and improperly withholding information by overusing FOIA exemptions and overclassifying documents. Agencies frequently withhold information by claiming it falls under exception 7 for law enforcement records, particularly the (7)(E) exemption for law enforcement

¹⁵ Letter from USCG FOIA Coordinator to EPIC (Aug. 28, 2018), <https://epic.org/wp-content/uploads/2022/07/EPIC-14-08-01-USCG-FOIA-20180829-Continued-Interest-Letter.pdf>.

¹⁶ FOIA by the Numbers, *supra* note 10.

¹⁷ *The Increase in FOIA Lawsuits Isn't the Problem—It's Agencies Underfunding Their Transparency Obligations*, Am. Oversight (Mar. 17, 2020), <https://www.americanoversight.org/the-increase-in-foia-lawsuits-isnt-the-problem-its-agencies-underfunding-their-transparency-obligations>.

¹⁸ *Id.*

techniques. Exemption 7 accounted for 54.32% of all cited exemptions.¹⁹ Exemption 5, the deliberative process exception, is also frequently used to withhold materials, accounting for almost 7% of all exemptions.²⁰ Despite accounting for this comparatively small volume of exemptions, Exemption 5 is regularly abused. Agencies overuse this exemption and stretch it to cover more documents than it was intended to cover, often inappropriately citing it to withhold documents that would show the agency's stance on certain relevant issues.²¹ While there are valid uses of the FOIA exemptions, agencies abuse these exemptions to withhold information that can and should be released to the public.

Agencies also regularly overclassify documents and fail to declassify documents that could be released. In general, overclassification harms government transparency and reduces the amount of information to which the public has access. This problem has persisted for many decades.²² In 1989, a former U.S. Solicitor General wrote in a Washington Post op-ed that “there is massive overclassification,” and the issue remains today.²³ In 2016, a former director of the Information Security Oversight Office testified to Congress that overclassification is “rampant” and that “the opaque nature of the classification system can give the government a unilateral and almost insurmountable advantage.”²⁴ Reforming the classification system would improve transparency both on its own and in relation to FOIA. Similar to agencies' failure to proactively release documents, this routine overclassification also contributes to the FOIA backlog by forcing the public to file FOIA requests for documents that should already be public. Reducing the number of documents that are

¹⁹ *Id.*

²⁰ *Id.*

²¹ Nick Schwellenbach & Sean Moulton, *The “Most Abused” Freedom of Information Act Exemption Still Needs to Be Reined in*, Project on Gov't Oversight (Feb. 6, 2020), <https://www.pogo.org/analysis/2020/02/the-most-abused-foia-exemption-still-needs-to-be-reined-in>.

²² Adelia Henderson & Gabe Rottman, *Overclassification Is an Even Bigger Problem in an Age of Leak-Hunting*, Reporters Comm. for Freedom of the Press (Aug. 26, 2019), <https://www.rcfp.org/overclassification-bigger-problem-leak-hunting/>.

²³ *Id.*

²⁴ *Id.*

overclassified would remove a significant challenge the public faces in obtaining access to agency legal documents.

Alongside overuse of exemptions, agencies often conduct inadequate searches for information. When responding to FOIA requests, agencies often do not indicate where they have searched for the information. Without knowing what databases were searched or what the search parameters were, there is no way for a requester to know if the agency has completed a thorough search for the materials requested. This lack of information about the search itself is another obstacle that EPIC and others have faced in gaining access to agency legal materials.

Question 3: Are there certain types of agency legal materials or legal information that agencies are not making publicly available that would be valuable to you or others?

ACUS should require the release of certain types of agency decision-making documents and legal information not currently publicly available to preserve transparency and accountability in executive actions. Without proactive release of these materials, organizations like EPIC must use open records laws to request documents that explain key government decisions and actions—requests that are sometimes not addressed in a timely or responsive manner.²⁵ Delays or refusals to release information undermine public confidence in agencies and allow agencies to rely on secret justifications for executive actions and act in ways invisible to the public eye. Releasing a wider range of documents to the public promotes transparency and trust in federal agencies and strengthens our constitutional order. EPIC has identified a non-exhaustive list of documents that we urge ACUS to require agencies to release for public knowledge on a regular basis.

I. OLC Legal Opinions

Public disclosure of opinions made by the Office of Legal Counsel (OLC) in the Department of Justice (DOJ) is essential. The OLC writes legal opinions that are used to justify major policy

²⁵ See, e.g., *EPIC v. CBP Complaint for Injunctive Relief*, EPIC (2021), <https://epic.org/wp-content/uploads/2021/10/1-Complaint.pdf>.

decisions or executive actions in two formats: “formal opinions” and “informal advice.” Both create the legal basis for executive actions and follow a formal approval process. In the interest of government transparency, both should be disclosed regardless of format. The DOJ itself has endorsed a more transparent approach to OLC opinions, writing a statement in October 2020 that supported publishing final OLC opinions; disclosing to Congressional committees OLC advice classified, privileged, or sensitive when an agency relies upon that advice to justify a major policy decisions or executive action; and releasing a public index of its memoranda.²⁶

EPIC urges ACUS to require all OLC legal opinions, with narrow exceptions, to be released to the public—if not in whole, then in part and with sufficient notice that as much information about that opinion as possible has been made publicly available. OLC opinions have far-reaching effects on Executive Branch actions and shape the policies of numerous agencies. Lawyers in the OLC also do not often depart from previous decisions and opinions, making their unreleased “informal” advice all the more relevant to policymaking.²⁷

Currently, requests for more transparency in OLC opinions must be made through the FOIA process, where the agency can withhold records, allowing the OLC to continue operating with little public accountability.²⁸ The OLC has also failed to follow the “reading room” provision of FOIA, which requires agencies to proactively disclose final legal opinions or interpretations. Shrouding such opinions in secrecy gives the DOJ and other agencies more room to justify radical or partisan actions and use legal opinions that do not reflect the law. In the interest of transparency and accountability, ACUS should require these records to be released to the public.

II. Privacy Threshold Analyses & The Department of Homeland Security

²⁶ *The Office of Legal Counsel and the Rule of Law*, Am. Const. Soc’y (Oct. 2020), <https://www.acslaw.org/wp-content/uploads/2020/10/OLC-ROL-Doc-103020.pdf>.

²⁷ Trevor W. Morrison, *Stare Decisis in the Office of Legal Counsel*, 110 Columbia L. Rev. 1448 (2010).

²⁸ Stephanie Krent & Larry Siems, *Op-ed: Challenging secrecy in the Justice Department’s Office of Legal Counsel*, Colum. J. Rev. (May 11, 2022), <https://www.cjr.org/opinion/knight-institute-doj-olc-foia-lawsuits.php>.

The Department of Homeland Security (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).²⁹ 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).³⁰ Under Section 208 of the E-Government Act of 2002, agencies must produce and publish PIAs, if practicable, to explain what personally identifiable information the agency is collecting and how that information will be collected, stored, and transferred.³¹ As such, these privacy assessments are crucial for the public to assess how new technologies intrude on the lives of ordinary people.³² However, the requisite PIAs for many DHS programs have not been released. EPIC regularly submits FOIA requests and litigates to ensure that agencies comply with the requirements of the E-Government Act.³³

ACUS should call on DHS to proactively and consistently disclose PTAs. 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

²⁹ *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](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 accessed July 11, 2022).

³⁰ *Id.*

³¹ *Id.*

³² *EPIC v. DEA - Privacy Impact Assessments*, EPIC, <https://epic.org/documents/epic-v-dea-privacy-impact-assessments/> (2016).

³³ *Privacy Impact Assessments*, EPIC (2022), <https://epic.org/issues/open-government/privacy-impact-assessments/>.

and protections are incorporated into all activities of the Department.”³⁴ DHS processes highly sensitive data in programs such as the Comprehensive Biometric Entry/Exit Plan, which collects facial scans and iris images at entry and exit points of travel (where the traveler cannot meaningfully opt out of participation or mitigate the risks to their privacy).³⁵ In light of the significant privacy risks such programs and data pose, it is crucial to bring accountability DHS’s activities through the regular publication of PTAs.

III. Standard Operating Procedures:

ACUS should also urge DHS and other Executive Branch agencies to release standard operating procedure (SOP) documents and manuals for programs that affect the public. Such documents are critical to ensuring federal programs are being implemented as designed and for identifying gaps in compliance. EPIC previously requested SOPs from Customs and Border Protection (CBP) to assess what impact the Biometric Entry-Exit Program would have on airline passengers who opted out of facial recognition and whether the program mitigated accuracy and bias problems.³⁶ Without such records, EPIC and other public organizations cannot assess the extent which a program like the biometric entry/exit system respects privacy rights.

EPIC is also concerned by programs like DHS’ Standard Operating Procedure 303, which codified “a shutdown and restoration process for use by commercial and private wireless networks during national crises.”³⁷ EPIC submitted FOIA requests concerning SOP 303 and petitioned for the release of the operating procedure and guidelines.³⁸ Such programs can affect huge swaths of the

³⁴ *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).

³⁵ *EPIC v. CBP (Biometric Entry/Exit Program)*, EPIC (2017), <https://epic.org/documents/epic-v-cbp-biometric-entry-exit-program/>.

³⁶ *EPIC v. CBP (Biometric Entry/Exit Program)*, EPIC (2017), <https://epic.org/documents/epic-v-cbp-biometric-entry-exit-program/>.

³⁷ *EPIC v. DHS – SOP 303*, EPIC (2016), <https://epic.org/documents/epic-v-dhs-sop-303/>.

³⁸ *Id.*

population with little to no input and often no way to opt out.³⁹ Given the scale and ubiquity of many federal programs, it is key to ensure public disclosure of the rules and guidelines these programs and their sponsoring agencies must abide by.

The public release of SOPs would aid the efforts of EPIC and other organizations that pursue government transparency and oversight. The purpose of SOPs is to ensure compliance with the law, but as the Environmental Protection Agency has noted, “the best written SOPs will fail if they are not followed.”⁴⁰ The proactive release of these types of documents across the federal government will help advance compliance and accountability.

IV. Memoranda of Agreement/Memoranda of Understanding:

ACUS should require the public release of any memoranda of understanding or agreement (MOUs/MOAs) between federal agencies and other federal, state, local, or international agencies or companies. MOUs and MOAs specifically pertaining to the access, transfer, and use of personal data can have enormous implications for privacy rights. For example, the Department of State’s Bureau of Consular Affairs collects personal identification information and biometric data from U.S. and non-U.S. persons and sends that information to other federal agencies. This practice creates privacy risks when massive amounts of biometric data are disclosed to other programs like CBP’s Biometric Entry and Exit program, which uses such data for its facial recognition systems.⁴¹ EPIC has a strong interest in the MOUs and MOAs that codify these information-sharing agreements. Their public release would allow the public to better understand how our data is being transferred and what protections are currently in place.

³⁹ See Rachel Metz, *IRS Now Lets Taxpayers Opt Out of Facial Recognition After Backlash*, CNN (Feb. 22, 2022), <https://www.cnn.com/2022/02/22/tech/irs-facial-recognition-opt-out/index.html> for an example of a federal agency who has allowed consumers to opt out of facial recognition software after public backlash.

⁴⁰ *Guidance for Preparing Standard Operating Procedures*, Env’t Prot. Agency (Apr. 2007), <https://www.epa.gov/sites/default/files/2015-06/documents/g6-final.pdf>.

⁴¹ *EPIC v. State Department (Facial Recognition Database)*, EPIC (2019), <https://epic.org/documents/epic-v-state-department-facial-recognition-database/>.

Though federal agencies do maintain websites for public access to MOAs and MOUs, those databases are not complete and often fail to include important agreements that shape how personal data is used by the federal government. Outside of these agreements, there is little information as to how personal and biometric data is used and transferred between agencies. Public disclosure of MOUs and MOAs will meaningfully contribute to increased understanding of agency operations and the attendant risks to privacy.

Question 4: What types of legal materials should agencies proactively disclose to the general public? What types of legal materials may or should agencies disclose only in response to a request from a member of the public?

The E-Government Act and the Federal Advisory Committee Act both enable public access to government materials and empower democratic oversight of government functions. In addition to ensuring that agencies are compliant with these statutes, ACUS should recommend that Congress amend the relevant statutes to (1) ensure that there is a more robust disclosure requirement for Privacy Impact Assessments, (2) require all federal agencies to conduct and publish Privacy Threshold Analyses, and (3) impose transparency requirements on advisory subcommittees.

I. Privacy Impact Assessment Compliance

Over the past decade, EPIC has identified numerous instances in which the 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 2019, the DHS responded to EPIC's FOIA request and revealed that no PIA had been completed at the time for its "Homeland Advanced Recognition Technology" biometric database.⁴² In 2015, EPIC sued the FBI over its FOIA request for PTAs and PIAs related to facial recognition technology, license plate readers, and domestic drone surveillance—documents which had not been publicly updated for years, if at all.⁴³

⁴² EPIC, *EPIC FOIA: Massive DHS Biometric Database Still Lacks a Privacy Impact Assessment*, EPIC (May 3, 2019), <https://epic.org/epic-foia-massive-dhs-biometric-database-still-lacks-a-privacy-impact-assessment/>.

⁴³ EPIC, *EPIC v. FBI – Privacy Assessments* (2017), <https://epic.org/documents/epic-v-fbi-privacy-assessments/>.

The same year, EPIC filed a FOIA lawsuit against the DEA for its 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.⁴⁴

EPIC has also filed suit to compel agencies to produce required privacy assessments 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.⁴⁵ 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.⁴⁶ 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.⁴⁷

In view of this checkered history of compliance, Congress must reinforce the E-Government Act's PIA disclosure requirement. First, the fact that many of the cases above arose from FOIA requests highlights this policy's benefits for FOIA administrability. Given the immense backlogs many agencies face, proactively disclosing information on how programs directly affect the public may preempt FOIA requests. Second, disclosing information about agencies' collection and use of personal data is necessary for government transparency and public understanding of what the government is up to. As set forth below in response to Question 10, ACUS should recommend

⁴⁴ EPIC, *EPIC v. DEA – Privacy Impact Assessments* (2016), <https://epic.org/documents/epic-v-dea-privacy-impact-assessments/>.

⁴⁵ EPIC, *EPIC v. Presidential Election Commission* (2018), <https://epic.org/documents/epic-v-presidential-election-commission/>.

⁴⁶ EPIC, *EPIC v. Commerce (Census Privacy)* (2019), <https://epic.org/documents/epic-v-commerce-census-privacy/>.

⁴⁷ EPIC, *EPIC v. U.S. Postal Service* (2022), <https://epic.org/documents/epic-v-u-s-postal-service/>.

stronger enforcement mechanisms for federal agencies' PIA obligations under the E-Government Act, including language that will enable parties to bring suit when agencies fail to comply with section 208.

II. Privacy Threshold Analysis (PTA) Requirement

Section 208 of the E-Government Act and the implementing guidance from the Office of Management & Budget make clear that privacy assessments should be conducted as early as possible in the development of a new collection of personal information or covered information technology. Agencies such as the DHS have accomplished this in parts through the use of Privacy Threshold Analyses. ACUS should urge Congress to mandate the creation and publication of PTAs across other agencies. First, PTAs⁴⁸ are typically simple checklists that can be quickly completed by one person; mandating the creation and release of these documents would impose little administrative burden. Second, proactively disclosing these documents would have knock-on effects for privacy assessments and transparency. As PTAs show whether or not a program would necessitate a PIA, should a program that was found to require a PIA go into effect without one, the agency will publicly be breaking its own word. Moreover, a false negative (a program that was incorrectly designated to not need a PIA) signals to the public an internal breakdown in privacy assessment, which may warrant further action.

III. Subcommittees Subject to FACA

Finally, ACUS should amend FACA so that subcommittees created by committees covered by FACA are similarly subject to its disclosure provision. Last year, in a case brought by EPIC, the U.S. Court of Appeals for the D.C. Circuit ruled that the Federal Aviation Administration's Drone Advisory Committee (DAC) did not have to produce documents made by DAC's subcommittees

⁴⁸ Dep't of Homeland Sec., *DHS Privacy Threshold Analysis (PTA)* (2012), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf.

because those subcommittees were created by the committee itself rather than the FAA.⁴⁹ This reading of FACA enables committees to circumvent the statute’s otherwise robust transparency requirements by burying important documents and proceedings in closed-door subcommittees. For example, the Washington Post obtained documents showing that one of the DAC’s subgroups “included industry insiders with a financial stake in the outcome and was co-chaired by a lobbyist for DJI, a Chinese drone maker that dominates the U.S. market.”⁵⁰ Meanwhile, a parent committee can effectively rubberstamp a subcommittee’s recommendations without having to disclose the materials or deliberations those recommendations were based on.

In order to preserve FACA’s transparency mandate, ACUS should urge Congress to amend FACA and close this subcommittee loophole. As a template, ACUS should look to H.R. 1608 (2019),⁵¹ which directly addresses the lack of transparency across advisory subcommittees.

Question 5: For agency legal materials that should be proactively disclosed, where or how should agencies make them publicly available (on agency websites, in the Federal Register, or elsewhere)?

Proactive disclosure ensures the public has prompt access to certain documents of substantial public interest. Reforming proactive disclosure processes would benefit the public by providing more information about government activities without imposing the burden of requesting records. Improving proactive disclosure would also benefit federal agencies by reducing the volume of FOIA requests agencies receive. ACUS should urge Congress and the Office of Management and Budget to implement the following reforms: (1) make Privacy Impact Assessments available through a single centralized database, (2) require all agencies to maintain well-designed FOIA reading rooms.

⁴⁹ *EPIC v. DAC*, 995 F.3d 993 (D.C. Cir. 2021).

⁵⁰ Michael Laris, *A U.S. drone advisory group has been meeting in secret for months. It hasn't gone well.*, Washington Post (Oct. 23, 2017), https://www.washingtonpost.com/local/trafficandcommuting/a-us-drone-advisory-group-has-been-meeting-in-secret-for-months-its-work-has-not-gone-well/2017/10/23/f53106e0-6c01-11e7-b9e2-2056e768a7e5_story.html.

⁵¹ H.R. 1608, <https://www.congress.gov/bill/116th-congress/house-bill/1608/text>.

I. PIAs Should be Available Through a Centralized Database.

PIAs are required by §208 of the e-Government Act of 2002.⁵² The statute requires that PIAs be made available to the general public through a website, the Federal Register, or similar means.⁵³

PIAs provide important information to members of the public and civil society groups. They enable the public to engage in thoughtful debate about the use of their personally identifiable information and to understand the systems operated by the government and the privacy risks associated with those systems.⁵⁴ They also encourage public trust by providing information about the risks and benefits of those systems and the use of personal data.⁵⁵ They encourage public confidence by identifying privacy risks and mitigation strategies before a technology is implemented.⁵⁶

PIAs should be proactively disclosed through a centralized and searchable database that is run by the Office of Management and Budget (“OMB”). 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.⁵⁷ 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.

Furthermore, 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,

⁵² E-Government Act, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).

⁵³ *Id.*

⁵⁴ Bureau of Just. Assistance, Dep’t of Just., *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities* 4 (2016).

⁵⁵ *Id.*

⁵⁶ Gary T. Marx, *Privacy is Not Quite Like Water*, in *Privacy Impact Assessment v. v Wright, D., & De Hert, P.* (David Wright & Paul de Hert eds., 2012).

⁵⁷ *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).

topic, and date of publication. A good example of such a webpage is the Department of Homeland Security's Privacy Impact Assessments repository.⁵⁸

II. Congress Should Require Agencies to Adopt Reading Rooms Designed by OMB.

While many agencies have reading rooms, the level of information available across each reading room varies, particularly with respect to the way that proactive disclosures are displayed. Many reading rooms, including the Department of Homeland Security OIG's office reading room, the Federal Reserve reading room, and the Social Security Administration reading room, include subpages that lead to proactive disclosures or frequently requested documents.⁵⁹ However, there is significant variation in whether or how proactive disclosures are displayed. Some agencies provide a specific sub-page with all frequently requested documents,⁶⁰ some agencies create a subsection for frequently requested documents on a central page,⁶¹ and some agencies do not provide a frequently requested documents section at all.⁶²

This inconsistency is likely to confuse users. To alleviate this confusion, Congress should direct OMB to design a template for each FOIA reading room. Agencies should be required to adopt the template. This change will create uniformity and streamline public understanding of and access to records. OMB's Reading Room design should have the following characteristics:

⁵⁸ *Privacy Documents for Department-Wide Programs*, Dep't of Homeland Sec., <https://www.dhs.gov/privacy-documents-department-wide-programs> (2022).

⁵⁹ *FOIA Reading Room*, Department of Homeland Security Office of the Inspector General, <https://www.oig.dhs.gov/foia/reading-room> (last visited July 7, 2022); *FOIA Reading Room*, Board of Governors of the Federal Reserve System, <https://www.federalreserve.gov/foia/readingrooms.htm> (last visited July 7, 2022); *FOIA Reading Room*, Social Security Administration, <https://www.ssa.gov/foia/readingroom.html> (last visited July 7, 2022).

⁶⁰ *Frequently Requested Documents*, U.S. Securities and Exchange Commission, <https://www.sec.gov/foia-frequently-requested-documents> (last visited July 7, 2022); *Legal Library: Frequently Requested FOIA Records*, Federal Trade Commission, <https://www.ftc.gov/legal-library/browse/frequently-requested-foia-records> (last visited July 7, 2022).

⁶¹ Social Security Administration, <https://www.ssa.gov/foia/readingroom.html> (last visited July 7, 2022); *FOIA Reading Room*, Department of Homeland Security Office of the Inspector General, <https://www.oig.dhs.gov/foia/reading-room> (last visited July 7, 2022); *FOIA Reading Room*, Board of Governors of the Federal Reserve System, <https://www.federalreserve.gov/foia/readingrooms.htm> (last visited July 7, 2022). **Error! Hyperlink reference not valid.**

⁶² *Freedom of Information Act Electronic Reading Room*, Central Intelligence Agency, <https://www.cia.gov/readingroom/> (last visited July 7, 2022).

a. OMB Should Require Agencies to Maintain a “Frequently Requested Records” Page.

Each Reading Room should include a page with “Frequently Requested Records” that includes the documents which are proactively disclosed. Having these documents available in one place will make document access easier and agency materials more accessible to the general public. It will also reduce the number of duplicative records requests by allowing members of the public to quickly understand what records are available.⁶³

b. Agencies should be required to ensure that their proactively released records are searchable.

Many of the agencies that provide a specific sub-page or subsection for proactively released records do not provide a search functionality for the records in question.⁶⁴ Instead, pages often include a list of proactively released records.⁶⁵ Sometimes these records are arranged by date, but this is not always true. Members of the public may not have enough information about what each record contains, and thus may not be able to determine whether the information they are searching for is in a particular document. Instead, OMB should require agencies to create a search feature that allows users to filter content by date of publication, sub-component of the agency, meta-tags, and any other filtering mechanisms that may be useful.

c. Congress or OMB should require that agencies update their Reading Rooms at least quarterly.

Though agencies are required to make proactive disclosures by law, many agencies delay these disclosures or never complete them at all.⁶⁶ In order to ensure that proactive disclosures are as useful as possible, agencies should be required to release documents that fall under their proactive

⁶³ *Id.* at 17.

⁶⁴ See e.g., *Legal Library: Frequently Requested FOIA Records*, Federal Trade Commission, <https://www.ftc.gov/legal-library/browse/frequently-requested-foia-records> (last visited July 7, 2022).

⁶⁵ *FOIA Reading Room*, Social Security Administration, <https://www.ssa.gov/foia/readingroom.html> (last visited July 7, 2022).

⁶⁶ United States Government Accountability Office, *Freedom of Information Act: Actions Needed to Improve Agency Compliance with Proactive Disclosure Requirements* 3 (Mar. 2021) (finding that two out of three surveyed agencies had proactively disclosed an average of less than ten documents during the fiscal years 2018 and 2019).

disclosure requirements on a quarterly basis. They should also include some means of notifying members of the public of these disclosures, such as posting an update on social media or writing “new” next to newly released documents. This will ensure that the public has access to the most useful, up-to-date information.

Question 8: Are there certain best practices regarding disclosure of legal materials on agency websites that should be required by statute (e.g., indexing of legal materials, search functions to help find legal materials)? If so, should these practices be required for all legal materials or only certain types of legal materials?

ACUS should recommend that Congress amend the FOIA to 1) lower the threshold for proactive disclosure of documents, 2) improve the navigability and search functions of FOIA.gov, 3) require agencies to return documents in searchable electronic format, 4) require agencies to archive webpages and social media accounts, and 5) require agencies to disclose when documents otherwise eligible for proactive disclosure are withheld. Federal agencies are required to publish agency regulations, policies, and procedural rules in the Federal Register⁶⁷ and to make various other legal materials “available for public inspection in an electronic format.”⁶⁸ These materials include: (1) final opinions and orders from adjudicatory proceedings; (2) specific policies not published in the Federal Register; (3) staff manuals and instructions affecting members of the public; and (4) any materials released following a FOIA request that the agency deems of public interest or that have been requested at least three times.⁶⁹ The E-Government Act requires agencies to publish such materials on their websites,⁷⁰ while the Federal Records Act requires agencies to programs dedicated to identifying records “of general interest or use to the public” and posting those records “in a publicly accessible electronic format.”⁷¹ Finally, President Obama’s FOIA Memorandum directs

⁶⁷ 5 U.S.C. § 552(a)(1).

⁶⁸ 5 U.S.C. § 552(a)(2).

⁶⁹ *Id.*

⁷⁰ E-Government Act § 207(f).

⁷¹ 44 U.S.C. § 3102.

agencies to “take affirmative steps to make information public,”⁷² while DOJ FOIA Guidelines direct agencies to “readily and systematically post information online in advance of any public request.”⁷³ President Biden’s administration affirmed this commitment to proactive disclosure by directing agencies to “post records online as soon as feasible.”⁷⁴

I. Lower the Threshold for Proactive Disclosure

FOIA requires proactive disclosure of a limited list of regular agency work product and records that have been requested more than three times.⁷⁵ But the current proactive disclosure standard has done little to provide the public with meaningful access to relevant documents or to reduce the burden of processing FOIA requests on agencies. The easiest and most democratic solution is to release all records that have been requested at least once on behalf of the public interest. Agencies already make this determination when considering a request’s eligibility for the fee waiver under 5 U.S.C. § 552(a)(4)(A)(iii). Thus, agencies can easily publish all records that qualify for the fee waiver.

There’s no principled reason not to publish such records. Agencies are already required to release requested records that have been disclosed in response to earlier requests,⁷⁶ and many of these records are already publicly shared on websites like MuckRock.com.⁷⁷ In fact, the Obama administration piloted a “Release for One, Release for All” policy that proactively posted FOIA

⁷² President Barack Obama, Memorandum of January 21, 2009, on the Freedom of Information Act, 74 Fed. Reg. 4,683, 4,683, <https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/presidential-foia.pdf>.

⁷³ *Proactive Disclosure of Non-Exempt Agency Information: Making Information Available Without the Need to File a FOIA Request*, Office of Info. Pol’y, Dep’t of Justice, (Dec. 17, 2021), https://www.justice.gov/oip/oip-guidance/proactive_disclosure_of_non-exempt_information**Error! Hyperlink reference not valid.**

⁷⁴ Attorney General Merrick Garland, Memorandum for Heads of Executive Departments and Agencies Regarding Freedom of Information Guidelines (Mar. 15, 2022), at 2, <https://www.justice.gov/ag/page/file/1483516/download>.

⁷⁵ 5 U.S.C. §552(a)(2).

⁷⁶ *Nat’l Archives & Records Admin. v. Favish*, 541 U.S. 157, 172 (2004) (“As a general rule, if the information is subject to disclosure, it belongs to all”); *Fitzgibbon v. CIA*, F.2d 755, 765 (D.C. Cir. 1990).

⁷⁷ *About MuckRock*, MuckRock <https://www.muckrock.com/about/> (last visited July 11, 2022).

responses online, excluding first-party requests.⁷⁸ The pilot was a success, with agencies and the public benefitting from (1) the elimination of duplicate requests; (2) the streamlining of the FOIA response process; (3) increased collaboration across agencies; and (4) greater awareness of what information is posted on agency websites.⁷⁹ Moreover, the Office of Information Policy (“OIP”) recognized the “inherent value” of making government records more accessible to the public. Informed by the pilot, the OIP proposed a plan to implement the policy across all agencies and solicited public comments.⁸⁰ Sadly, however, the Trump Administration killed the plan without explanation.⁸¹

ACUS now has the opportunity to revive the “Release to One, Release to All” policy and restore the presumption of access to our nation’s government. The policy should incorporate the lessons learned from the 2016 pilot, including the following:

- Excluding first-party requests for an individual’s records that would not normally be public information.⁸²
- Creating a “good cause” exception for the following:
 - Records that are particularly difficult to post online, such as large videos;
 - Records that are graphic, obscene, or otherwise inappropriate to post on government websites;
 - Records including deidentified data that threaten an individual’s privacy by “exposing individuals to harms such as identity theft, reputational harm, embarrassment, financial loss, and risk to personal safety”;

⁷⁸ *Request for Public Comment on Draft “Release to One, Release to All” Presumption*, United States Department of Justice, <https://www.justice.gov/oip/blog/request-public-comment-draft-release-one-release-all-presumption> (Dec. 9, 2016).

⁷⁹ Office of Information Policy, *Proactive Disclosure Pilot Assessment* 19 (June 2016), https://www.justice.gov/oip/reports/proactive_disclosure_pilot_assessment/download.

⁸⁰ *Request for Public Comment on Draft “Release to One, Release to All” Presumption*, United States Department of Justice, <https://www.justice.gov/oip/blog/request-public-comment-draft-release-one-release-all-presumption> (Dec. 9, 2016).

⁸¹ Letter from American-Arab Anti-Discrimination Committee et al. to Mick Mulvaney, Director, Office of Management and Budget, and Melanie Ann Pustay, Director, U.S. Department of Justice (Oct. 31, 2017), <https://www.aallnet.org/wp-content/uploads/2017/12/Finalize-Proactive-FOIA-Disclosure-Policy.pdf>.

⁸² Office of Information Policy, *“Release to One, Release to All” Presumption: Achieving Greater Transparency by Making More Information Available Online* 2, <https://www.regulations.gov/docket/DOJ-LA-2016-0024>.

- Records that would directly interfere with active investigations by law enforcement.⁸³
- Posting descriptions of records falling under the “good cause” exception without endangering the interests protected by the exception.⁸⁴
- Formatting records in accordance with Section 508 of the Rehabilitation Act to provide “individuals with disabilities access to electronic information and data comparable to those without disabilities.”⁸⁵

If ACUS does not recommend a lower threshold, it should at least recommend a clearer threshold. FOIA already incorporates public interest balancing tests limiting the extent of FOIA Exemptions 6 and 7(C).⁸⁶ ACUS should recommend legislative reform that empowers agencies to adopt this test for proactive disclosures as well, publishing all records that “contribut[e] significantly to public understanding of the operations or activities of the government” so long as disclosure does not effect “substantial” harm.⁸⁷

Even when clear standards exist, however, agencies may fail to proactively disclose materials as required by law. Last year, the Government Accountability Office reviewed agency compliance with proactive disclosure requirements and found that three of the eighteen agencies reviewed did not comply with proactive disclosure requirements.⁸⁸ All three agencies responded with new processes to fulfill their statutory obligations,⁸⁹ but evidently OIP must exercise thorough and regular oversight to guarantee compliance in the future. ACUS should recommend that Congress require the OIP to conduct regular audits to ensure proactive disclosure and provide OIP the resources and personnel it requires to fulfill that duty.

⁸³ *Id.* at 3.

⁸⁴ *Id.*

⁸⁵ *Id.* at 4.

⁸⁶ Cong. Res. Serv., *The Freedom of Information Act (FOIA): A Legal Overview* 35, 39 (Aug. 24, 2020), <https://crsreports.congress.gov/product/pdf/R/R46238>.

⁸⁷ *Id.*

⁸⁸ Government Accountability Office, *Freedom of Information Act: Actions Needed to Improve Agency Compliance with Proactive Disclosure Requirements* 5 (Mar. 2021), GAO-21-254.

⁸⁹ *Id.*

II. *Improve the Navigability of FOIA.gov*

FOIA.gov currently serves as the central repository for locating public records across various agency websites. Unfortunately, the user interface is overwhelming, with no way to filter, sort, or evaluate the results. The Attorney General recently released guidance requiring agencies to “ensure that the public can readily find information” and to make FOIA websites “easily navigable” with records “presented in the most useful, searchable, and open formats possible.”⁹⁰ ACUS should affirm this policy of accessibility and recommend that Congress pass legislation that (1) provides a FOIA.gov user experience that meets industry standards for search engines; (2) requires all agencies to participate in FOIA.gov; and (3) utilizes “smart” searching to comprehend the user’s needs and produce the most relevant records.

Currently, FOIA.gov fails to provide even basic functions that citizens expect from search engines. Congress should require FOIA.gov to meet industry standards for search functionality, which at a minimum includes the following features:

- A result count⁹¹
- Previews for each result, including a summary description of the record, the date of the record, the redacted status, and highlighting the portion relevant to the search
- Filters for agencies, general subject matters, state or region, date, file type, and type of legal material (e.g., regulations, adjudicatory orders, policy guidance, or briefs)
- Sorting options for relevance, date, and popularity
- Editing search terms and adjusting filters while viewing the results⁹²
- Advanced search options that include Boolean operators, proximity operators, wildcard operators, and numeric operators⁹³

⁹⁰ *Id.*

⁹¹ Louise Vollaire & Alexandra Prokhorova, *Search Filters: 5 Best Practices for a Great UX*, Algolia (Mar. 27, 2020), <https://www.algolia.com/blog/ux/search-filter-ux-best-practices>.

⁹² *Id.*

⁹³ *Search Query Operators*, govinfo, <https://www.govinfo.gov/help/search-operators> (last visited July 11, 2022).

Furthermore, citizens should not need to construct the perfect query in order to access public records. Congress should require the OIP to investigate opportunities to incorporate “smart” searching into FOIA.gov to make it easier for users to find answers to their questions. Search engines are increasingly utilizing Natural Language Processing (NLP) and Natural Language Understanding (NLU) to provide users the information they actually seek, not just the information they technically request. and FOIA.gov should use NLP/NLU to provide the following capabilities:

- Correcting typos⁹⁴
- Auto-completing search queries⁹⁵
- Suggesting related searches⁹⁶
- Answering questions with excerpts from relevant records⁹⁷

To make these reforms possible, agencies will need to tag their records with common, relevant search terms as well as by category. OIP, in collaboration with the National Archives (“NARA”), should provide a standard set of tags as well as guidance on how tags should be applied.

Finally, Congress should clarify that the government bears the burden of producing relevant records through user-friendly and centralized search results. Currently, some agencies do not use FOIA.gov.⁹⁸ Moreover, presumptive and proactive disclosure mean little if citizens have to manually sort through unmanageable databases to find the information they need. All of the improvements listed above would improve access to public records, but current law does not clearly require agencies to provide such access through FOIA.gov. FOIA does not compel agencies to create new

⁹⁴ Gabriela Gentile, *UX for Search 101*, Medium (July 13, 2020), <https://uxdesign.cc/ux-for-search-101%EF%B8%8F-2ab4b2f2384d>.

⁹⁵ *Id.*

⁹⁶ *Id.*

⁹⁷ For an example of a search engine that provides records-based answers to questions, see Lexis Answers, <https://www.lexisnexis.com/pdf/lexis-advance/lexis-answers.pdf>; see also Dustin Coates, *How NLP & NLU Work for Semantic Search*, Search Engine Journal (Apr. 25, 2011), <https://www.searchenginejournal.com/nlp-nlu-semantic-search/444694/>; Dave Davies, *How Search Engines Answer Questions*, Search Engine Journal (May 27, 2020), <https://www.searchenginejournal.com/search-engines/answering-questions/>.

⁹⁸ FOIA.gov, <https://www.foia.gov/> (July 11, 2022).

records to satisfy a citizen’s curiosity,⁹⁹ but courts are divided over whether the time and effort invested in organizing search results counts as the creation of a new record.¹⁰⁰ Congress should resolve the confusion once and for all by amending FOIA to require participation in and meaningful search results from FOIA.gov.

III. *Require Agencies to Upload All Legal Materials as High-Quality, Searchable, PDFs*

FOIA requires agencies to electronically publish all records subject to proactive disclosure¹⁰¹ and to make a reasonable effort to produce records in the format requested.¹⁰² The current policy under President Biden is to produce records in “the most useful, searchable, and open formats possible.”¹⁰³ For most legal materials, the ideal format would be high-quality, searchable pdfs with clickable links embedded in the table of contents.¹⁰⁴ All images should have alternative text, and materials should be hashed for easy indexing within the search engine.¹⁰⁵

IV. *Include Archived Webpages and Social Media*

It is now standard practice for agencies to communicate with the public through their websites and social media accounts.¹⁰⁶ In the last ninety days alone, there were over 4.8 billion visits to government websites seeking passport applications and tax forms, tracking USPS packages and

⁹⁹ *Forsham v. Harris*, 445 U.S. 169, 186 (1980); *Nat’l Sec. Counselors v. CIA*, 969 F.3d 406, 409 (D.C. Cir. 2020).

¹⁰⁰ *Compare Nat’l Sec. Counselors*, 969 F.3d at 409 (finding that the manual compilation of records is creating a new record but declining to rule on whether an electronic compilation counts as a new record), *and Guidry v. Comey*, 692 Fed. Appx. 975, 978 (11th Cir. 2017) (finding that the results of a “manual keyboard search” counts as a new record), *with Ctr. for Investigative Reporting v. United States DOJ*, 14 F.4th 916, 938 (9th Cir. 2020) (finding that the results of a query does not count as a new record).

¹⁰¹ 5 U.S.C. § 552(a)(2).

¹⁰² 5 U.S.C. § 552(a)(3).

¹⁰³ Garland memo, *supra* note 76, at 3.

¹⁰⁴ *See Recommended Preservation Formats for Electronic Records*, Smithsonian Institution Archives, <https://siarchives.si.edu/what-we-do/digital-curation/recommended-preservation-formats-electronic-records> (last accessed July 11, 2022).

¹⁰⁵ *See Checking PDFs for Accessibility*, University of Washington, <https://www.washington.edu/accessibility/documents/check-pdfs/> (last accessed July 11, 2022).

¹⁰⁶ *Improving the Accessibility of Social Media in Government*, Digital.gov, <https://digital.gov/resources/improving-the-accessibility-of-social-media-in-government/#:~:text=Government%20agencies%20are%20increasingly%20using,and%20effectively%20than%20ever%20before> (last accessed July 11, 2022).

social security benefits, and accessing life-saving information about COVID, hurricanes, and other natural disasters.¹⁰⁷ Even as websites and social media accounts become the primary point of contact between citizens and their government, records of these online interactions disappear every day. In 2005, NARA provided broad guidance to agencies on how to manage website records.¹⁰⁸ Agencies were instructed to retain webpages as long as necessary to “satisfy business needs and mitigate risk, taking into account Government accountability and the protection of legal rights.”¹⁰⁹

While “most web records do not warrant permanent retention,” NARA works with agencies to preserve webpages with historical value,¹¹⁰ such as White House websites.¹¹¹ However, website records are not available through FOIA.gov. As a result, it can be very difficult for citizens to find even basic information about the administration of their government. For example, it is incredibly—and ironically—difficult to access information on the Interagency Committee on Government Information (“ICGI”),¹¹² which was established by the E-Government Act of 2002 to recommend ways to expand access to government information.¹¹³ The best source of information on the ICGI may be its now-defunct webpage, which is more readily accessible via the Internet Archive than NARA and certainly not found on FOIA.gov.¹¹⁴

Citizens shouldn’t have to rely on private archivists in order to understand how their government is, or is not, working towards transparency and fulfilling its statutory duties. Accessibility in the internet age means accessibility to web-native materials, and ACUS should work

¹⁰⁷ *All Participating Websites*, Analytics.usa.gov, <https://analytics.usa.gov/> (last accessed July 8, 2022).

¹⁰⁸ *NARA Guidance on Managing Web Records Background*, National Archives (Jan. 2005), <https://www.archives.gov/records-mgmt/policy/managing-web-records-background.html>.

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *Archived Presidential White House Websites*, National Archives, <https://www.archives.gov/presidential-libraries/archived-websites> (last accessed July 11, 2022).

¹¹² James A. Jacobs & James R. Jacobs, *Government Recommendations to Preserve Government Information Not Preserved by Government*, Free Government Information (Sept. 27, 2021), <https://freegovinfo.info/node/14266/>.

¹¹³ E-Government Act § 207(d).

¹¹⁴ Jacobs, *supra* note 114.

with Congress to (1) better retain records of webpages and social media posts that lack hardcopy alternatives and (2) make those records available through FOIA.gov.

V. *Agencies should be required to identify and publicize the existence of proactively disclosable documents that are withheld pursuant to FOIA exceptions.*

The American people have an interest in knowing what information the government collects and creates, even if the records are not directly accessible under FOIA. “The basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.”¹¹⁵ That purpose is defeated if the government can withhold records without any public oversight. Thus, for every claimed FOIA exemption, courts require agencies to “identify[] the documents withheld, the FOIA exemptions claimed, and a particularized explanation of why each document falls within the claimed exemption.”¹¹⁶ Courts have recognized that this minimal level of transparency is necessary to both disincentivize overly broad applications of FOIA exemptions and enable citizens to challenge those claimed exemptions in court.¹¹⁷ Moreover, the public has a right to know “what their government is up to,”¹¹⁸ including what their government is withholding from them in the name of the public interest.¹¹⁹

The same principles apply to proactive disclosure,¹²⁰ and accountability under FOIA requires some insight into which records are being withheld for which reasons. Congress recognized as much when it required the executive branch to submit an annual report disclosing the number of times the agency relied on each exemption to withhold records and a “concise description of the scope of any

¹¹⁵ *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978).

¹¹⁶ *Burton v. Wolf*, 803 Fed. Appx. 120, 122 (9th Cir. 2020); *see also Roth v. DOJ*, 642 F.3d 1161, 1178 (D.C. Cir. 2011) (affirming the “general rule that agencies must acknowledge the existence of information responsive to a FOIA request).

¹¹⁷ *Vaughn v. Rosen*, 484 F.2d 820, 826-27 (D.C. Cir. 1973).

¹¹⁸ *United States Dep’t of State v. Ray*, 502 U.S. 164 (1991).

¹¹⁹ *See Roth*, 642 F.3d at 1178.

¹²⁰ *Proactive Disclosure of Non-Exempt Agency Information*, United States Department of Justice (updated Dec. 17, 2021), [https://www.justice.gov/oip/oip-guidance/proactive_disclosure_of_non-exempt_information#:~:text=The%20fundamental%20purpose%20of%20the,749%2C%20773%20\(1989\).](https://www.justice.gov/oip/oip-guidance/proactive_disclosure_of_non-exempt_information#:~:text=The%20fundamental%20purpose%20of%20the,749%2C%20773%20(1989).)

information withheld.”¹²¹ However, there is currently no way to easily identify withheld records relevant to a specific query or understand why they were withheld. As a result, citizens are effectively denied the right to challenge those withholdings simply because they may not know the records exist. Citizens and agencies may also waste time and resources chasing records that are less relevant to their concerns or else more difficult to obtain.

FOIA guarantees the right to hold our government accountable. FOIA.gov can better secure that right if search results include not only public but withheld records. For an example of how such disclosures could work, the OIP should consider how agencies post PIAs online. PIAs name and describe the system assessed, identify the privacy interests at stake, and explain how those interests would be protected under the planned implementation of the system.¹²² Ideally, these PIAs are posted online and organized by topic and date. Some agencies include a search function.¹²³ OIP can similarly demand transparency from agencies by gathering agency interpretations of FOIA exceptions in one place.

For every withheld record, agencies should be required to post their response denying access to the record. The online posting should include the title of the requested record, the exception claimed, and the reasons that the exception applies. All such postings should be available through FOIA.gov and indexed by agency, date, and exception claimed. Of course, this requirement would not compel agencies to proactively identify records that would be withheld if requested but only to list records that the agency has a priori deemed exempted by FOIA and that are subject to FOIA’s

¹²¹ 5 U.S.C. § 552(e)(1).

¹²² *Privacy Impact Assessment*, Office of Privacy & Open Government, <https://www.osec.doc.gov/opog/privacy/pia.html> (last accessed July 11, 2022).

¹²³ *See Privacy Impact Assessments (PIA) Collection*, Department of Homeland Security, <https://www.dhs.gov/publications-library/collections/privacy-impact-assessments-%28pia%29> (last accessed July 11, 2022).

proactive disclosure requirements, i.e., if the record was requested at least three times or is of public concern.¹²⁴

Finally, FOIA.gov users should be able to find the names of any cases litigating access to a withheld record via the search results. This capability would enable citizens to coordinate efforts and save resources. All of this information should be accessible in the FOIA logs agencies should update on a quarterly basis, as recommended by the FOIA Federal Advisory Committee.¹²⁵

VI. *All Legal Materials Should Be Subject to these Best Practices*

Americans deserve better access to public records as well as the opportunity to hold agencies accountable when records are withheld. That right of access does not depend on the nature of the records sought, and so the ACUS should recommend these best practices for all agency legal materials.

Question 10: What other statutory reforms might be warranted to ensure adequate public availability of agency legal materials?

Congress should amend section 208 of the E-Government Act to enhance public access to privacy impact assessments, to strengthen agency compliance, and to ensure the availability of judicial redress.

The E-Government Act was enacted with the aim of “promot[ing] better informed decisionmaking by policy makers”; “provid[ing] enhanced access to Government information”; and “mak[ing] the Federal Government more transparent and accountable.”¹²⁶ Among the “constituencies” Congress intended to account for in the Act are “the public access community,” “privacy advocates,” and “non-profit groups interested in good government.”¹²⁷ In order to “ensure

¹²⁴ 5 U.S.C. § 552(a)(2).

¹²⁵ Freedom of Information Act Federal Advisory Committee, 2020-2022 Committee Term Final Report and Recommendations 19 (June 2, 2022), https://www.archives.gov/files/ogis/foia-advisory-committee/2020-2022-term/meetings/foia-advisory-committee-report-recommendations.final_draft_6.2.2022-1.pdf.

¹²⁶ E-Government Act §§ 2(b)(7), (9), (11).

¹²⁷ 148 Cong. Rec. 11,228 (2002) (statement of Sen. Lieberman)

sufficient protections for the privacy of personal information,” section 208 of the E-Government Act requires federal agencies to complete and publish a privacy impact assessment prior to initiating a new collection of personal data or developing or procuring information technology that will process personal data in some fashion.¹²⁸ In this way, section 208 fulfills a dual purpose: it forces agencies to “fully consider[] privacy and incorporate[] appropriate privacy protections from the earliest stages of [an] agency activity,”¹²⁹ and it “make[s] the Federal Government more transparent and accountable.”¹³⁰

Regrettably, a string of recent court decisions has undermined both of these purposes by discounting the information-disclosure function of section 208 and preventing organizations or individuals from bringing suit when an agency fails to produce a required privacy impact assessment.¹³¹ These rulings have further weakened a key privacy provision that agencies already had a track record of violating without consequence.¹³²

Accordingly, ACUS should urge Congress to make the following amendments to enhance public access to privacy impact assessments, to strengthen agency compliance with section 208, and to ensure the availability of judicial redress when an agency violates the statute.

- **Clarify the purposes of section 208.** In addition to “ensur[ing] sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government,”¹³³ Congress should make clear that section 208 is also intended “to ensure that individuals and public interest organizations are given timely and comprehensive notice of agency activities which implicate the processing of personal information” and “to ensure that

¹²⁸ E-Government Act §§ 208(a)–(b).

¹²⁹ Office of Mgmt. & Budget, OMB Circular A-130: Managing Information as a Strategic Resource (2016), app. II at 10.

¹³⁰ E-Government Act § 2(b)(9).

¹³¹ See *EPIC v. U.S. Dep’t of Commerce*, 928 F.3d 95 (D.C. Cir. 2019); *EPIC v. Presidential Advisory Comm’n on Election Integrity*, 878 F.3d 371 (D.C. Cir. 2017); *EPIC v. USPS*, No. 1:21-CV-02156 (TNM), 2022 WL 888183 (D.D.C. Mar. 25, 2022).

¹³² See, e.g., *EPIC, EPIC v. FBI – Privacy Assessments* (2017), <https://epic.org/documents/epic-v-fbi-privacy-assessments/>; *EPIC, EPIC v. DEA – Privacy Impact Assessments* (2016), <https://epic.org/documents/epic-v-dea-privacy-impact-assessments/>.

¹³³ E-Government Act § 208(a).

agencies are publicly accountable for the processing and safeguarding of personal information.”

- **Sharpen the conditions under which an assessment is required.** In addition to the existing triggers for the completion and publication of a privacy impact assessment, Congress should specify that an impact assessment is required for any information technology that “processes” personal information and any new collection of personal information that will be “processed” using information technology. Congress should also codify OMB’s requirement that privacy impact assessments be updated when a covered piece of informational technology or collection of personal information is materially modified.¹³⁴
- **Narrow the circumstances in which an assessment can be withheld from the public.** Under the current text of section 208, an agency need only publish a privacy impact assessment “if practicable”—a phrase that is both vague and overly permissive of agencies withholding vital information from the public.¹³⁵ Congress should revise section 208(b)(1) to require publication by default of each privacy impact assessment through the Federal Register, through the respective agency’s website, and through a searchable online database of assessments to be developed by the Office of Management and Budget. To accommodate circumstances in which an agency has a colorable interest in withholding some or all of a privacy impact assessment, Congress should permit agencies to withhold such information only to the extent that it falls “within one or more of the exemptions set forth in [the FOIA] . . . except that no information contained in a privacy impact assessment may be withheld on the grounds that it is deliberative or predecisional.” Consistent with the FOIA, Congress should also require agencies that seek to withhold any portion of a privacy impact assessment to “take reasonable steps necessary to segregate and release all nonexempt information contained in the assessment.”
- **Require assessments to be conducted earlier in an agency’s decision-making process.** To make privacy impact assessments as useful as possible to both agencies and the public, Congress should mandate that agencies “commence preparation of a privacy impact assessment as close as possible to the time the agency considers” developing or procuring covered information technology or initiating a new collection of personal information. Congress should also underscore that, in any event, an agency may not develop or procure covered information technology or initiate a new collection of personal information until it has conducted, reviewed, and published the requisite privacy impact assessment(s).
- **Require the creation and publication of privacy threshold analyses.** As set forth above in response to Question 4, Congress should require the creation and publication of privacy threshold analyses as the first step in the privacy impact assessment process.s

A redlined version of section 208 reflecting the above amendments is attached to these comments as Exhibit A.

¹³⁴ Joshua B. Boltin, Dir., OMB, Executive Office of the President, M03-22, Memorandum for Heads of Executive Departments and Agencies, attachment A § II.C.2.a.i (Sept. 26, 2003).

¹³⁵ E-Government Act § 208(b)(1)(B)(iii).

Conclusion

EPIC applauds ACUS's decision to investigate federal agencies' compliance with existing open records laws and encourages ACUS to focus on the gaps in these laws that allow agencies to withhold records of vital interest to the public. ACUS should provide Congress with a set of suggested statutory amendments to make records more accessible, easier to search, and harder to withhold and to ensure that agencies fully comply with their statutory obligations. Please address any questions to EPIC Law Fellow Jake Wiener at wiener@epic.org.

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
Senior Counsel

Jake Wiener
Jake Wiener
EPIC Law Fellow

John Davisson
John Davisson
EPIC Director of Litigation

Exhibit A

Proposed edits to section 208 of the
E-Government Act of 2002

Public Law 107-347
107th Congress

An Act

To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 208. PRIVACY & DISCLOSURE PROVISIONS.

- (a) **PURPOSE.**—The purpose of this section is—
- (1) to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government;
 - (2) to ensure that individuals and public interest organizations are given timely and comprehensive notice of agency activities which implicate the processing of personal information; and
 - (3) to ensure that agencies are publicly accountable for the processing and safeguarding of personal information.
- (b) **PRIVACY IMPACT ASSESSMENTS.**—
- (1) **RESPONSIBILITIES OF AGENCIES.**—
 - (A) **IN GENERAL.**—An agency shall take actions described under subparagraph (B) before—
 - (i) developing or procuring information technology that collects, maintains, processes, or disseminates information that is in an identifiable form;
 - (ii) initiating a new collection of information that—
 - (I) will be collected, maintained, processed, or disseminated using information technology; and
 - (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government; or

(iii) materially modifying, repurposing, or altering the agency's use of information technology covered by clause (i) or a collection of information covered by clause (ii).

(B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall—

- (i) conduct a privacy impact assessment;
- (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
- (iii) after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, and publication in a online, publicly searchable database of agency privacy documentation to be developed and maintained by the Director.

(C) PERMISSIBLE WITHHOLDING OF INFORMATION.—

(i) To the extent that information contained in a privacy impact assessment falls within one or more of the exemptions set forth in subsection 552(b) of title 5, the agency may withhold that information notwithstanding subparagraph (B)(iii), except that no information contained in a privacy impact assessment may be withheld on the grounds that it is deliberative or predecisional.

(ii) If an agency withholds any portion of a privacy impact assessment under subparagraph (C)(i), the agency shall take reasonable steps necessary to segregate and release all nonexempt information contained in the assessment.

(D) COPY TO DIRECTOR.—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

(E) TIMING OF ASSESSMENTS—

(i) An agency shall commence preparation of a privacy impact assessment as close as possible to the time the agency considers taking an action described in subparagraph (A). The agency must conduct, ensure the review of, and publish a privacy impact assessment early enough that the assessment will serve as an important contribution to the decisionmaking process and will not be used to rationalize or justify decisions already made.

(ii) In any event, an agency may not undertake an action described in subparagraph (A) prior to satisfying the requirements of subparagraph (B).

(F) PRIVACY THRESHOLD ANALYSES—

(i) If an agency intends to take an action that may plausibly satisfy subparagraph (A), it shall promptly conduct a privacy threshold analysis to determine whether in fact such action satisfies subparagraph (A) and would thus trigger the requirements of subparagraph (B) if undertaken.

(ii) An agency shall promptly make each privacy threshold analysis publicly available through the website of the agency, publication in the Federal Register, and the online database described in subparagraph (B), provided that an agency may withhold information contained in a privacy threshold analysis pursuant to subparagraph (C) as if it were information contained in a privacy impact assessment.

(2) CONTENTS OF A PRIVACY IMPACT ASSESSMENT.—

(A) IN GENERAL.—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) GUIDANCE.—The guidance shall—

(i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and

(ii) require that a privacy impact assessment address—

(I) what information is to be collected;

(II) why the information is being collected;

(III) the intended use of the agency of the information;

(IV) with whom the information will be shared;

(V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(VI) how the information will be secured; and

(VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the “Privacy Act”).

(3) RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

(A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;

(B) oversee the implementation of the privacy impact assessment process throughout the Government; and

(C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

(c) PRIVACY PROTECTIONS ON AGENCY WEBSITES.—

(1) PRIVACY POLICIES ON WEBSITES.—

(A) GUIDELINES FOR NOTICES.—The Director shall develop guidance for privacy notices on agency websites used by the public.

(B) CONTENTS.—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—

- (i) what information is to be collected;
- (ii) why the information is being collected;
- (iii) the intended use of the agency of the information;
- (iv) with whom the information will be shared;
- (v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
- (vi) how the information will be secured; and
- (vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the “Privacy Act”), and other laws relevant to the protection of the privacy of an individual.

(2) PRIVACY POLICIES IN MACHINE-READABLE FORMATS.—

The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

(d) DEFINITION.—In this section, the term “identifiable form” means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
