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, 2013 – SEPTEMBER 30, 2016

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, detailing the 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, 2013, through September 30, 2016.

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.

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.

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
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.

[1] 28 U.S.C. § 509 note (2012).

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, 2013, to September 30, 2016, and discusses the continued efforts of the CPCLO and OPCL to safeguard individual privacy and civil liberties while protecting DOJ's overall mission.

THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER

The CPCLO serves as the principal advisor to the Attorney General and the heads of Department components on issues relating to privacy and civil liberties. The CPCLO is also responsible to ensure 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 part of the Office of the Deputy Attorney General (ODAG) and 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]

THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

OPCL was created as a separate office in 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 information privacy issues. The Director of OPCL reports directly to the CPCLO, and is an experienced attorney in the career Senior Executive Service, with demonstrated expertise in privacy law, policy, and compliance. Additionally, OPCL is comprised of a team of privacy attorneys and specialists, which include the Director, a Deputy Director, four Attorney-Advisors, two Privacy Analysts, and two Contract Support Specialists. 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 advice function by reviewing all legislative,

---

[2] *See id*.; *see also* Implementing Recommendations of the 9/11 Commission Act of 2007 § 803, 42 U.S.C. § 2000ee-1 (2012).
[3] The Department defines PII as "information that can be used to distinguish or trace an individual's identity such as name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." DOJ Order 0601, *Privacy and Civil Liberties* (Feb. 6, 2014).
[4] *See* 28 U.S.C. § 509 note; *see also* 42 U.S.C. § 2000ee-1.
[5] 5 U.S.C. § 552a (2012).
[6] 44 U.S.C. § 3501 note (2012).

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 information 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 with state, local and tribal authorities, as well as with foreign governments.
- Developing and providing guidance to Department components to ensure they comply with federal information privacy laws, regulations, and policies;
- Reviewing and finalizing all Department privacy 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;
- Preparing and/or coordinating the semi-annual and annual reports in accordance with 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; and
- Publishing the *Overview of the Privacy Act of 1974*, a treatise of Privacy Act case law.

SENIOR COMPONENT OFFICIALS FOR PRIVACY

OPCL oversees 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," 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 to the privacy compliance process, announcements, suggestions, and concerns, as well as provides yearly 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 (U.S.), and ensure public safety. As it fulfills these missions, the Department must also fulfill its responsibility to manage and protect the sensitive PII it collects on individuals. 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.

INITIAL PRIVACY ASSESSMENTS

The privacy compliance process begins when the Department first determines it needs to collect, maintain, disseminate, or otherwise use PII. The Department has established the Initial Privacy Assessment (IPA) template, which consolidates various 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 documentation (e.g., completion of a Privacy Impact Assessment (PIA) or development or modification of a System of Records Notice (SORN)) 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 2015. The Department has incorporated the IPA process into its IT certification and accreditation process and the software application used to track compliance of electronic systems with the FISMA. This certification and accreditation process requires program managers for IT systems, whether in development or operation, to evaluate security controls to ensure that security risks have been properly identified and mitigated. The inclusion of the IPA in this process assists in identifying information assets requiring appropriate security 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. During this reporting period, OPCL reviewed and made determinations on a total of 56 IPAs submitted by Department components.

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 collection of such information that will be collected, maintained, or disseminated using information technology.[7] 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

[7] *Id.*

information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[8]

By way of the IPA process, OPCL makes final determinations on whether a PIA is required to be completed by the component. 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 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 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 2015, 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.[9] In addition, the Department created an alternative PIA template for components, known as the "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. The CPCLO reviewed and finalized 16 PIAs during this period, and all PIAs for non-national security systems can be found on OPCL's website at www.justice.gov/opcl/doj-privacy-impact-assessments.

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 legal.[10] 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 will share the information in the system.[11] 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.[12]

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 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. OPCL reviews all such SORNs and accompanying exemption regulations for approval and issuance by the CPCLO.[13] Within this SORN review process, OPCL also 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.

---

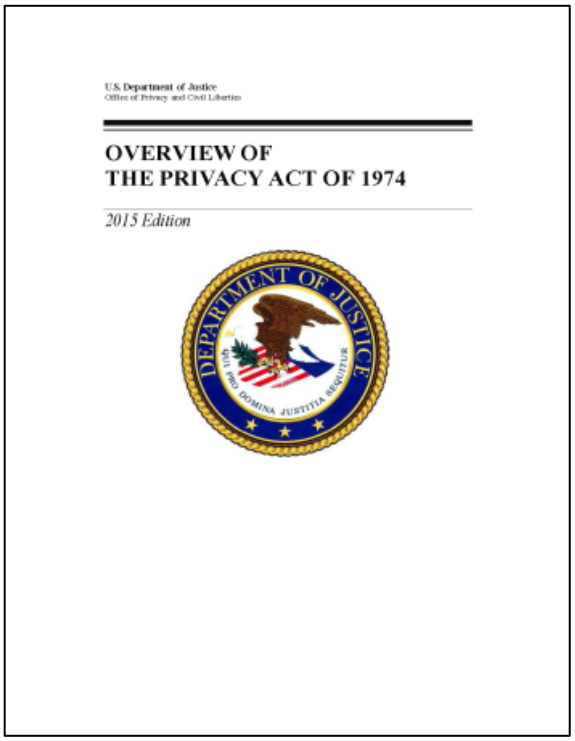
[8] *See* OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Attachment A, § II-A(f) (Sept. 26, 2003), http://www.whitehouse.gov/omb/memoranda_m03-22.
[9] http://www.justice.gov/file/dojpiatemplatemay2015pdf/download.
[10] *See* 5 U.S.C. § 552a.
[11] *See id.* § 552a(e)(4).
[12] There may be several subsystems of records that are covered by the same SORN.
[13] The Attorney General delegated his authority to carry out these responsibilities to the CPCLO by order in January 2008.

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. The Department published 9 new or modified SORNs and published 3 Privacy Act exemption regulations[14] during the reporting period. 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

TRAINING PROVIDED BY OPCL

OPCL attorneys serve as legal counsel for the Department on certain federal information privacy compliance requirements, policies, and initiatives. In this capacity, OPCL advises 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; develops and conducts privacy training; and reviews pending legislation, Congressional testimony, Executive Orders, and reports.


U.S. Department of Justice
Office of Privacy and Civil Liberties

OVERVIEW OF
THE PRIVACY ACT OF 1974

2015 Edition

In 2015, OPCL prepared and issued online and in print, a revised edition of the *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. OPCL is currently working on the 2017 edition of the *Overview*.

OPCL also conducts a comprehensive and robust 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, topics of OPCL training included: overview of Privacy Act requirements; DOJ IT issues; and Hague evidence collection. In 2015, OPCL published on its website a series of Frequently Asked Questions to aid both the public and Department employees in understanding DOJ's privacy compliance program. Finally, OPCL staff also conducts component-specific privacy training, as well as training at other federal agencies upon request.

[14] This number reflects only the number of final Privacy Act exemption regulations published during the reporting period.
[15] *See* 5 U.S.C. § 552a(b).
[16] *See id.* § 552a(e)(3).
[17] http://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

During the reporting period, OPCL hosted its first and second DOJ Privacy Forums. The DOJ Privacy Forum is an internal event that features engaging panel discussions on important and timely privacy topics. In November 2014, OPCL hosted its first DOJ Privacy Forum, which included panels on the FBI's Next Generation Identification (NGI) program, emerging technologies, information sharing, big data, and privacy compliance within the Department. The all-day Forum was attended by almost 80 Department employees, and received positive feedback. In October 2016, OPCL hosted its second Privacy Forum that included panels on Cybersecurity Information Sharing Act of 2015 (CISA) and Executive Order 13636, surveillance technologies, such as Unmanned Aircraft Systems (UAS) and Cell Site Simulators (CSS), insider threat, and breaches and incident response. The second Forum was open to other government agencies and was attended by approximately 250 agency employees.

TRAINING RECEIVED BY OPCL

In order to most effectively achieve their missions, it is important that the CPCLO and OPCL remain informed of current privacy issues and policies. Thus, the CPCLO and OPCL participate in trainings throughout the year, both inside and outside the Department. During the reporting period, OPCL staff attended the International Association of Privacy Professionals Global Privacy Summit, the Intelligence Community (IC) Legal Conference, the Department of Homeland Security (DHS) Annual Privacy Workshop, the Georgetown Law Privacy Center Conference on the 40th Anniversary of the Privacy Act, the Federal Chief Information Officer (CIO) Council Privacy Summit, the Federal Privacy Council's inaugural Federal Privacy Boot Camp, and numerous briefings at various Department components' on-site locations.

LEGAL REVIEW PROVIDED BY OPCL

The Department conducts privacy reviews of information systems and programs to ensure that privacy issues are identified and analyzed in accordance with federal privacy laws enumerated in controlling authorities such as the Privacy Act, the privacy provisions of the E-Government Act of 2002, as well as federal privacy policies articulated in Office of Management and Budget (OMB) guidance, including, but not limited to, OMB Circular A-130. During the reporting period, OPCL conducted 1041 reviews of proposed legislation, testimony, and reports for privacy and civil liberties issues.

OPCL also conducted two reviews of data breach and incident reports. A data breach or incident includes intentional or inadvertent losses of PII in the control of the Department or its contractors who process, store, or possess DOJ PII. For purposes of this report, this number includes data breaches and incidents that have been formally reviewed by the Department's Core Management Team (DOJ's organizational team which convenes in the event of a significant data breach involving PII).[18]

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 education and engaging the federal workforce, the advocacy community, and the public on privacy-related topics:

Speaking engagements:

[18] DOJ Order 0900.00.01, *Incident Response Procedures for Data Breach* (Aug. 6, 2013), http://www.justice.gov/opcl/breach-procedures.pdf.

- On February 26, 2014, the CPCLO served as a guest speaker on a panel titled: "Watching the Watchers: The New Privacy Officers Inside the U.S. Government" at the 2014 RSA Conference.

- On March 17, 2014, the CPCLO participated in conference titled "The Social, Cultural & Ethical Dimensions of 'Big Data' Conference." This conference was co-hosted by the OSTP, the Data & Society Research Institute, and the New York University Information Law Institute.

- On March 27, 2014, the CPCLO moderated a panel titled "Reclaim Your Name: Privacy in the Era of Big Data," at the 62nd American Bar Association (ABA) Section of Antitrust Law Spring Meeting. The panel addressed the latest federal and legislative developments, as well as trends regarding big data, and the implications for business practices.

- On June 19, 2014, the CPCLO participated on a panel titled "Big Data and Discrimination" as part of a workshop titled "Improving Government Performance in the Era of Big Data: Opportunities and Challenges for Federal Agencies." This workshop was hosted by the White House's Office of Science and Technology Policy (OSTP) and the Georgetown University McCourt School of Public Policy's Massive Data Institute. The panel addressed the potential discriminatory effects from the collection and use of big data by federal government agencies.

- On October 9-10, 2014, the CPCLO participated in an ABA event titled "Antitrust Masters Course VII," hosted by the ABA Section on Antitrust Law. On October 9, 2014, the CPCLO was a keynote speaker at the luncheon. On October 10, 2014, the CPCLO participated on a panel titled "Hot Antitrust and Consumer Protection Issues for High-Tech Companies." This panel focused on "hot topics" in antitrust and consumer protection relating to technology that are the subject of recent agency enforcement actions and private litigation.

- On October 30, 2014, the CPCLO participated in roundtables at the "Big Data and Civil Rights Conference," hosted by the Data & Society Research Institute, the Leadership Conference on Civil and Human Rights, and New America's Open Technology Institute.

- On November 12, 2014, the CPCLO presented on a panel titled "What privacy interests have government privacy officials identified and how are they addressed in the counterterrorism context?" as part of the "Defining Privacy Conference" hosted by the Privacy and Civil Liberties Oversight Board (PCLOB).[19]

- On December 2, 2014, the Director of OPCL participated in a panel titled "The Privacy Act @40: A Celebration and Appraisal on the 40th Anniversary of the Privacy Act and the 1974 Amendments to the Freedom of Information Act," hosted by the Georgetown Law's Center on Law and Technology. This panel discussed whether the Privacy Act of 1974 is sufficient for the challenges of today's technology and society.

[19] The PCLOB is an independent agency within the Executive branch charged with assisting the President and other senior Executive Branch officials in ensuring that privacy and civil liberties concerns are appropriately considered in the implementation of all laws, regulations, and policies related to efforts to protect the nation against terrorism. Implementing Recommendations of the 9/11 Commission Act of 2007 § 801, 42 U.S.C. § 2000ee (2012).

- On February 12, 2015, the CPCLO participated in a panel titled "The Internet of Things: Big Data and You" hosted by George Washington University's Trachtenberg School of Public Policy and the ABA's Consumer Protection Section. This panel discussed the potential benefits and challenges, including data security and transparency and choice, of utilizing connected electronic devices.

- On March 5, 2015, the CPCLO presented on a panel titled "The Job of Protecting Both the Nation's Security and Privacy" as part of International Association of Privacy Professionals' (IAPP) 2015 Global Privacy Summit. This panel included Chief Privacy Officers from various federal agencies to discuss their roles and the role of a privacy office within organizations that have national and homeland security missions.

- On June 9, 2015, the CPCLO participated in an IAPP event titled "Privacy: An Equal Playing Field for Women and Men." This panel discussed leading women in privacy in this emerging profession, where success is based on experience and merit.

- On August 12, 2015, the CPCLO presented on a panel titled "A facilitated dialogue concerning the pros and cons of non-public safety UAS operations and their impact on privacy" as part of the "The National Institute of Justice's Unmanned Aircraft Systems Expert Convening" event.

- On September 11, 2015, the CPCLO participated in a Policymaker Roundtable hosted by The Privacy Salon, and participated on a panel discussion titled, "Big Data and the Internet of Things."

- On February 4, 2016, the CPCLO presented on a program titled "Cyber Security Threat – Are Mobile Apps and Internet of Things Gateways to Security Breaches?" at the LegalTech Conference.

- On April 5, 2016, the CPCLO presented on a program titled "Privacy Across Borders: Maintaining Global Trust in Overseas Data Sharing" at the International Association of Privacy Professionals, Global Privacy Summit.

- On April 8, 2016, Attorneys from OPCL participated in a panel titled "Predictive Policing and Sentencing" as part of the Georgetown Law Center Conference, "Color of Surveillance: Government Monitoring of the African American Community." This Conference was organized by the Georgetown Law Center on Privacy & Technology and examined the impact government surveillance has had on the black community.

- On May 3, 2016, the CPCLO participated in a program titled "Privacy and Civil Liberties Interim Guidelines of CISA" hosted by the American Bar Association Cybersecurity, Data Protection, and Privacy Committee.

- On June 9, 2016, Attorneys from OPCL participated in a panel titled "Privacy Considerations and the Cybersecurity Information Sharing Act of 2015 (CISA)," as part of the "CISA Implementation Public Workshop." This Workshop was hosted by the Department of

Homeland Security to engage and educate stakeholders and the general public on CISA implementation and the Automated Indicator Sharing (AIS) initiative.

- On June 15, the CPCLO participated on a program titled "Working With the U.S. Government on Data Security" hosted by the Compliance, Governance, & Oversight Council Summit.

- On September 16, 2016, the CPCLO served as a panelist on a program titled "The Tension Between Privacy and Security" at the ChIPs Women, Tech, Law and Policy Global Summit.

- On September 28, 2016, the CPCLO participated on a "Hot Topics" program at the Cybersecurity Conference for Lawyers, sponsored by Department of Homeland Security and Department of Justice.

Meeting with Privacy Advocates and Community Stakeholders:

- OPCL met with Cultural Vistas and European delegates under the auspices of the U.S. Department of State's International Visitor Leadership Program (IVLP) to discuss transparency of federal government operations and the Department's privacy initiatives and Department's privacy compliance program.

- On March 26, 2014, The CPCLO and OPCL met with privacy advocates to discuss the Department's privacy initiatives and provided an overview of the Department's privacy compliance program. In addition, the CPCLO and OPCL met with privacy advocates to discuss the Big Data Report published by the Executive Office of the President, led by John Podesta, Counselor to the President.

- On April 4, 2014 the CPCLO hosted an interagency meeting with Data Protection Authorities from over 20 jurisdictions.

- In October 2014, the CPCLO also submitted to the White House a description of the conferences and in-person meetings provided by the Department in 2014 in order to enhance collaboration and information sharing about privacy best practices among state and local law enforcement agencies receiving federal grants. This privacy outreach is ongoing, and occurs regularly throughout the country.

- From March 2014 to March 2015, the CPCLO and OPCL participated in meetings with the White House, the PCLOB, and other federal agencies to discuss ways to improve the Department's privacy and civil liberties reports, including the privacy and cybersecurity assessment required by Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. Discussions on improving such reports are still ongoing.

- From January 2013 to June 2016, the CPCLO and OPCL continued to meet with the European Delegation regarding EU-U.S. Data Protection and Privacy Agreement (DPPA) negotiations. For instance, the CPCLO participated in a negotiation session of the DPPA on May 22-23, 2014, in Brussels, Belgium. In concert with such negotiations, the CPCLO led a process that included federal agencies to develop proposed legislation that extends to citizens of certain countries the core benefits that Americans enjoy under the Privacy Act with regard

to information shared with the U.S. for law enforcement purposes. This proposed bill, H.R. 1428, introduced on March 18, 2015, and titled "Judicial Redress Act of 2015," was signed into law on February 24, 2016.[20]

- On February 20, 2015, the CPCLO and OPCL met with members of the civil society advocacy community to discuss making privacy compliance information more accessible and how to use Big Data to support greater openness and accountability. These meetings were hosted by the White House's OSTP.

- On July 20, 2015, OPCL met with civil society representatives on the National Action Plan (NAP) regarding surveillance activities.

- On July 23, 2015, the CPCLO attended a meeting with other Federal Government Chief Privacy Officers hosted by the PCLOB.

Increasing Transparency of Privacy Policies:

- In June 2015, to increase transparency and better educate the public on the work of the CPCLO and OPCL, changes were made to OPCL's website to include a "Frequently Asked Questions" section that details OPCL's mission, structure, and statutory and administrative authorities. The Frequently Asked Questions section can be found on OPCL's website at http://www.justice.gov/opcl/faq.

- Throughout the reporting period, the CPCLO and OPCL have also worked with the PCLOB 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 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.

PRIVACY POLICY AND LEADERSHIP

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:

Social Media

OPCL has continued to work with the Department's Social Media Working Group, which formed in 2010 following OMB's issuance of policies governing the implementation of the Administration's Open Government Initiative.[21] The purpose of this working group is to review proposed uses of social media and other new media communication technologies by the Department for legal and policy issues, such as privacy,

[20] *See* 5 U.S.C. 552a note.
[21] *See* OMB Memorandum, M-10-16, *Open Government Directive* (Dec. 8, 2009), http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.

ethics, records management, and public affairs. As part of the working group's clearance process, OPCL receives IPAs from Department components seeking to use social media or other new media technologies to communicate with the public and reviews the IPAs to ensure that the proposed use is consistent with federal privacy laws, such as the Privacy Act, Section 208 of the E-Government Act of 2002, and OMB policies.[22]

OPCL reviewed social media IPAs during this reporting period. As new media uses have developed, this working group has also reviewed new Department policies on such uses, including reviewing the Department's use of applications on mobile devices. In June of 2015, OPCL and the Social Media Working Group successfully conducted a privacy compliance review prior to the launch of Attorney General Lynch's Twitter account. In an effort to formalize the Department's use of social media to communicate with the public, the Social Media Working Group is in the process of formalizing Department-wide policies on social media use.

Data Breach Response and Reviews

The CPCLO and OPCL participate in the Department's review of incidents and data breaches in accordance with the Department's Incident Response Procedures.[23] The Incident Response Procedures established a Core Management Team (CMT), which is co-chaired by the CPCLO and the Department's CIO. The CPCLO and OPCL are notified, as necessary, of actual or suspected breaches of PII, and provide legal and policy guidance to the CMT regarding the privacy implications associated with data breach incidents and any Department response.

In April 2015, the Office of Personnel Management (OPM) discovered a data breach involving personnel data of current and former Federal government employees, including current and former DOJ employees. A thorough investigation of the initial incident revealed that additional information including background investigation records of current, former, and prospective Federal employees and contractors had been compromised. In response to the OPM breach, the Department conducted a review to determine the institutional risks posed to the Department. The Department's Core Management Team—the CPCLO and CIO, as co-chairs, are responsible for managing the Department's response to data breaches involving PII—identified and contacted potentially impacted DOJ components to participate in a Department-wide risk assessment and analysis.

Data Integrity Board

The CPCLO is also a member of the Department's Data Integrity Board. The Data Integrity Board oversees and coordinates the implementation of the Computer Matching and Privacy Protection Act of 1988[24] by conducting reviews and approvals of computer matching agreements entered into by Department components, and by providing interpretations and guidance to Department components in the conduct of matching agreements. During this reporting period, the Data Integrity Board considered and approved 4 computer matching agreements.

---

[22] *See e.g.*, OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf; OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept.29, 2003), https://www.whitehouse.gov/omb/memoranda_m03-22.

[23] DOJ Order 0900.00.01, *Incident Response Procedures for Data Breach* (Aug. 6, 2013), http://www.justice.gov/opcl/breach-procedures.pdf.

[24] *See* 5 U.S.C. § 552a(o).

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 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.

National Security Reviews

The CPCLO receives National Security Review (NSR) reports, which include findings and conclusions from audits of different FBI field offices by the National Security Division. The CPCLO reviews these reports to ensure both that FBI field offices are in compliance with laws, policies, and procedures designed to protect privacy and civil liberties, and that the NSRs are conducted appropriately.

Insider Threat Working Group

DOJ Order 0901, signed on February 12, 2014, 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."[25] Pursuant to this mandate, OPCL has been an active member of the DOJ Insider Threat Working Group, advising on privacy and civil liberties issues as part of the development of the DOJ ITPDP. OPCL's advice and assistance regarding insider threat issues has included assisting the FBI in drafting a PIA, and publishing a SORN and an accompanying Notice of Proposed Rulemaking for its insider threat program records. OPCL has also assisted in preparing an Insider Threat Working Group "Watch the Watchers" Guide, which seeks to ensure that the processes and responsibilities for oversight and compliance of DOJ's ITPDP are implemented and that the "Watch the Watchers" controls are sufficient to maintain confidentiality, integrity and availability. Finally, OPCL has worked closely with Justice Insider Management System (JIMS) managers in connection with preparing an IPA.

Privacy and the Department's Risk Management Framework

On November 18, 2014, the Department's CIO issued a memorandum to all Component CIOs requiring them to comply with the National Institute of Standards and Technology Special Publication (SP) 800-53, Revision 4, including the Appendix J, Privacy Control Catalog, in implementing the Department's Risk Management Framework. In that memorandum, the CIO announced that all of the Appendix J privacy controls were included in the Department's Fiscal Year 2015 Core Controls assessment, and Components were informed that they were expected to complete the Fiscal Year 2015 Core Control assessments by September 30, 2015. In an effort to assist components implement and assess the Appendix J privacy controls by the CIO's deadline, OPCL released "DOJ OPCL Assessment of Appendix J Privacy Controls." To further assist Department

[25] DOJ Order 0901, *Insider Threat* (Feb. 12, 2014), https://www.justice.gov/jmd/file/865256/download.

personnel and components comply with the DOJ OPCL Assessment of Appendix J Privacy Controls, OPCL generated documents for the proper selection, implementation, and assessment of the Appendix J privacy controls.

On July 27, 2016, OMB released an update to OMB Circular A-130 titled, *Managing Information as a Strategic Resource*.[26] 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 PII. These responsibilities included a number of requirements for agencies to integrate its privacy programs into its Risk Management Framework, including but not limited to, the selection, implementation, and assessment of the Appendix J privacy controls. OPCL is currently collaborating with the Department's OCIO to ensure that all requirements outlined in OMB Circular A-130 are satisfied.

Social Security Number Reduction Initiatives

During the reporting period, the Department has continued its effort to identify and reduce the collection and use of Social Security Numbers (SSNs) by Department components. In FY2015, for instance, the Department's OCIO expanded its data loss prevention solutions to not only detect sensitive information in transit, but to also automate certain privacy-protective measures. To further safeguard sensitive PII, such as the SSN, the Department implemented automated capabilities to prevent the sending of unencrypted SSNs in either the body of an email or embedded within an attachment. These enhanced features are designed to notify the sender that data must be encrypted and to block non-compliant emails from leaving the Department's network. The CPCLO and OPCL met with Department components to discuss the implementation of these new technical solutions, and have assisted a number of components in altering current business processes to account for these new privacy-protective measures.

In addition, a number of outreach efforts have been taken over the past few years to remind all Department employees of their responsibilities to safeguard PII, including SSNs. In April 2015, a joint memorandum was sent from the Department's CPCLO and CIO to the heads of Department components, requiring them to work with their respective SCOPs and CIOs to assess and, where necessary, update their policies, procedures, and technical solutions for safeguarding PII. Additionally, in August 2015, a joint memorandum was sent from the Department's CPCLO and CIO, reminding all Department employees of the cybersecurity and privacy protections that apply to PII maintained in the Department's systems. Department employees were also reminded of their continuing obligations related to the safeguarding of sensitive PII, including their responsibilities to minimize the use of SSNs, and when using SSNs is absolutely necessary, to redact or mask the data to the extent feasible.

Going forward, 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.

INTER-AGENCY LEADERSHIP

[26] https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

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:

Information Sharing Environment

The CPCLO and OPCL continue to be active members of the Information Sharing Environment (ISE) working groups. For example, the CPCLO serves on the Executive Committee of the Privacy and Civil Liberties (PCL) Sub-Interagency Policy Committees (IPC), along with the Chief Privacy Officer of the Department of Homeland Security and the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (ODNI). The PCL Sub-IPC meets regularly to ensure that federal agencies adopt, implement, and enforce privacy and civil liberties protection policies before sharing terrorism-related information in the ISE. OPCL also supports the PCL Sub-IPC on various sub-working groups.

Nationwide Suspicious Activity Reporting Initiative

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a partnership for sharing terrorism-related SARs among federal, state, local, and tribal agencies. The NSI is a critical part of the federal government's National Strategy for Information Sharing, which articulated a plan to establish a network of state and major urban area fusion centers that could gather and report locally generated information to appropriate federal, state, and local entities, while protecting the privacy and other legal rights of Americans.[27] In this reporting period, the CPCLO worked with the FBI, the Program Manager of the ISE (PM-ISE), and other federal privacy officers to review the adoption of a revised Functional Standard for Suspicious Activity Reports in the ISE.[28] In this context, the CPCLO participated in a roundtable of privacy advocates coordinated by the PM-ISE to discuss the proposed revisions and will continue to work in this area as the revisions are further considered.

International Efforts

The CPCLO and OPCL have been extensively engaged in efforts to facilitate the sharing of information across borders. The activities include participation in the US delegation that negotiated an agreement with the EU; leading interagency efforts regarding the Administration's commitment to seek legislation to extend certain rights under the Privacy Act to non-US citizens; and participation in the law enforcement and national security aspects of the Privacy Shield framework. Additionally, the CPCLO has participated in the International Conference for Data Privacy and Protection Commissioners since 2015.

- *The Data Protection and Privacy Agreement*—The CPCLO served as part of the US delegation that, on December 1, 2016, successfully negotiated over the past five years, an executive agreement between the European Union (EU) and the U.S. relating to privacy protections for personal information transferred between the US, the EU, and the EU Member States for the prevention, detection, investigation or prosecution of criminal offenses. The Agreement, commonly known in the U.S. as the DPPA, establishes a set of protections that the Parties are to apply to personal information exchanged for the purpose of preventing, detecting, investigating, and prosecuting criminal offenses. The DPPA will allow for improved information exchange with Europe and will strengthen U.S. law

[27] *See* National Strategy for Information Sharing, *Successes and Challenges In Improving Terrorism-Related Information Sharing*, 11 (Oct. 2007), http://ise.gov/sites/default/files/nsis_book_0.pdf.
[28] http://ise.gov/sites/default/files/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf.

enforcement partnerships with those countries. Article 19 of the DPPA establishes an obligation for the Parties to provide, in their domestic law, specific judicial redress rights to each other's citizens. This provision addresses a longstanding EU concern that certain judicial redress rights in the U.S. under the Privacy Act were limited to U.S. citizens and lawful permanent residents. The CPCLO and OPCL also worked closely with the interagency team drafting whitepapers for the European Parliament to help the Members of that body better understand the U.S. system of protections for privacy and transparency. On December 1, 2016, these efforts were rewarded when the European Parliament ratified the DPPA.

- *The Judicial Redress Act of 2015*—The CPCLO had a leadership role the inter-agency efforts with regard to the Judicial Redress Act of 2015 to implement the provisions of Article 19 of the DPPA. Article 19 establishes an obligation for the Parties to provide, in their domestic law, specific judicial redress rights to each other's citizens. The Act establishes, with respect to information within the scope of the DPPA that has been transferred by a covered country to the U.S., a basis for affording the citizens of covered countries a number of the same judicial redress rights to the same extent and subject to the same conditions that U.S. citizens and lawful permanent residents enjoy under the Privacy Act. The Act authorized the Department to designate foreign countries or regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act against certain government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records transferred from a foreign country to the U.S. to prevent, investigate, detect, or prosecute criminal offenses.

- *EU-U.S. Privacy Shield Framework*—On July 12, 2016, the European Commission ratified the EU-U.S. Privacy Shield Framework,[29] which provides "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 to the United States in support of transatlantic commerce."[30] The CPCLO and OPCL worked closely with colleagues at ODNI, the Department of Commerce, and other Federal departments and agencies to create the EU-U.S. Privacy Shield Package. Specifically, Annexed to the EU-U.S. Privacy Shield Framework were letters from the Department of Justice,[31] and the Office of the Director of National Intelligence,[32] among other Federal agencies and Departments, detailing the safeguards and limitations on U.S. Government access for U.S. national security, law enforcement, and public interest purposes. Additional information concerning the EU-U.S. Privacy Shield Framework can be found at https://www.privacyshield.gov.

[29] Dept. of Com., EU-U.S. Privacy Shilled Framework Principles, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.
[30] Dept. of Com., Privacy Shield Framework: EU-U.S. Privacy Shield Program Overview, https://www.privacyshield.gov/Program-Overview (last visited Jan. 3, 2017).
[31] *See* Letter to Mr. Justin S. Antonipillai, Couns., Dept. of Com., and Mr. Ted Dean, Deputy Assistant Secretary, Int'l Trade Admin., from Bruce C. Swartz, Dept. of Justice, Deputy Assistant Att'y General and Couns. for Int'l Affairs (Feb. 19, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0W.
[32] *See* Letter to Mr. Justin S. Antonipillai, Couns., Dept. of Com., and Mr. Ted Dean, Deputy Assistant Secretary, Int'l Trade Admin., from Robert S. Litt, General Couns., Off. of the Director of Nat'l Intel. (June 21, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1A; Letter to Mr. Justin S. Antonipillai, Couns., Dept. of Com., and Mr. Ted Dean, Deputy Assistant Secretary, Int'l Trade Admin., from Robert S. Litt, General Couns., Off. of the Director of Nat'l Intel. (Feb. 22, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F.

- *International Conference of Data Privacy and Protection Commissioners*—The International Conference of Data Privacy and Protection Commissioners (ICDPPC) 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 2015, the CPCLO attended the 37 International Conference of Data Privacy and Protection Commissioners (ICDPPC). The Office of Privacy and Civil Liberties was granted Observer Status for the 38th ICDPPC, and in October 2016, 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.

Federal Privacy Council

On February 9, 2016, the President signed an Executive Order establishing the Federal Privacy Council. The Council 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 initiative, educate the Federal workforce, and exchange best practices. The CPCLO is a member of the Executive Committee of the Council, and serves as Co-Chair of the Technology and Innovation Committee, which is composed of the Digital Privacy Sub-committee, and the Electronic Authentication Taskforce. The OPCL Director has also worked on several projects for the Council, including teaching an introduction to privacy law to a wide group of agency privacy officials at a Privacy "Bootcamp," and creating content for a government-wide website to help the public better understand the wide array of U.S. privacy protections.

Open Government Initiatives

The CPCLO and OPCL continue to support the goals of public participation 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.

Unmanned Aircraft Systems Working Group Policy

OPCL participates in an interagency working group on government-wide privacy issues related to federal use of UAS, the planned opening of the National Airspace System to private and commercial UAS, and the use of federal funds by state, local, tribal, and territorial governments to acquire UAS. OPCL offers unique perspectives, and is working to achieve the highest level of transparency in its work on UAS. In February 2015, the president issued an Executive Order on the federal domestic use of UAS.[33] On May 22, 2015, Department issued a policy governing the use of UAS.[34] The CPCLO and OPCL are working to publish additional

[33] Memorandum from President Barack Obama to Heads of Executive Departments and Agencies, *Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (Feb. 15, 2015), https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[34] Memorandum from the Dep't of Justice, Office of Deputy Attorney General to Heads of Law Enforcement Components, *Domestic Use of Unmanned Aircraft Systems (UAS)* (May 22, 2015) [hereinafter DOJ UAS Policy], https://www.justice.gov/file/441266/download.

documentation that addresses the concerns of transparency and accountability in the Department's domestic use and operation of UAS, and is designed to help ensure that Department personnel continue to respect individuals' privacy, civil rights, and civil liberties.

Privacy Overlay with Committee on National Security Systems

The Privacy Overlay applies security and privacy controls beyond those required by any individual baseline prescribed in Committee on National Security Systems (CNSSI) No. 1253. It is a repeatable risk management process that provides agencies a consistent approach for selecting privacy and security controls for information systems containing PII, including protected health information (PHI), in National Security Systems. OPCL provided some suggestions during the Overlay's development, and gave a brief overview to SCOPs on its application in February 2015.

Cybersecurity Information Sharing Act of 2015, 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.[35] As part of the process, the CPCLO and OPCL also participated in interagency and external outreach to obtain stakeholder input.

Department of Defense Attorney General Guidelines

The CPCLO played a significant role in working with the Department of Defense (DoD) and ODNI in completing an update of procedures that govern the conduct of DoD intelligence activities as they pertain to collection, retention, and dissemination of US person information. These procedures, first issued in 1982, are published in DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities." They are required by Executive Order 12333, which authorizes elements of the IC 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. The new DoD Manual 5240.01 was signed by the Attorney General and Secretary of Defense, and was effective as of August 8, 2016.

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 UAS; and meetings with members of the PCLOB to discuss

[35] Dep't of Justice & Dep't of Homeland Security, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (June 15, 2016), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_(Sec%20105(b)).pdf.

Department programs and operations and how privacy and civil liberties issues are considered in the counterterrorism context.

PRIVACY AND CIVIL LIBERTIES COMPLAINTS

OPCL receives numerous inquiries from members of the public through 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 an estimated 1,292 inquiries from members of the public; however, none of these met the threshold for a privacy and/or civil liberties complaint against the Department.

In addition, OPCL received 11 privacy and civil liberties violations in connection with the Department's handling of information.[36] 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.

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 28 Privacy Act amendment appeals.

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 www.justice.gov/opcl/reports.htm. These reports are described in more detail below:

Federal Information Security Modernization Act of 2014

[36] The inquiries described above did not qualify as privacy and/or civil liberties complaints because the matters raised in those inquiries either fell outside the purview of the Office (e.g., the complaints were against private entities or other non-DOJ entities) or did not raise issues concerning privacy and/or civil liberties matters.

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.[37] 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 & 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.

Data Mining Report

The Data Mining Report describes the Department's activities that qualify as data mining under the Federal Agency Data Mining Reporting Act of 2007[38] and the privacy and civil liberties protections built into such activities. During this reporting period, OPCL worked with other Department components to streamline the reporting process, and to identify and review privacy and civil liberties procedures in place in such qualifying data mining activities.

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."[39] Each fiscal year, OPCL has worked 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,

---

[37] *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).
[38] 42 U.S.C. § 2000ee-3.
[39] 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.

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. The Department is currently evaluating the privacy policies for mobile applications developed by or on behalf of the Department.

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. The Department is currently evaluating a process to regularly review privacy policies for mobile applications developed by or on behalf of the Department.

FUTURE INITIATIVES

The CPCLO and OPCL are committed to building and sustaining a strong foundation of privacy at the Department and will continue to build upon the initiatives discussed in this report. To that end, the CPCLO and OPCL will continue the work of strengthening the Department's components' roles and responsibilities in order to build a successful and accountable privacy program in every component of the Department. The Department will continue to explore innovative and efficient ways to incorporate privacy in the Department's complex and diverse mission work, and looks forward to discussing these new initiatives in the next annual report.

OPCL ORGANIZATIONAL RESTRUCTURING

In the aftermath of a series of high-profile data breaches, and the Department's growing dependence on information technology, the demand for privacy capabilities is at its zenith. To meet the demands of the Department, the CPCLO, and the SCOPs, OPCL is in the process of reorganizing into two divisions focusing on OPCL's primary responsibilities—a Law and Policy Division, and a Compliance Division.

Each division will be headed by an Assistant Director. The Compliance Division will be staffed by both privacy analysts and attorneys. The Compliance Division will be responsible for: reviewing IPAs, PIAs, and SORNs; responding to privacy and civil liberties complaints; overseeing OPCL's breach response, policy implementation, and advice responsibilities; meeting all privacy-related reporting obligations, such as under the FISMA and the Federal Agency Data Mining Reporting Act of 2007; and providing advice and implementation regarding OMB requirements mandated through OMB Circulars and Memoranda. Each of these responsibilities may, at times, necessitate work from the Law and Policy Division.

The OPCL Law and Policy Division will be staffed by privacy and civil liberties attorneys. The Law and Policy Division is responsible for: overseeing the Office's legislative coordination and clearance process and responding to requests for review from both the Office of Legislative Affairs and Office of Legal Policy; overseeing the Office's directives management review and advice process; participating in working groups, such as those regarding the Attorney General Guidelines, insider threat issues, UAS, social media, and open government; adjudicating Privacy Act amendment appeals; updating and publishing *The Overview of the Privacy Act of 1974*; and providing legal advice and guidance to the CPCLO on specific policy initiatives.

OPCL anticipates that its reorganization will assist in meeting the oversight, reporting, and guidance demands that are expected to grow in upcoming years. This reorganization is also consistent with the Department's requirement to ensure that adequate resources and staff are devoted to meeting the Department's privacy-related functions and obligations.[40]

[40] *See* 42 U.S.C. § 2000ee–1(d)(1); *see also* Violence Against Women Act and Department of Justice Reauthorization Act of 2005 § 1174(b)(4), 28 U.S.C. § 509 note (2012).