U.S. Department of Justice

THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER AND THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

PRIVACY AND CIVIL LIBERTIES ACTIVITIES SEMI-ANNUAL REPORT

FIRST SEMI-ANNUAL REPORT, FY 2021

OCTOBER 1, 2020 – MARCH 31, 2021

United States Department of Justice
Semi-Annual Section 803 Report

Message from the Chief Privacy and Civil Liberties Officer

I am pleased to present the Department of Justice's Semi-Annual Report for the period from October 1, 2020 through March 31, 2021 as required by Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2018). Section 803 directs the privacy officers and civil liberties officers of each department, who at the Department of Justice is the Chief Privacy and Civil Liberties Officer (CPCLO), to provide the following information:

- The number and types of privacy reviews undertaken by the CPCLO (including reviews of legislation and testimony, initial privacy assessments, privacy impact assessments, system of records notices, Privacy Act exemption regulations, OMB Circular A-130, data breach incidents, and Privacy Act amendment appeals).
- The type and description of advice undertaken by the CPCLO and the Department's Office of Privacy and Civil Liberties (OPCL).
- The number and nature of privacy complaints received by the CPCLO and OPCL for alleged violations and a summary of the disposition of such complaints.
- The outreach to the public informing it about the activities of the CPCLO.
- The other functions of the CPCLO and OPCL.

Overall, the Department's privacy program is supported by a team of dedicated privacy professionals who strive to reinforce a culture and understanding of privacy within the complex and diverse mission of the Department. The work of the Department's privacy team is evident in the care, consideration, and dialogue about privacy that is incorporated in the daily operations of the Department.

As a member of the Department's privacy team, I am committed to developing innovative, practical, and efficient ways to incorporate and implement privacy requirements and principles as the Department carries out its important mission of protecting and serving the American public.

Peter A. Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

I. INTRODUCTION

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2018) (hereinafter "Section 803"), requires designation of a senior official to serve as the Attorney General's principal advisor on privacy and civil liberties matters and imposes reporting requirements on certain activities of such official. The Department of Justice's ("Department" or "DOJ") Chief Privacy and Civil Liberties Officer (CPCLO), in the Office of the Deputy Attorney General, serves as the principal advisor to the Attorney General on these matters, and is supported by the Department's Office of Privacy and Civil Liberties (OPCL).

Specifically, Section 803 requires periodic reports[1] related to the discharge of certain privacy and civil liberties functions of the Department's CPCLO, including information on: the number and types of privacy reviews undertaken by the CPCLO; the type of advice provided and the response given to such advice; the number and nature of complaints received by the Department for alleged violations; and a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such an officer. To provide a standard reportable framework, the Department has coordinated with the Office of Management and Budget (OMB) in order to tailor this report to the missions and functions of the Department's CPCLO.

II. PRIVACY REVIEWS

Pursuant to Section 803, this First Semi-Annual Report for Fiscal Year 2021 includes "information on the number and types of reviews undertaken."[2] Among these are the reviews the Department conducts of information systems and other programs to ensure that privacy issues are identified and analyzed, in accordance with federal privacy laws such as the Privacy Act of 1974, as amended, 5 U.S.C. § 552a ("Privacy Act"), the privacy provisions of Section 208 of the E-Government Act of 2002, 44 U.S.C. § 3501 (note), as well as federal privacy policies articulated in OMB guidance.[3] Regular reviews conducted pursuant to the requirements of Section 803 include the following:

1. **Proposed legislation, as well as testimony, and reports prepared by departments and agencies within the Executive Branch:**

   OPCL and the CPCLO review proposed legislation, testimony, and reports for any privacy and civil liberties issues.

[1] On July 7, 2014, the statute was amended to require semiannual submissions of the periodic reports rather than quarterly submissions. *See id*. § 2000ee-1(f) (2018); Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014).
[2] *See* 42 U.S.C. § 2000ee-1(f)(2)(A).
[3] *See e.g.*, OMB Circular No. A-130, Managing Information as a Strategic Resource, 81 Fed. Reg. 49689 (July 28, 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

2. **Initial Privacy Assessments (IPA):**

An IPA is a privacy compliance tool developed by the Department as a first step to: facilitate the identification of potential privacy issues; assess whether privacy documentation is required; and ultimately ensure the Department's compliance with applicable privacy laws and policies.[4] OPCL coordinates and reviews IPAs conducted by Department components.[5] For purposes of this First Semi-Annual Report for Fiscal Year 2021, this number represents IPAs that OPCL has reviewed and closed (issuance of a Final Determination).

3. **Privacy Impact Assessments (PIA):**

A PIA is an analysis, required by Section 208 of the E-Government Act of 2002, of how information in identifiable form is processed to: ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[6] For purposes of this First Semi-Annual Report for Fiscal Year 2021, this number represents PIAs that OPCL and/or the CPCLO have reviewed, approved, and/or closed.

4. **System of Records Notices (SORN):**

A SORN is a notice document required by the Privacy Act that describes the existence and character of a system of records, including the categories of individuals whose records are in the system; the categories of records; and the routine uses of the records.[7] The SORN is published in the *Federal Register*. For purposes of this First Semi-Annual Report for Fiscal Year 2021, this number represents published SORNs that have exhausted their comment periods.

5. **Privacy Act Exemption Regulations:**

The Privacy Act provides that agencies may exempt some systems of records from certain provisions of the Act. A Privacy Act exemption regulation is the regulation promulgated by an agency and published in the *Federal Register* that provides the reasons why a system of records maintained by the agency is exempt from certain

[4] For further information about the Department's IPA process, *see* https://www.justice.gov/opcl/privacy-compliance-process.
[5] The DOJ CPCLO (Acting) has delegated to the FBI Privacy and Civil Liberties Officer the authority to approve FBI Privacy Threshold Analyses ("PTAs" - FBI's equivalent of IPAs) with those approved PTAs accessible to the DOJ CPCLO or designee. IPA numbers indicated in this Report do not include FBI PTA numbers.
[6] *See* OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A, Section II.A.6 (Sept. 26, 2003), https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf.
[7] *See* 5 U.S.C. § 552a(e)(4).

provisions of the Privacy Act.[8] For purposes of this report, this number represents published Privacy Act exemption regulations that have resulted in final rules that have taken effect.

6. **Information Collection Notices:**

An information collection notice is a notice to individuals as required by subsection 552a(e)(3) of the Privacy Act.[9] The notice, which must be on the form used to collect the information or on a separate form that the individual can retain, includes the authority for collecting the information; the principal purposes for which the information is intended to be used; the routine uses of the information; and the effects on the individual, if any, of not providing all or any of part of the requested information. For purposes of this First Semi-Annual Report for Fiscal Year 2021, OPCL's review to determine whether an information collection notice is required occurs during the IPA and final determination review.

7. **Other Assessments of Privacy Program Requirements:**

For purposes of this First Semi-Annual Report for Fiscal Year 2021, reviews are conducted on an annual basis in coordination with the Federal Information Security Modernization Act (FISMA)[10] reviews. Specific details of such FISMA reviews are submitted through the annual FISMA report.

On July 28, 2016, OMB released an update to OMB Circular A-130 titled, *Managing Information as a Strategic Resource*.[11] OMB Circular A-130 serves as the governing document for the management of federal information resources. Appendix II to OMB Circular A-130, *Responsibilities for Managing Personally Identifiable Information*, outlines many of the responsibilities for agencies managing information resources that involve personally identifiable information (PII). These responsibilities include a number of requirements for agencies to integrate their privacy programs into their Risk Management Framework, including but not limited to, the selection, implementation, and assessment of the Appendix J[12] privacy controls. OPCL is currently collaborating with the Department's Office of the Chief Information Officer (OCIO) to ensure that all requirements outlined in OMB Circular A-130 are satisfied.

8. **Data Breaches:**

The DOJ Instruction 0900.00.01, *Reporting and Response Procedures for a Breach of Personally Identifiable Information*, was updated February 16, 2018, to account for OMB Memorandum M-17-12 requirements. The Instruction defines a breach as "the loss of

[8] *See id.* § 552a(j), (k).
[9] *See id.* § 552a(e)(3).
[10] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).
[11] *See supra* note 3.
[12] National Institute for Standards and Technology, NIST Special Pub. No. 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. It includes both intrusions (from outside the organization) and misuse (from within the organization)." The Instruction applies to all DOJ components and personnel that process, store, or transmit DOJ information, and contractors and other users of information systems that support the operations and assets of DOJ. For purposes of this report, this number depicts DOJ data breaches reported to OPCL by the Justice Security Operations Center during the reporting period.[13]

9. **Privacy Act Amendment Appeals:**

A Privacy Act amendment appeal is an appeal of an initial agency action regarding a request from an individual to amend their record that is maintained in a Privacy Act system of records.[14] For purposes of this report, this number represents the number of appeals that have been adjudicated and closed by OPCL.

PRIVACY REVIEWS	
Type of Review	**Number of Reviews**
Legislation, testimony, and reports	276
Initial Privacy Assessments	47
Privacy Impact Assessments[15] • COPS FOIAXpress • CRM CLOUD Act Case Management & Data Retrieval Systems (CLOUD) • FBI Bioterrorism Risk Assessment Group (BRAG) Database • FBI Next Generation Identification Iris Service (NGI-Iris Service) • FBI Passport Visa Database (PVDB) • FBI Threat Intake Processing System (TIPS) • OJP Justice Grants System (JustGrants) • TAX Office Automation System (TAX-OAS)	10
System of Records Notices[16] • SORN OJP-016, Justice Grants System (JustGrants)	1

[13] These numbers do not include FBI data breach numbers, which are reported in FBI's Section 803 report for the same reporting period.
[14] *See* 5 U.S.C. § 552a(d)(2), (3).
[15] DOJ PIAs, https://www.justice.gov/opcl/doj-privacy-impact-assessments. Note: Two of the PIAs included in the number of reviews have not been listed because of the sensitivity of the associated systems.
[16] DOJ SORNs, https://www.justice.gov/opcl/doj-systems-records.

PRIVACY REVIEWS	
Type of Review	**Number of Reviews**
Privacy Act Exemption Regulations	0
Data breach reviews	47
Privacy Act Amendment Appeals	8

III. ADVICE

Pursuant to Section 803, First Semi-Annual Report for Fiscal Year 2021 includes "the type of advice provided and the response given to such advice."[17] The CPCLO's responsibilities include the provision of both formal and informal advice addressing the issuance of a wide variety of formal written policies, procedures, guidance, or interpretations of privacy requirements for certain circumstances or business processes. This advice has been drafted or authorized by the CPCLO to respond to issues or concerns regarding safeguards for privacy and civil liberties and relates to the issuance of regulations, orders, guidance, agreements, or training. The CPCLO received appropriate responses to the formal and informal advice provided.

For this semi-annual period, the CPCLO and OPCL continued working with DOJ components and inter-agency partners to address many international privacy questions affecting the Department, as well as international privacy matters, which included discussions with the United Nations Special Rapporteur on Privacy.

For this semi-annual period, the CPCLO and OPCL continued advising Department components on the impact of emerging technologies on privacy and civil liberties. For example, given the emergence of Artificial Intelligence (AI), and consistent with Executive Order 13859, Maintaining American Leadership in Artificial Intelligence,[18] and Executive Order 13960, Promoting Use of Trustworthy AI in the Federal Government,[19] OPCL has been involved in a number of Department- and government-wide initiatives, including the Department's newly established AI Community of Interest, to ensure that the Department's use of AI is developed and deployed in a manner that fosters public trust and confidence, while protecting privacy, civil rights, civil liberties, and other American values.

The CPCLO and OPCL attended the International Conference of Data Privacy and Protection Commissioners, which is an organization comprising 110 privacy and data protection authorities from across the world that provides leadership at the international level in data protection and privacy. In October 2020, the CPCLO and OPCL virtually attended the Global Privacy Assembly, formerly known as International Conference of Data Privacy and Protection Commissioners (ICDPPC). The CPCLO and the OPCL Acting Director attended both the closed

[17] *See* 42 U.S.C. § 2000ee-1(f)(2)(B).
[18] 84 Fed. Reg. 3967 (Feb. 14, 2019), https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf.
[19] 85 Fed. Reg. 78939 (Dec. 8, 2020), https://www.govinfo.gov/content/pkg/FR-2020-12-08/pdf/2020-27065.pdf.

sessions for Data Protection Authorities and the open session for invited representatives from industry, academia, and other non-governmental entities.

OPCL continues to represent the CPCLO as an active member of the DOJ Insider Threat Working Group pursuant to DOJ Order 0901 (Feb. 12, 2014), which established the DOJ Insider Threat Prevention and Detection Program (ITPDP) and mandated that the ITPDP "include appropriate protections for legal, privacy, civil rights, and civil liberties requirements." OPCL is also an active member of the NT-50 Insider Threat Legal Community of Practice.

The CPCLO and OPCL continue to participate in a number of working groups, including but not limited to:

- Open Government working groups internally and in the inter-agency. OPCL also advised on implementing the Information Quality Act and assisted in updating DOJ guidance;
- DOJ-wide Social Media Working Group. OPCL also handled all DOJ social media-related privacy compliance documentation;
- Artificial Intelligence (AI) and Machine Learning (ML) working groups. In particular, the CPCLO and OPCL continued to coordinate with stakeholders, to ensure that impacts to privacy and civil liberties are a primary consideration as agencies investigate whether, and how, to develop and/or deploy the use of AI/ML technologies;
- Meetings with international officials. The CPCLO and OPCL met with international officials to discuss the US privacy framework and international privacy matters.
- Section 230 Working Group. The CPCLO and OPCL worked with representatives across the Department to coordinate a both public and private event aimed at updating Section 230 of the Communications Decency Act and worked to draft proposed legislation.
- Crime Victims and Witnesses Attorney General Guidelines Working Group. The CPCLO and OPCL worked to update attorney general guidelines to provide stronger privacy protections to crime victims and witnesses as a matter of DOJ policy.
- Investment Review working groups (IT Acquisition Review/Department Investment Review Council). The CPCLO and OPCL participate in IT Acquisition Review and Department Investment Review Committee meetings to ensure Department investments are privacy compliant and aligned with existing Department privacy policy.
- DOJ-wide Unmanned Aircraft Systems (UAS) Working Group. OPCL advised the Department on privacy and civil liberties-related aspects of the development of UAS and Counter-UAS policies.

The CPCLO and OPCL continues to mitigate the operational, security, and privacy risks caused by the intrusion into the Department's Microsoft O365 email environment.

The CPCLO and OPCL continued participating in a number of training-related initiatives within the Department, and creating and posting LearnDOJ training, hosting in-person training events, and publishing videos of those events more broadly.

In response to the requests of other Federal agencies, received by OPCL through its public-facing "Privacy Inbox" email address, OPCL provided training regarding, *inter alia,*

agency responsibilities under the Privacy Act of 1974, the E-Government Act of 2002, OMB Guidance, and NIST Special Publications.

IV. COMPLAINTS

Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2018), this First Semi-Annual Report for Fiscal Year 2021 includes "the number and nature of the complaints received by the department, agency, or element concerned for alleged violations."[20] A privacy complaint encompasses a written allegation (excluding complaints filed in litigation against the Department) concerning a violation of privacy protections in the administration of the programs and operations of the Department that is submitted to or through the CPCLO and/or OPCL. Complaints directly received by components without notice to the CPCLO and/or OPCL are handled by components and are not counted for purposes of this report. Privacy complaints are separated into three categories:

1. Process and procedural issues (such as whether appropriate consent and/or notice was given, or collection was proper);
2. Redress issues that are outside of the Privacy Act amendment process (issues such as misidentification or correction of personally identifiable information are within the amendment process scope); and
3. Operational law enforcement issues (such as complaints regarding persons' privacy being violated; also complaints of statutory Privacy Act violations).

A civil liberties complaint encompasses a written allegation (excluding complaints filed in litigation against the Department) of a problem with or violation of civil liberties safeguards concerning the handling of personal information by the Department in the administration of Department programs and operations that is submitted to or through the CPCLO and/or OPCL.

For each type of privacy or civil liberties complaint received by the CPCLO and/or OPCL during the semi-annual period, the report will include the number of complaints in which (1) responsive action was taken or (2) no action was required. In the event a complaint is received within five business days of the last day of the close of a semi-annual period, the complaint may be counted and addressed in the subsequent semi-annual period if time constraints hinder a thorough examination of the complaint in semi-annual period in which it is received.

In addition to privacy and civil liberties complaints that, by the definitions above, pertain to the Department, OPCL receives correspondence of privacy and civil liberties inquiries that are not amenable to disposition by DOJ as a complaint. OPCL may respond to such correspondence in a number of ways, such as by referring the correspondent to the appropriate non-DOJ entity

[20] *See* U.S.C. § 2000ee-1(f)(2)(C).

for assistance.[21] The number of inquiries referred outside DOJ, broken down by category, are reflected in the table below.

PRIVACY AND/OR CIVIL LIBERTIES INQUIRIES/COMPLAINTS					
Type of Inquiry or Complaint	**Number of Complaints Handled by DOJ**	**Disposition of Complaints Handled by DOJ**			**Inquiries Referred Outside of DOJ**
		Adjudicated by OPCL	**Referred to Component for Review**	**Referred to Office of Inspector General**	
Process and Procedure	0	0	0	0	1
Redress	0	0	0	0	0
Operational	0	0	0	0	15
Civil Liberties Complaints	0	0	0	0	4
Total	0	0	0	0	20

V. INFORMING THE PUBLIC

Pursuant to Section 803, the CPCLO shall "otherwise inform the public of the activities of such officer, as appropriate and in a manner consistent with the protection of classified information and applicable law."[22] The CPCLO and OPCL have continued to engage stakeholders in the privacy community. They have conducted outreach to the privacy advocacy community, the technology industry, and international organizations. The CPCLO also participated in a number of speaking engagements to promote transparency of the Department's policies, initiatives, and oversight with respect to the protection of privacy and civil liberties.

VI. OTHER FUNCTIONS

Pursuant to Section 803, the First Semi-Annual Report for Fiscal Year 2021 "shall include information on the discharge of each of the functions of the officer concerned."[23] Throughout the reporting period, the CPCLO and OPCL have also worked with the Privacy and Civil Liberties Oversight Board and OMB to address privacy concerns, as well as ways to improve agency outreach. Moreover, the CPCLO and OPCL have met with other Federal agencies to improve inter-agency coordination, and to discuss agency privacy practices and

[21] OPCL might refer correspondents to other federal agencies, state agencies, state attorneys general, local police, local agencies, or even state bar associations to assist in locating a reduced or no-fee attorney to help them with their issues. Also, OPCL in some cases informs the correspondent that OPCL is unable to assist them with their issue, or determines that the inquiry does not warrant any response, although OPCL does not report numbers for these situations.
[22] *See* 42 U.S.C. § 2000ee-1(g)(2).
[23] *See* 42 U.S.C. § 2000ee-1(f)(2).

common concerns. These meetings enable OPCL to review and assess the Department's information and privacy-related policies, and make improvements where appropriate and necessary.

OPCL completed a comprehensive revision of the *Overview of the Privacy Act of 1974*, an important resource for government privacy officials. The 2020 Edition includes legislative and case law updates from the past 5 years, and significant enhancements to improve readability.

The CPCLO and OPCL have also worked on several projects for the Federal Privacy Council (FPC), including teaching an introductory privacy class to a wide group of agency privacy officials at a Privacy "Bootcamp" and contributing to the Federal Privacy Council's Executive Committee. Additionally OPCL attorneys participated on various speaking engagements at FPC to discuss the 2020 Edition of the *Overview of the Privacy Act of 1974*.

The CLOUD Act authorizes the Attorney General, with the concurrence of the Secretary of State, to enter into an executive agreement with foreign governments governing access by a foreign government to data. During the evaluation period, the U.S. continued its negotiations with Australia on a CLOUD Act Executive Agreement,[24] and the CPCLO and OPCL continued to assist the Department in meeting many of its disclosure obligations under the CLOUD Act.

The Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act), Pub L. No. 116-50, 133 Stat. 1073, 5 U.S.C. § 552a note, requires each agency to accept electronic identity proofing and authentication processes for the purposes of allowing an individual to provide prior written consent for the disclosure of the individual's records, or access the individual's records, in accordance with the Privacy Act. During this reporting period, the CPCLO and OPCL, in coordination with the Office of Information Policy and the Justice Management Division, began efforts to implement the CASES Act requirements.

Finally, during the reporting period, OPCL led the Department's efforts, in coordination with the Department of Homeland Security, to update the *Privacy and Civil Liberties Guidelines: Cybersecurity Information Sharing Act of 2015*. CISA 2015 requires the Attorney General and the Secretary of Homeland Security to jointly develop, submit to Congress, and make publicly available interim and final guidelines relating to privacy and civil liberties which govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with activities authorized in CISA 2015. The final guidelines were last updated in 2018 and then again in January 2021.[25]

---

[24] Press Release, U.S. Department of Justice, Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton (Oct. 7, 2019) https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

[25] Department of Justice & Department of Homeland Security, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (Jan. 4, 2021), https://www.cisa.gov/sites/default/files/publications/CISA_PCL_Guidelines_Periodic_Review_2020_final.pdf.