U.S. DEPARTMENT OF JUSTICE

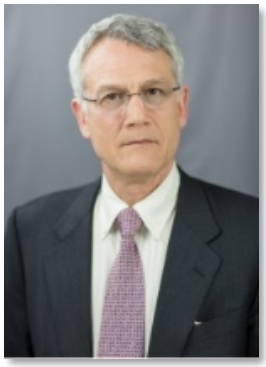
ANNUAL PRIVACY REPORT

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

OCTOBER 1, 2016 – SEPTEMBER 30, 2020

(MULTI) ANNUAL PRIVACY REPORT

MESSAGE FROM THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER



I am pleased to present the Department of Justice's (Department or DOJ) Annual Privacy Report, describing the operations and activities of the Chief Privacy and Civil Liberties Officer (CPCLO) and the Office of Privacy and Civil Liberties (OPCL), in accordance with Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005. This report covers the period from October 1, 2016, through September 30, 2020.

The Department's privacy program is supported by a team of dedicated privacy professionals who strive to build a culture and understanding of privacy within the complex and diverse mission work 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.

During this reporting period, there has been an evolving landscape of technological development and advancement in areas such as artificial intelligence, biometrics, complex data flows, and an increase in the number of cyber security events resulting in significant impacts to the privacy of individuals. Thus, the CPCLO and OPCL have developed new policies and guidance to assist the Department with navigating these areas, some of which include the following: implementation of the Department's Security and Privacy Assessment and Authorization (SPAA) Handbook, which adopts the National Institute of Standards and Technology's Risk Management Framework at the Department and assists with meeting the requirements of the Office of Management and Budget's (OMB) Circular A-130, Managing Information as a Strategic Resource; implementation of DOJ Order 0601, Privacy and Civil Liberties, which applies to all Department components and sets forth the roles and responsibilities of the CPCLO, OPCL, Heads of Components, and Senior Component Officials for Privacy (SCOPs), reaffirming the Department's commitment to protecting privacy and civil liberties; and working cross-functionally with the Justice Management Division and the Office of the Chief Information Officer to implement DOJ Instruction 0900.00.01, Reporting and Response Procedures for a Breach of Personally Identifiable Information which incorporates OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information at the Department.

As a member of the Department's privacy team, I am committed to continuing the development of 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

Table of Contents

LEGISLATIVE LANGUAGE

This report has been prepared in accordance with Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005,[1] which states:

Section 1174. PRIVACY OFFICER

> (d) **ANNUAL REPORT**. -- The privacy official shall submit a report to the Committees on the Judiciary of the House of Representatives and of the Senate on an annual basis on activities of the Department that affect privacy, including a summary of complaints of privacy violations, implementation of section 552a of title 5, United States Code, internal controls, and other relevant matters.

BACKGROUND

The principal mission of the CPCLO and OPCL is to ensure the trust of the American People in the Department's operations through the shaping of new policies and laws affecting privacy and civil liberties, and overseeing the Department's compliance with established privacy law and policy. As the Department harnesses new information technologies, particularly in connection with its law enforcement and national security missions, the CPCLO and OPCL use their expertise to effectively identify, assess, and mitigate risks to privacy and civil liberties. This report covers the period from October 1, 2016, to September 30, 2020, and discusses the continued efforts of the CPCLO and OPCL to safeguard individual privacy and civil liberties while protecting DOJ's overall mission.

1. THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER

The CPCLO serves as the principal advisor to the Attorney General, Department Leadership, and components on issues relating to privacy and civil liberties policy and compliance. The CPCLO is also responsible for ensuring Departmental compliance with federal privacy laws and policies. The Department appointed its first CPCLO in 2006 pursuant to the Violence Against Women and Department of Justice Reauthorization Act of 2005.[2] The CPCLO is designated by the Attorney General and reports to the Deputy Attorney General as a member of the Office of the Deputy Attorney General. The CPCLO serves as the Department's principal advisor on privacy policy in connection with the Department's collection, use, maintenance, and disclosure of personally identifiable information (PII)[3] and all issues of privacy and civil liberties when implementing or developing laws, regulations, policies, procedures, or guidelines related to the Government's counterterrorism efforts.[4] The CPCLO is also responsible for overseeing the Department's compliance with established privacy laws and policies, including the Privacy Act of 1974, as amended[5] ("Privacy Act"), and Section 208 of the E-Government Act of 2002.[6]

---

[1] 28 U.S.C. § 509 note (2018).
[2] *See id*.; *see also* Implementing Recommendations of the 9/11 Commission Act of 2007 § 803, 42 U.S.C. § 2000ee-1 (2018).
[3] The Department defines PII as "information that can be used to distinguish or trace an individual's identity, alone or when combined with other information that is linked or linkable to a specific individual." DOJ Order 0601, *Privacy and Civil Liberties* (May 14, 2020).
[4] *See* 28 U.S.C. § 509 note; *see also* 42 U.S.C. § 2000ee-1.
[5] 5 U.S.C. § 552a (2018).
[6] 44 U.S.C. § 3501 note (2018).

2. THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

The Office of Privacy and Civil Liberties (OPCL) was established as a separate office in March 2008 to support the work of the CPCLO, consolidate the Department's privacy compliance, policy, and legal work, and provide consistency and leadership to all Department components on privacy and civil liberties issues. Peter Winn has been the Department's CPCLO since 2017, and is an experienced attorney in the career Senior Executive Service, with demonstrated expertise in privacy law, policy, and compliance. Katherine Harman-Stokes is the Director (Acting) and Deputy Director of OPCL, and also is an attorney with many years of experience and a deep understanding of United States and international privacy law and policy. Additionally, OPCL is comprised of a team of privacy attorneys and analysts, which include the Senior Counsel, Attorney-Advisors, Privacy Analysts, and a Program Specialist, and Privacy Program Management Officer. Each OPCL staff attorney is responsible for a defined set of Department components, and specializes in certain subject areas of federal information privacy law.

OPCL supports both parts of the two-fold mission of the CPCLO, providing advice on new legal or policy proposals affecting privacy and civil liberties, as well as overseeing the Department's compliance with existing privacy laws and policies. OPCL supports the CPCLO's advisory function by reviewing all legislative, regulatory and other policy proposals which involve privacy and civil liberties, particularly in connection with law enforcement and national security. OPCL supports the CPCLO's compliance function by overseeing the Department's adherence to federal privacy laws, regulations, policies, and other authorities in all of its programs and information systems. OPCL accomplishes this two-fold mission by:

- Reviewing legislative and policy proposals pertaining to privacy and civil liberties issues arising from the Department's operations;
- Serving on working groups and developing policies, guidelines, and procedures for the Department's law enforcement and national security operations;
- Advising the Department in connection with information sharing agreements and arrangements with state, local and tribal authorities, as well as with foreign governments;
- Advising Department leadership and components concerning international data protection and privacy laws and policies, and participating in international organizations charged with addressing data protection and privacy;
- Developing and providing guidance to Department components to ensure they comply with federal information privacy laws, regulations, and policies;
- Overseeing the Department's response to any data breaches that occur, consistent with applicable laws and policies;
- Reviewing and finalizing all Department privacy compliance documentation, including system of records notices and accompanying exemption regulations pursuant to the Privacy Act, and privacy impact assessments pursuant to Section 208 of the E-Government Act of 2002;
- Adjudicating appeals of denials by DOJ components to amend records under the Privacy Act;
- Establishing and providing annual and specialized privacy compliance, legal, and awareness training to Department personnel;
- Ensuring adequate procedures for responding to privacy and civil liberties inquiries and complaints from the public; and

- Preparing and/or coordinating the semi-annual and annual reports in accordance with, among other legal requirements, Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, the Federal Information Security Modernization Act (FISMA) of 2014, Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005, and the Federal Agency Data Mining Reporting Act of 2007.

3. SENIOR COMPONENT OFFICIALS FOR PRIVACY

OPCL supports the CPCLO with overseeing the compliance by the Department's components with respect to existing privacy laws, regulations, and policies. Pursuant to DOJ Order 0601, "Privacy and Civil Liberties" (May 14, 2020), each component has designated a Senior Component Official for Privacy (SCOP), who is accountable and responsible for the component's privacy program. The SCOPs, in turn, coordinate their components' privacy issues and concerns through OPCL to the CPCLO and Department leadership. The Department's SCOPs have varied resources. Some components, such as the Federal Bureau of Investigation (FBI), have large privacy and civil liberties units; others may only have a single person assigned to this position on a part-time basis. To assist SCOPs in their important role, OPCL has developed a "SCOP Manual" which explains, in detail, the duties of the SCOPs, and provides them with materials to help in the discharge of these duties. Many of the Department's SCOPs work closely on a day-to-day basis with OPCL when seeking OPCL's guidance on questions of law and policy. OPCL also holds periodic SCOP meetings to discuss any changes or significant issues related to the Department's Privacy Program, announcements, suggestions, and concerns. OPCL also provides annual role-based training programs focused on the responsibilities of the SCOPs.

THE COMPLIANCE PROCESS

The Department's collection, maintenance, and use of information about individuals are critical to its ability to effectively enforce the law, defend the interests of the United States, and ensure public safety. As it fulfills these missions, the Department must also fulfill its responsibility to manage and protect the sensitive personally identifiable information (PII) it collects on individuals. During this reporting period, OPCL and the Office of the Chief Information Officer (OCIO) developed and implemented the Department's Security and Privacy Assessment and Authorization (SPAA) Handbook, which adopts the National Institute of Standards and Technology's Risk Management Framework at the Department and assists with meeting the requirements of the Office of Management and Budget's (OMB) Circular A-130, *Managing Information as a Strategic Resource*.[7] The Handbook embeds privacy assessments and controls into the system design and development lifecycle. Ensuring an appropriate balance between meeting the government's critical information needs, while scrupulously guarding against unwarranted invasions of personal privacy, is at the core of the federal privacy laws that OPCL administers as part of the Department's privacy compliance program.

1. INITIAL PRIVACY ASSESSMENTS

The privacy compliance process begins when the Department first determines it needs to collect, maintain, disseminate, or otherwise use PII, or materially revise existing processes through updated technologies or other activities. The Department has established the Initial Privacy Assessment (IPA) template, which consolidates various threshold privacy compliance requirements into a single, unified, and comprehensive process. The IPA template consists of questions designed to help components and OPCL determine whether a particular information system requires further privacy assessment and/or documentation (e.g., completion of a Privacy Impact

[7] OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016).

Assessment (PIA), development or modification of a System of Records Notice (SORN)), implementation of enhanced privacy controls, or raises other privacy issues or concerns. It also bridges the information technology (IT) security and privacy processes and communities.

To account for the evolving information technologies used throughout the Department, and to better identify and assess the PII collected by the Department components, OPCL updated the IPA template in May 2019. The Department has incorporated the IPA process into the Department's risk management framework outlined in the SPAA Handbook, including in the IT information system "Authorization to Operate" (ATO) security authorization process, and utilizes a software application managed by OCIO to track compliance of electronic systems with the FISMA. This ATO process requires program managers for IT systems, whether in development or operation, to evaluate security and privacy controls to ensure that security and privacy risks have been properly identified and mitigated. The inclusion of the IPA in this process assists in identifying information assets requiring appropriate security and privacy controls and permits better identification of those systems containing and maintaining PII.

Through the IPA process, components can identify steps to mitigate any potential adverse impact on privacy at the outset of the information collection or program. For example, a component may determine that the collection and use of Social Security Numbers (SSNs) or other sensitive PII within a system is not necessary. The component can then forego the collection of such PII in accordance with applicable privacy protection directives and policies.

2. PRIVACY IMPACT ASSESSMENTS

Section 208 of the E-Government Act of 2002 requires all federal agencies to conduct a PIA in certain circumstances before developing or procuring information technology that collects, maintains, or disseminates information in identifiable form or before initiating a new electronic "collection of information" that will be collected, maintained, or disseminated using information technology.[8] PIAs provide an analysis of how information is handled to ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[9]

Through the IPA process, OPCL generally makes final determinations on whether a component is required to complete a PIA. In conducting a PIA, the Department considers the privacy impact from the beginning of a system's development through the system's lifecycle to ensure that system developers and owners have made technology and operational choices that incorporate privacy protections into the underlying architecture of the system. As with the IPA, PIAs have been incorporated in the DOJ IT security risk management framework, which ensures the identification of all IT systems that require PIAs and allows OPCL and Department components to resolve privacy and related security issues before a system is certified and accredited.

In May 2019, consistent with the SPAA Handbook, OPCL updated the Department's PIA template to include more detailed guidelines for properly assessing issues and responding to the questions in the PIA template.[10] In addition, the Department created an alternative PIA template for components, known as the

[8] *Id.*
[9] *See* OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Attachment A, § II-A(f) (Sept. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.
[10] https://www.justice.gov/opcl/file/629231/download.

"Admin PIA" template. The Admin PIA template is designed primarily for those systems used for administrative purposes, rather than for law enforcement purposes or for any other duties or responsibilities related to the component's mission. PIAs appropriate for publication can be found on OPCL's website at www.justice.gov/opcl/doj-privacy-impact-assessments.

3. SYSTEM OF RECORDS NOTICES

Under the Privacy Act, agencies must assess their handling of information about individuals and ensure the collection, maintenance, use, disclosure, and safeguarding of such information is appropriate and lawful.[11] As part of this compliance process, agencies must review each system of records that contains such information and document and describe the proper maintenance and handling of such information in a SORN. A SORN provides the public with details about a system of records, including its purpose for collection and maintenance, the categories of individuals serving as the subject of such records, the categories of information to be used and collected by the agency, the location where the agency maintains the information, the means of access and correction available to the individual, the security safeguards that will protect the information, and the parties with whom and under what conditions the agency may share the information in the system.[12] The Department of Justice maintains more than 200 systems of records. The SORNs for these systems can be found on OPCL's website at http://www.justice.gov/opcl/doj-systems-records.[13]

Through the IPA process, OPCL advises the Department's components on the proper maintenance of information in systems of records in order to ensure compliance with the numerous Privacy Act requirements that govern such information. For example, once OPCL determines, via the IPA tool, that a particular information system qualifies as a system of records, it may be necessary to draft a SORN or modify an existing SORN and any accompanying Privacy Act exemption regulation. Coordinating with the relevant components, OPCL reviews all such existing or proposed SORNs and updates, and any accompanying exemption regulations, managing the review and approval process through issuance by the CPCLO.[14] As part of this work, OPCL assists components in reviewing routine use disclosures included in SORNs to ensure that each routine use disclosure contemplated is compatible with the purpose for which the information was collected.

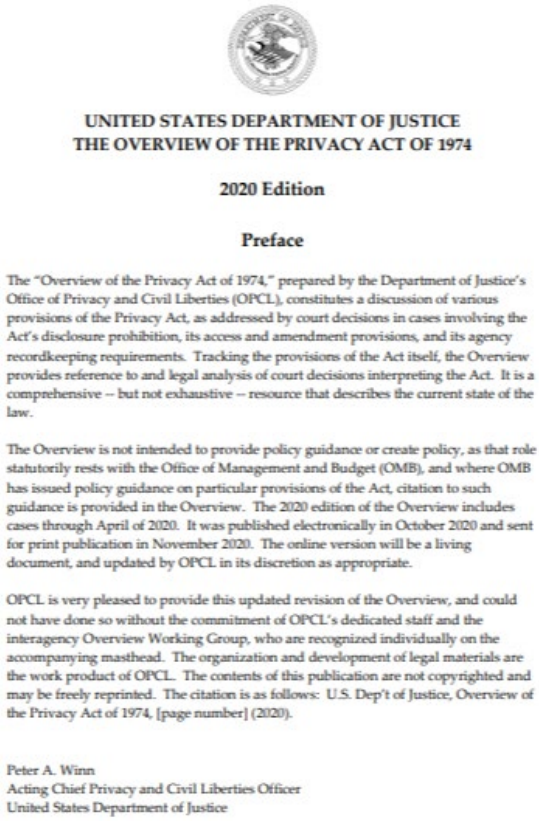
During this reporting period, OPCL revised the Department's guidance and templates on SORNs and exemption regulations in order to provide better assistance to components when drafting and preparing these documents. In addition to publishing SORNs and regulations, OPCL advises components on preparing other Privacy Act documents, such as Privacy Act consent forms,[15] and Privacy Act notice statements, which provide actual notice to an individual about an agency's collection authority and the possible uses of information collected from individuals.[16]

LEGAL GUIDANCE AND TRAINING PROVIDED BY OPCL

OPCL provides legal advice and guidance to Department leadership and components on certain federal information privacy compliance requirements, policies, and initiatives. In this capacity, OPCL advises

[11] *See* 5 U.S.C. § 552a.
[12] *See id.* § 552a(e)(4); *see also* OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* (2016).
[13] There may be several subsystems of records that are covered by the same SORN.
[14] The Attorney General delegated his authority to carry out these responsibilities to the CPCLO by order in January 2008.
[15] *See* 5 U.S.C. § 552a(b).
[16] *See id.* § 552a(e)(3).

components about the applicability and requirements of federal information privacy laws, such as the Privacy Act and the E-Government Act of 2002, to help components perform their operations and functions while protecting the privacy rights of individuals. In addition, OPCL advises Department components on privacy issues that arise in connection with litigation, policy development, and program implementation; advises components on international data protection and privacy laws that may impact the sharing or use of PII for mission purposes; develops and conducts privacy training; and reviews pending legislation, Congressional testimony, Executive Orders, and reports.



UNITED STATES DEPARTMENT OF JUSTICE
THE OVERVIEW OF THE PRIVACY ACT OF 1974

2020 Edition

Preface

The "Overview of the Privacy Act of 1974," prepared by the Department of Justice's Office of Privacy and Civil Liberties (OPCL), constitutes a discussion of various provisions of the Privacy Act, as addressed by court decisions in cases involving the Act's disclosure prohibition, its access and amendment provisions, and its agency recordkeeping requirements. Tracking the provisions of the Act itself, the Overview provides reference to and legal analysis of court decisions interpreting the Act. It is a comprehensive -- but not exhaustive -- resource that describes the current state of the law.

The Overview is not intended to provide policy guidance or create policy, as that role statutorily rests with the Office of Management and Budget (OMB), and where OMB has issued policy guidance on particular provisions of the Act, citation to such guidance is provided in the Overview. The 2020 edition of the Overview includes cases through April of 2020. It was published electronically in October 2020 and sent for print publication in November 2020. The online version will be a living document, and updated by OPCL in its discretion as appropriate.

OPCL is very pleased to provide this updated revision of the Overview, and could not have done so without the commitment of OPCL's dedicated staff and the interagency Overview Working Group, who are recognized individually on the accompanying masthead. The organization and development of legal materials are the work product of OPCL. The contents of this publication are not copyrighted and may be freely reprinted. The citation is as follows: U.S. Dep't of Justice, Overview of the Privacy Act of 1974, [page number] (2020).

Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer
United States Department of Justice

OPCL has published, and in 2020 updated, the Department of Justice's *Overview of the Privacy Act of 1974* (*Overview*).[17] This publication provides a thorough and up-to-date legal analysis of the Privacy Act's agency record-keeping requirements, disclosure prohibition, access and amendment provisions, and provides a reference to, and legal analysis of, court decisions interpreting the Privacy Act's provisions. The *Overview* is a valued resource and is widely used throughout the federal government for guidance in this field.

Furthermore, OPCL conducts a comprehensive and meticulous training program to ensure that appropriate personnel are well-trained to spot issues, resolve problems, and ensure compliance with privacy laws and policies. During this reporting period, elements of OPCL training included: annual mandatory training for all Department employees and contractors, annual voluntary training provided for all federal agencies, breach response training regarding DOJ Instruction 0900.00.01 (Reporting and Response Procedures for Breach of Personally Identifiable Information), and issue-specific training as requested by Senior Component Officials for Privacy. During the reporting period, OPCL has initiated the development of incident response role-based training modules for Department employees engaged in law enforcement or litigation, among other critical functions. For the reporting period, OPCL hosted three annual DOJ Privacy Fora: The DOJ Privacy Forum is an event that features engaging panel discussions on important and timely privacy topics. The May 2019 OPCL Privacy Forum included panels on international privacy issues, developments in privacy litigation, legislative initiatives related to draft federal consumer privacy bills, and component privacy program development. The 2019 Forum was attended by approximately 250 federal employees.

The CPCLO was accredited as an observer and, along with the Director, attended the annual meetings of the International Conference of Data Privacy and Protection Commissioners (ICDPPC), now known as the Global Privacy Assembly (GPA), in 2017-2020. The GPA is an organization comprising 130 data protection and privacy authorities from across the world that provides leadership at the international level in data protection and privacy. In each of the annual meetings, the CPCLO and OPCL Director attended both the closed sessions for Data Protection Authorities and the open session for invited representatives from industry, academia, and other non-governmental entities. At the October 2019 meeting in Tirana, Albania, they also hosted two side events: a panel discussion on Privacy Best Practices and Transparency in Law Enforcement, featuring the Chief Privacy Officer

[17] See Overview of the Privacy Act of 1974 (2020 Edition), https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition.

of the Danish National Police, the Data Protection Specialist at EUROPOL, a member of France's data protection authority (the Commission nationale de l'informatique et des libertés, (CNIL)), and a Professor from the Washington College of Law; and a breakfast meeting for a discussion of biometrics, featuring the founder and executive director of the World Privacy Forum and others.

In September 2019, the United States hosted the annual review of the EU-U.S. Privacy Shield Framework, which provided "companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union (EU) to the United States in support of transatlantic commerce." The CPCLO and OPCL worked closely with colleagues at the Office of the Director of National Intelligence (ODNI), the Department of Commerce, and other Federal departments and agencies on responding to questions from the EU and presenting USG updates during the Shield Review at the 2019 review and earlier reviews. As of summer 2020, over 5,000 companies relied upon the Privacy Shield to support their data transfers. In July 2020, the Court of Justice of the (EU) issued a judgment declaring the Privacy Shield "invalid." The CPCLO and OPCL advise Department leadership on the Court's decision, and are supporting efforts by the Department and other U.S. Government agencies to address the Court's judgment. Additional information concerning the EU-U.S. Privacy Shield Framework can be found at https://www.privacyshield.gov.

The CPCLO and OPCL continued participating in a number of training-related initiatives within the Department, 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, including those received by OPCL through its public-facing "Privacy Inbox" email address, OPCL provided training on a significant range of topics, including agency responsibilities under the Privacy Act of 1974, the E-Government Act of 2002, OMB Guidance, and NIST Special Publications.

The CPCLO and OPCL continued to participate in a number of different internal and external working groups. Among others, the CPCLO and OPCL participated in:

- 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;

- Artificial Intelligence (AI) and Machine Learning (ML) working groups. In particular, the CPCLO and OPCL continued to coordinate with internal and external 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.

- Discussions with international officials through the International Visitor's Leadership Program regarding the US privacy framework and international privacy matters.

- Various resolutions and statements related to the UN General Assembly and other international organizations.

1. TRAINING RECEIVED BY OPCL

In order to provide effective guidance to the privacy audience, it is imperative that the CPCLO and OPCL staff remain informed of current privacy issues and policies. During the report period, the CPCLO and OPCL

staff attended the International Association of Privacy Professionals (IAPP) Annual Global Privacy Summits; Federal Privacy Council (FPC) Boot Camp and the Annual Summits hosted by the Federal Privacy Council; National Security Law Institute training hosted by the Center for National Security Law at the University of Virginia School of Law; Homeland Security Law Institute training hosted by the American Bar Associations Section of Administrative Law & Regulatory Practice; Federal Privacy Summit Workshops hosted by the Federal Privacy Council; Privacy Law Scholars Conferences; and Intelligence Community Legal Conferences.

2. LEGAL AND POLICY REVIEW PROVIDED BY OPCL AND THE CPCLO

During the reporting period, OPCL conducted legal and policy reviews pertaining to many Department matters and functions. To facilitate the compliance with the Department's legal obligations and policy requirements, the following types of reviews were conducted by OPCL and the CPCLO, among others.

- **Proposed legislation, policies, testimony, and reports prepared by departments and agencies within the Executive Branch:**
  OPCL and the CPCLO review proposed legislation, policies, testimony, and reports for any privacy and civil liberties issues. More than 200 requests for review are typically received annually.

- **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.[18] IPAs are conducted by Department components with coordination and review by OPCL.

- **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.[19]

- **System of Records Notices (SORN):**
  A SORN is a notice document required by the Privacy Act of 1974 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.[20] The SORN is published in the Federal Register.

- **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

[18] For further information about the Department's IPA process, *see* https://www.justice.gov/opcl/privacy-compliance-process.
[19] *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.
[20] *See* 5 U.S.C. § 552a(e)(4).

in the Federal Register that provides the reasons why a system of records maintained by the agency is exempt from certain provisions of the Act.[21]

- **Privacy Act Notices:**
  A Privacy Act Notice is a notice to individuals as required by subsection (e)(3) of the Privacy Act.[22] 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.

- **Assessments required by OMB Circular A-130:**
  OMB Circular A-130 reviews include assessments of the following: SORNs to ensure that they are accurate and up to date; routine uses to ensure that they are still required and compatible with the purpose for which the information was collected; record practices and retention schedules to ensure that they are still appropriate; exemption regulations to ensure that they are still necessary; contracts to ensure that appropriate Federal Acquisition Regulation language is used to bind the contractor to provisions of the Privacy Act; Computer Matching programs to ensure compliance; civil or criminal violations of the Privacy Act to assess concerns; and agency programs for any privacy vulnerabilities.[23] These reviews are conducted on an annual basis in coordination with the Federal Information Security Modernization Act (FISMA)[24] 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*.[25] 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[26] privacy controls. OPCL and OCIO implemented these new requirements in the Department's Security and Privacy Assessment and Authorization (SPAA) Handbook.

- **Data Breaches or Incidents:**
  The DOJ Instruction 0900.00.01, *Reporting and Response Procedures for a Breach of Personally Identifiable Information*,[27] was updated during the reporting period to account for OMB Memorandum M-17-12 requirements. The Instruction defines a data breach as "the loss of 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

[21] *See id.* § 552a(j), (k).
[22] *See id.* § 552a(e)(3).
[23] *See supra* note 4.
[24] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).
[25] *See supra* note 4.
[26] 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.
[27] *See* DOJ Instruction 0900.00.01, *Reporting and Response Procedures for A Responsibilities for Managing Breach of Personally Identifiable Information* (Feb. 16, 2018).

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)." In addition, the Instruction defines an incident as: "An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." The Instruction applies to all DOJ components and personnel that process, store, or transmit DOJ information including contractors and other users of information systems that support the operations and assets of DOJ. The CPCLO and the Chief Information Officer co-chair the Department's Core Management Team that convenes in the event of certain significant data breaches involving PII, which advises on whether notification to Congress is required, and the types of mitigation measures that may be appropriate. During this reporting period, one breach of PII involving the U.S. Marshals Service resulted in notification to Congress.

- **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 information that is maintained in a Privacy Act system of records.[28] Refer to OPCL's Semi Annual Section 803 Reports for the number of appeals that have been adjudicated and closed by OPCL every six months.[29]

- **Inspector General Coordination:**
  By statute and policy, the CPCLO and OPCL are required to coordinate with the Inspector General of the Department of Justice on matters such as the FISMA privacy audit and significant data breach situations. In addition, OPCL enjoys a close working relationship with the Inspector General's Office, and frequently receives requests for advice on questions of privacy law and policy.

3. ADVICE AND OUTREACH PROVIDED BY THE CPCLO AND OPCL

Throughout this reporting period, the CPCLO and OPCL have developed and participated in events aimed at educating and engaging the federal workforce, the advocacy community, and the public on privacy-related topics, examples of which include the following.

- **SPEAKING ENGAGEMENTS**

  - From 2016 to 2019, the CPCLO and various OPCL attorneys participated on various panels during the Federal Privacy Council's Annual Privacy Summit.

  - The CPCLO has served on the faculty of the Federal Privacy Council "boot camp" since 2016 when this training program for federal privacy professionals began.

  - The CPCLO and OPCL staff have attended and participated on panels at the Global Privacy Summit of the International Association of Privacy Professionals (IAPP) from 2016-2020.

[28] *See* 5 U.S.C. § 552a(d)(2), (3).
[29] https://www.justice.gov/opcl/reports.

- The CPCLO participated as an observer at the International Conference of Data Protection and Privacy Commissioners now known as the Global Privacy Assembly, attending the annual meetings in Hong Kong, China in October 2017, Brussels, Belgium, in October 2018, and Tirana, Albania in 2019. He also participated at the virtual annual meeting held in October 2020.

- From 2016 until 2018, the CPCLO served as an Advisor helping to fashion the American Law Institute's "Principles of the Law, Data Privacy."

- The CPCLO serves as an ex officio member of the National Domestic Communications Assistance Center Executive Advisory Board.

- The CPCLO serves as an observer on a committee of the Uniform Law Commission developing model state privacy legislation.

- In June 2016, 2017, 2018, 2019 and 2020, the CPCLO attended and served on panels at the annual Privacy Law Scholars Conference held alternatively in Berkeley, California and Washington, D.C.

- In December 2017, the CPCLO spoke on a panel on "Digital Westphalia" held by the Atlantic-Bruecke, in Berlin, German.

- In April 2019, the CPCLO gave a speech about possible domestic privacy legislation at the American Enterprise Institute.

- OPCL attorneys spoke at the American Bar Association (ABA), Young Lawyers Division Spring Conference, on "Confronting Cyber Threats and the Mission of the Department of Justice," which included a short publication in the ABA's *TYL* 2018; American Society of Access Professionals 11th Annual National Training Conference and at a 2019 conference; Specialized Analytic Seminar Series: Privacy, Civil Rights, and Civil Liberties, in Lincoln, Nebraska; U.S. Department of Veterans Affairs (VA) Privacy Service Speaker Series Virtual Panel Event titled "It Takes a Team: A Deeper Look at How Privacy, Records and FOIA Intersect"; and a DOJ Office of Information Policy FOIA Conference.

- Upon request, OPCL attorneys also provided training on various privacy topics such as breach response to handling personnel data at other agencies, including the U.S. Department of Agriculture and the U.S. Postal Service.

- **MEETING WITH PRIVACY ADVOCATES AND COMMUNITY STAKEHOLDERS**

  - The CPCLO and OPCL staff meet frequently with privacy advocates, business organizations, and academics to discuss issues of concern to them.

- **INCREASING TRANSPARENCY OF PRIVACY POLICIES**

OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services* (Nov. 8, 2016) places certain requirements on Federal agency public-facing websites and digital services to meet the Administration efforts to maintain high standards of effectiveness and usability and provide quality information to the public that is readily accessible on government websites. OPCL, in coordination with OCIO, led the effort

to comply with the privacy requirements outlined in OMB M-17-06. These and related efforts in updating OPCL's central resource page dedicated to the Department's privacy program, https://www.justice.gov/privacy, increase transparency and better educate the public on the work of the CPCLO and OPCL. Specifically, during the reporting period, OPCL:

- Updated the OPCL webpage to act as the central resource page dedicated to the Department's privacy program on DOJ's principal website.[30] DOJ's Privacy Program Page serves as a central source for information about DOJ's practices with respect to PII;

- Added a page listing and providing links to up-to-date matching notices and agreements for all active matching programs in which DOJ participates;[31]

- Revised the DOJ System of Records Notices Page to provide visitors with links to the DOJ System of Records Notices published in the Federal Register, as well as the Privacy Act exemptions claimed by a DOJ System of Records and promulgated in the Code of Federal Regulations;[32]

- Updated the list and provided links to all Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f);[33]

- Added a page providing instructions in clear and plain language for individuals who wish to request access to or amendment of their records pursuant to 5 U.S.C. § 552a(d).[34]

- Regularly updating OPCL's public "home" page at https://www.justice.gov/opcl, and "Frequently Asked Questions" page, at https://www.justice.gov/opcl/faq, including information concerning redress, e.g., OPCL's handling of complaints and inquiries from the public;

- Adding links to the central resource page in both the Department's "About Us" page and the Department's website privacy policy, https://www.justice.gov/doj/privacy-policy;

- Adding a "Judicial Redress Act of 2015 and the U.S.-EU Data Protection and Privacy Agreement" page to educate the public on the Judicial Redress Act of 2015, and inform the public of those countries and Federal agencies designated by the Attorney General as "covered countries" and "designated Federal agencies or components."

PRIVACY POLICY AND LEADERSHIP

1. INTRA-AGENCY LEADERSHIP

Within the Department, the CPCLO and OPCL collaborate and engage with Department components in the development of new policies and programs that affect the Department's handling of PII. Examples of such engagements include:

[30] https://www.justice.gov/privacy.
[31] https://www.justice.gov/opcl/computer-matching-agreements-and-notices.
[32] https://www.justice.gov/opcl/doj-systems-records.
[33] https://www.justice.gov/opcl/doj-privacy-act-regulations.
[34] https://www.justice.gov/opcl/doj-privacy-act-requests.

- **Use of Social Media to Communicate with the Public**

During this reporting period, OPCL has coordinated with other DOJ components to revise its comprehensive social media policies for communicating with the public. The Department's Social Media Working Group (SMWG) includes the Public Affairs Office, OPCL, the Office of Records Management Policy (ORMP), the Departmental Ethics Office (DEO), the Justice Management Division's (JMD) Office of General Counsel (OGC), and other relevant DOJ components. The SMWG reviews various issues, including privacy and records management issues, in order to ensure that the Department's uses are in accordance with applicable laws, policies, and regulations.

In coordinating with the SMWG, OPCL has:

- Developed formal policies on the appropriate approval for components wishing to utilize social media tools, and the appropriate collection, use, maintenance, and dissemination of personal information on its public facing websites. https://www.justice.gov/social;

- Revised the Department-wide Adapted Privacy Impact Assessment for the Department Use of Third-Party Social Media Tools to Communicate with the Public, https://www.justice.gov/Use_Third_Part_Social_Media_Tools/download; and

- Drafted, cleared, and published a concise policy on the Department's website privacy policy: https://www.justice.gov/doj/privacy-policy. Specifically, OPCL worked with the SMWG to substantially revise and update "The Department's Use of Third-Party Resources, Applications and Websites" section.

- Worked directly with components to review proposed uses of social media for privacy concerns, and provided approval and compliance documentation for those requests.

- **Judicial Redress Act Implementation**

Over the reporting period, OPCL was significantly involved in assisting the Department in implementing the Judicial Redress Act of 2015 (JRA), 5 U.S.C. § 552a note. The JRA extends certain rights of judicial redress established under the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, to citizens of certain foreign countries or regional economic organizations.[35]

On December 2, 2016, the European Union (EU) undertook the final steps necessary under EU law to approve an executive agreement between the U.S. and the EU (the Parties) relating to privacy protections for personal information transferred between the U.S., the EU, and the EU Member States for the prevention, detection, investigation, or prosecution of criminal offenses, known as the Data Protection and Privacy Agreement (DPPA). The DPPA establishes a set of protections that the Parties are to apply to personal information exchanged for the purpose of preventing, detecting, investigating, or prosecuting criminal offenses. On January 17, 2017, the Attorney General designated 26 countries and one regional economic integration organization as "covered countr[ies]," and four Federal agencies and nine components of other Federal agencies as "designated Federal agenc[ies] or component[s]," to be effective on February 1, 2017, which is the date of entry into force of the

[35] https://www.justice.gov/opcl/judicial-redress-act-2015.

DPPA. On February 12, 2019, the Department of Justice designated the United Kingdom (the "UK") as a "covered country," effective on April 1, 2018, the date the DPPA became applicable to the UK. The Acting CPCLO and OPCL were significantly involved in preparing and finalizing the Attorney General's designations.

- **Data Breach Response and Reviews**

OPCL led the Department's efforts to comply with OMB Memorandum M-17-12 "Preparing for and Responding to a Breach of Personally Identifiable Information" (Jan. 3 2017). OMB M-17-12 sets forth the policy for Federal agencies to prepare for and respond to a breach of personally identifiable information (PII). Implementation of OMB M-17-12 required the extensive communication, collaboration, teamwork, and partnership within OPCL and throughout the Department. During the reporting period, OPCL:

- Modified over 200 DOJ System of Records Notices to update the routine uses paragraph allowing for the disclosure of records in the event of a breach;
- Revised the Department's General Users and Privileges Users Rules of Behavior to require all DOJ employees to appropriately report suspected or confirmed data breaches;
- Revised DOJ Instruction 0900.00.01, *Reporting and Response Procedures for a Breach of Personally Identifiable Information*, to include all necessary elements of OMB M-17-12 in the Department's breach response plan; and
- Conducted a tabletop exercise for the DOJ Core Management Team—the Department's Breach Response Team—to test its policies and procedures and help ensure that the DOJ Core Management Team are familiar with DOJ Instruction 0900.00.01.

- **Computer Matching Agreements and the DOJ Data Integrity Board**

Throughout the reporting period, OPCL and the CPCLO continued to ensure that the Department was in compliance with the Computer Matching and Privacy Protection Act of 1988, as amended.[36] These activities included coordinating the review of all Computer Matching Agreements that were either established, re-established, or renewed during the reporting period. The CPCLO serves on the DOJ Data Integrity Board, and is responsible for reviewing and approving Computer Matching Agreements entered into on behalf of the Department. OPCL also assisted in preparing the Annual Computer Matching Activity Reports, in compliance with OMB Circular A-108.[37] During this reporting period, the Data Integrity Board re-established or renewed three computer matching agreements.

- **Executive Order 13636**

In February 2013, the President signed Executive Order 13636, which directs federal departments and agencies to establish, expand, or prioritize a number of activities to improve cybersecurity for U.S. critical infrastructure. Section 5 of the Executive Order requires Senior Agency Officials for Privacy and Civil Liberties to conduct assessments of the privacy and civil liberties risks of their agency activities under the Executive Order

[36] Pub. L. No. 100-503, 102 Stat. 2507 (1988), (codified at 5 U.S.C. § 552a)
[37] DOJ Annual Computer Matching Activity Reports can be found at: https://www.justice.gov/opcl/computer-matching-agreements-and-notices; *see supra* note [12 (re A-108)].

based on the Fair Information Practice Principles (FIPPs) and report on such assessments. During this reporting period, the CPCLO and OPCL coordinated with Department leadership to incorporate privacy and civil liberties protections into the Department's implementing instructions, section 4(a) of the Executive Order, to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The CPCLO and OPCL also worked closely with other Department components to review relevant activities implementing the Order, and to ensure that the FIPPs were and will continue to be appropriately considered and incorporated in such activities.

- **Privacy and the Department's Risk Management Framework**

On July 28, 2016, OMB updated OMB Circular A-130, *Managing Information as a Strategic Resource* (2016). Appendix II of OMB Circular A-130, *Responsibilities for Managing Personally Identifiable Information*, placed a number of privacy-related requirements on federal agencies and explicit responsibilities on the agency's Senior Agency Official for Privacy (SAOP), who at DOJ is the CPCLO. Specifically, agency privacy programs now have explicit responsibilities in the assessment and authorization process for DOJ information systems.

During the reporting period, OPCL, in coordination the Justice Management Division, Office of the Chief Information Officer, Cybersecurity Services Staff, prepared revisions to the Department's Risk Management Framework to ensure that DOJ and its components properly comply with all privacy requirements and properly identify and mitigate privacy risks. These revisions included the formal adoption of DOJ policies that recognize privacy as a necessary, integral, and distinct part of the DOJ Risk Management Framework. Additionally, the revisions included changes to the renamed "Department Security and Privacy Assessment and Authorization Handbook" (SPA&A Handbook), which outlines the process, documentation requirements, and automated tools essential to performing the successful security and privacy assessment and authorization of all DOJ information systems. Overall, the SPA&A Handbook serves as the foundation for assessing privacy controls and authorizing the operation of DOJ information systems.

- **Social Security Number Reduction Initiatives**

OPCL will continue its training initiatives to help ensure that component officials are fully supported in their efforts to reduce the use of SSNs in component programs, and will continue to work with DOJ components through the Department's privacy compliance process to identify and eliminate unnecessary uses of SSNs at the outset of a Department program, system, or operation.

In addition, OPCL is working with components to ensure compliance with the Social Security Number Fraud Reduction Act of 2017 (SSN Act), 42 U.S.C. § 405 note. The SSN Act requires agencies to submit to Congress an initial report detailing documents mailed by the agency during the previous year that contain a full SSN. The SSN Act also requires that agencies develop a plan to ensure that no documents are mailed containing a full SSN unless the head of the agency determines that inclusion of the SSN is necessary. This plan must be fully implemented by 2022. OPCL has submitted its initial report, and two subsequent annual reports on behalf of the Department, which includes a SSN reduction plan, and is in the process of implementation.

The SSN Act also requires agencies to issue regulations specifying the circumstances under which the inclusion of SSNs on a document sent by mail are necessary by 2022. OPCL is working to amend 28 CFR part 16, subpart D to include instructions for the partial redaction of social security account numbers where feasible; and a requirement that social security account numbers not be visible on the outside of any package sent by mail.

- **Information Collection Request Privacy Assessments**

In 2018, in order to ensure that the Department complies with its privacy notice requirements when engaging in an information collection subject to the Paperwork Reduction Act of 1995, as amended, 44 U.S.C. § 3501 *et seq.* (PRA), the Acting CPCLO instituted a new assessment requirement that DOJ components must complete prior to reporting an Information Collection Request (ICR) to the Office of Management and Budget (OMB), Office of Information and Regulatory Affairs (OIRA). The PRA establishes a statutory framework for minimizing reporting burdens on individuals and maximizing the potential utility of the information collected by an agency. To comply with the PRA, agencies must, among other things, complete an ICR for review and submission to OMB OIRA, which is responsible for government-wide information resources management policy.

Recently, OMB OIRA has required agencies to state whether each ICR will involve the collection of PII and whether the ICR includes a form that requires a Privacy Act Statement under 5 U.S.C. § 552a(e)(3). To assist DOJ components in answering these questions, OPCL has developed a new assessment tool, called an "Information Collection Request – Privacy Assessment" (ICR-PA). The ICR-PA will help components decide whether a collection instrument submitted to OMB OIRA as part of an ICR must comply with certain privacy notice requirements, which will appear either directly on the instrument or in a manner readily available for the individual completing it.

- **Cyber Digital Task Force**

On July 2, 2018, the Attorney General issued a memorandum establishing the Cyber Digital Task Force.[38] The Task Force's first task was to issue a comprehensive assessment of the Department's "work in the cyber area, and to identify how federal law enforcement can even more effectively accomplish its mission in this vital and evolving area." The Acting CPCLO, a member of the task force, and OPCL attorney contributors, were significantly involved in assisting the Office of the Deputy Attorney General in authoring the assessment report, which was issued in July 2018.[39]

2. INTER-AGENCY LEADERSHIP

The CPCLO and OPCL also engage in leadership roles within the federal privacy community and increased their participation and role in inter-agency privacy activities during this reporting period. Examples of such participation include:

- **Federal Cybersecurity Enhancement Act**

The CPCLO and OPCL assisted the Department in responding to DHS's assessment requirements under Title II of the Cybersecurity Act of 2015. Under Title II, the DHS CPO was required to consult with DOJ on its review of the DHS policies and guidelines for the government-wide intrusion detection and prevention capabilities, known as the EINSTEIN program, to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications. The CPCLO was responsible for reviewing this assessment, in which OPCL provided legal research, writing, and strategic assistance.

[38] https://www.justice.gov/opa/press-release/file/1035457/download.
[39] https://www.justice.gov/archives/ag/page/file/1076696/download.

- **International Efforts**

The CPCLO and OPCL staff worked extensively with the United States government's foreign partners to promote the sharing of information for authorized mission purposes.

- *Global Privacy Assembly (GPA), f/k/a, International Conference of Data Privacy and Protection Commissioners (ICDPPC)*—As noted earlier, the GPA is an organization comprising 130 privacy and data protection authorities from across the world that provides leadership at the international level in data protection and privacy. In October 2015, the CPCLO attended the 37 International Conference of Data Privacy and Protection Commissioners (ICDPPC). The CPCLO was accredited as an observer for the 38th, 39th, 40th, and 41st ICDPPCs, and in 2016-2019, the CPCLO attended both the closed sessions for Data Protection Authorities and the open session for invited representatives from industry, academia, and other non-governmental entities.

- Throughout the reporting period, the CPCLO and OPCL have engaged with United Nations Officials, including the United Nations Special Rapporteur on Privacy, and have advised the U.S. Department of State, and revised resolutions and other material, concerning privacy and civil liberties matters raised by other countries or international organizations, such as the Freedom Online Coalition, and the Red Cross and Red Crescent Movement.

- From 2017 to 2020, OPCL engaged with foreign officials, including French and Georgian Officials, through the Department of State's International Visitor Leadership Program. These engagements consisted of dialogues pertaining to the U.S. sectoral privacy regime and comparative systems around the world.

- The CPCLO and OPCL attorneys provide training to the interagency on international privacy laws, regulations, and policies.

- **Federal Privacy Council**

On February 12, 2016, the President signed an Executive Order 13719 establishing the Federal Privacy Council (FPC). The FPC serves as the principal interagency forum to improve the Government privacy practices of agencies and help Senior Agency Officials for Privacy better coordinate and collaborate on privacy initiatives, educate the Federal workforce, and exchange best practices. The CPCLO, as DOJ's SAOP, serves as a member of the FPC. OPCL attorneys and analysts regularly participate on FPC committees and working groups.

- **Open Government and Data Initiatives**

The CPCLO and OPCL continue to support the goals of public participation, open data, information quality, and transparency as the Department seeks to integrate privacy and civil liberties into its missions and operations.

- To further the goals of both the Open Government Plan 3.0 and 4.0, the CPCLO and OPCL have taken a number of steps to implement the commitments made in each plan to improve privacy compliance, increase transparency of privacy policies, and enhance sharing of best practices on data privacy. In addition, through the National Action Plan 3.0 and its

assessments, the Department and the CPCLO have committed to enhance transparency of federal use of investigative technologies. These commitments include the Department's issuance of policies on the use of UAS and CSS by law enforcement.

- In January 2019, Congress passed the Foundation for Evidence-based Policymaking Act of 2018. Title II of the Act includes the Open, Public, Electronic and Necessary (OPEN) Government Data Act, which notably requires public government data assets to be published as machine-readable data, as well as a designated agency Chief Data Officer (CDO). Pursuant to OMB's guidance on implementing the Foundations for Evidence-based Policymaking Act (M-19-23), the CDO established the Data Governance Board (Board) to provide enterprise guidance and direction for achieving data management objectives as defined by the Department's Data Strategy, the Federal Data Strategy, and the OPEN Government Data Act. The CPCLO is a Board Member and OPCL attorneys are members of the Department's Data Architecture Working Group that coordinate and facilitate the implementation of Department-wide processes and standards, and for addressing common issues affecting Component data programs and resources.

- On April 24, 2019, OMB issued an updated memorandum, M-19-15*, Improving Implementation of the Information Quality Act,* to reinforce, clarify, and interpret agency responsibilities with regard to responsibilities under the Information Quality Act (IQA). The update required agencies to revise their Information Quality Guidelines. As part of this process, the CPCLO and OPCL worked within the Department to revise the DOJ Guidelines that are available at https://www.justice.gov/information-quality.

- **Cybersecurity Information Sharing Act of 2015 (CISA), Privacy and Civil Liberties Guidelines**

On December 8, 2015, President Obama signed CISA into law, which required 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. The CPCLO and OPCL worked with DHS to draft and finalize both the interim and final guidelines. The final guidelines were effective as of June 15, 2016. As part of the process, the CPCLO and OPCL also participated in interagency and external outreach to obtain stakeholder input.

During the reporting period, OPCL led the Department's efforts, in coordination with the Department of Homeland Security, to update the final privacy and civil liberties guidelines, in accordance with CISA. The updated guidelines were published in June 2018.[40] In addition, OPCL provided insight and guidance on a number of audits evaluating the Federal Government's role in implementing CISA. The Intelligence Community Inspector General's Cybersecurity Information Sharing Act of 2015 Implementation assessment, and the Government Accountability Office's Cybersecurity Information Sharing Act of 2015 audit, were both conducted and completed during the reporting period.

- **Attorney General Guidelines**

[40] Dep't of Justice & Dep't of Homeland Security, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 15, 2018), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines.pdf.

The CPCLO played a key role in working with Department leadership, various elements of the Intelligence Community, and ODNI in completing updates of procedures that govern the conduct of the Intelligence Community as it pertains to collection, retention, and dissemination of U.S. person information. Elements of the Intelligence Community are required by Executive Order 12333 to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the IC element concerned or by the head of a department containing such element, and approved by the Attorney General, consistent with the authorities in the Executive Order, after consultation with the Director of National Intelligence. New procedures became effective for the Office of Intelligence and Analysis in the Department of Homeland Security on January 11, 2017; the CIA on January 17, 2017; and the intelligence components of the Department of Energy on January 17, 2017.

- **Other Leadership Efforts**

In addition, the CPCLO and OPCL participate in other OMB-led or inter-agency privacy working groups and leadership efforts. For example, the CPCLO and OPCL participated in a working group to develop OMB guidance to help federal agencies implement the Do Not Pay (DNP) Initiative under section 5 of the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA); various working groups created to assess the government's policies on Unmanned Aircraft Systems; various working groups created to represent the government's interests in the drafting of federal privacy and data breach legislation; and meetings with members of the PCLOB to discuss Department programs and operations and how privacy and civil liberties issues are considered in the counterterrorism context.

3. PRIVACY AND CIVIL LIBERTIES COMPLAINTS

OPCL receives numerous inquiries from members of the public through physical mail, its email inbox, and main phone number, and has established a process to review such inquiries in a timely manner. In this capacity, OPCL acts as an ombudsman for inquirers to ensure that their inquiries are properly reviewed and responses are properly provided and/or appropriately referred. For this reporting period, OPCL received numerous inquiries from members of the public.

In addition, OPCL received three complaints of privacy and civil liberties violations in connection with the Department's handling of information from FY17-FY20. A "complaint" here is defined as a written allegation, excluding complaints filed in litigation against the Department that concerns a violation of privacy protections in the administration of the programs and operations of the Department. Some examples of the types of privacy and/or civil liberties complaints that were received by OPCL include: a request from an individual seeking assistance to remove information about him from a Department webpage; a potential unlawful disclosure claim resulting in adverse employment issues; alleged dispute regarding collection of social security numbers on DOJ forms; and allegations regarding insufficient safeguarding of information within a DOJ component. In each of these instances, OPCL worked with the affected component to seek resolution and/or referred the complaints to the appropriate Department offices, such as the Office of the Inspector General, for review.

4. PRIVACY ACT AMENDMENT APPEALS

In addition to receiving general privacy inquiries, OPCL adjudicates all appeals of denials by Department components of requests to amend records under subsection (d)(2) of the Privacy Act. OPCL also adjudicates initial requests to amend records received by the Department's senior management offices. Within the reporting period, OPCL adjudicated 48 Privacy Act amendment appeals.

5. ACCOUNTABILITY AND REPORTING

The CPCLO and OPCL are responsible for issuing and contributing to numerous Department privacy reports, including: the Annual Report in accordance with Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005; the semi-annual reports on the activities of the CPCLO and OPCL under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (803 Reports); the Senior Agency Officials for Privacy and Civil Liberties' sections of annual reports in accordance with the FISMA; annual privacy and civil liberties assessments of the Department's activities under section 5(b) of Executive Order 13636; and the annual report under the Federal Agency Data Mining Reporting Act of 2007. Certain reports from this reporting period that have been approved by OMB and transmitted to Congress can be found on OPCL's webpage at https://www.justice.gov/opcl/reports/reports.htm. These reports are described in more detail below:

- **Federal Information Security Modernization Act of 2014 (FISMA) Annual Report**

Federal agencies are required to submit annual reports to OMB regarding their privacy programs in accordance with the FISMA and OMB guidance implementing the FISMA.[41] The annual report reflects the information provided in the Department's IPAs and helps OPCL determine the number of information systems in the Department that collect PII, require a PIA and/or SORN, and for which the Department has completed such documentation. It also requires the CPCLO and OPCL to collect data and report on the Department's privacy program.

- **Privacy and Civil Liberties Activities Semi-Annual Section 803 Reports**

The CPCLO submits the 803 Report to Congress and the PCLOB on a semi-annual basis. Over the course of the reporting period, the content of the 803 Reports has been expanded to provide information related to the fulfillment of certain privacy and civil liberties functions of the CPCLO, including information on the number and types of privacy reviews undertaken; the type of advice provided and the response given to such advice; the number and nature of the complaints received by the Department, agency, or element concerned for alleged violations; and a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of the CPCLO.

- **Executive Order 13636 Privacy and Civil Liberties Assessment Report**

As detailed above, Executive Order 13636 aims to strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with the private sector. Section 5(b) of the Executive Order requires Senior Agency Officials for Privacy and Civil Liberties of agencies engaged in activities under the Executive Order to "conduct assessments of their agency activities," and to provide such assessments to the DHS for consideration and inclusion in a yearly DHS report on the privacy and civil liberties risks of functions and programs undertaken by agencies as called for in the Executive Order. Such assessments "shall include evaluation of activities against the [FIPPs] and other applicable privacy and civil liberties principles, policies, and frameworks."[42] Each fiscal year, OPCL has worked

[41] *See* 44 U.S.C. § 3544(c) (2012); *see also* OMB Memorandum M-17-05, *Fiscal Year 2016 - 2017 Guidance On Federal Information Security And Privacy Management Requirements* (Nov 4, 2016).
[42] Executive Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, § 5(b) (Feb. 19, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

closely with Department components and the Assessments Working Group of the DHS Interagency Task Force to draft the Department's privacy and civil liberties assessments.

- **Websites, Mobile Applications, and Digital Privacy Compliance**

OPCL continues to work with Department components to ensure that they maintain an inventory of websites, applications, social media accounts, and other digital services. The Department maintains on its central website a DOJ Privacy Policy available at https://www.justice.gov/doj/privacy-policy. Per DOJ policy, all public-facing websites must link to the DOJ Privacy Policy on all home pages, major entry pages, and any web page that collects substantial personally identifiable information from the public. If a Department component has a compelling need to establish its own Privacy Policy, the component content authorizer may submit a request for a waiver to the Assistant Attorney General for Administration. Such a request would be assessed in coordination with the CPCLO and OPCL.

In addition, on a quarterly basis, content managers are required to certify to the Department's CIO that their websites are in compliance with Federal and DOJ content policies and guidelines. Included in the quarterly submission is a certification that the components are meeting DOJ Privacy Policy requirements. Additionally, the DOJ Office of Privacy and Civil Liberties has developed a privacy compliance process to identify potential privacy compliance issues that may merit an update to the Department's Privacy Policy.