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, 2020 – SEPTEMBER 30, 2024

(MULTI-YEAR) ANNUAL PRIVACY REPORT

MESSAGE FROM THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER

As the Acting Chief Privacy and Civil Liberties Officer (CPCLO) of the Department of Justice (Department or DOJ), I am pleased to present the Department's Annual Privacy Report, describing the operations and activities of 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, 2020, through September 30, 2024.

The Department's privacy program is supported by a team of dedicated privacy professionals who work to maintain the trust of the pubic in carrying out the mission of the Department, particularly in connection with national security and law enforcement. The Department's privacy team includes the staff of OPCL as well as the Senior Component Officials for Privacy and their teams within each of the Department's forty-two components.

During this reporting period, the landscape of technological development and advancement in areas such as artificial intelligence, biometrics, and international data flows evolved rapidly. The Department's components also experienced an increase in the complexity of new systems and processes, and in the number of cyber security events threatening the privacy of individuals as well as the mission of the Department.

As the Department carries out its mission of protecting public safety and national security, and upholding the administration of justice, the Department's privacy team is committed to continuing the development of innovative, practical, and efficient ways to protect privacy and maintain public trust.

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 OFFICE . . .** (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.[2]

I. PRIVACY AND CIVIL LIBERTIES PROGRAM GOVERNANCE

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 domestic and international 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. With the CPCLO role in advising the Attorney General and others in Department leadership, OPCL's role coordinating policy and compliance across the Department's forty-two components, and the role of the Senior Component Officials for Privacy (SCOPs) in each component addressing day-to-day privacy and civil liberties policy and compliance issues, the Department's privacy program has the breadth and depth needed to effectively and efficiently govern privacy and civil liberties matters to protect the public trust.

Moreover, the privacy program's governance framework includes administrative, technical, and physical controls that build privacy safeguards into each step of the Department's consideration, assessment, and development of new technologies and data collections, from procurement through design, to the software development lifecycle and the authorization to operate. The framework is well-established throughout the Department and uniquely suited to address threshold questions and risk assessment of emerging technologies and data uses, including artificial intelligence and biometrics.

This report covers the period from October 1, 2020, to September 30, 2024, and discusses the continued efforts of the CPCLO and OPCL to safeguard individual privacy and civil liberties while advancing the Department's overall mission.

[1] 28 U.S.C. § 509 (note) (2018).
[2] *Id*.

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 and is 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.[3] Legislation enacted the following year expanded the CPCLO's responsibilities, and in 2008, the Department established the Office of Privacy and Civil Liberties (OPCL) to support the CPCLO's duties.

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),[4] and on all issues of privacy and civil liberties when implementing or developing laws, regulations, policies, procedures, or guidelines related to the Government's counterterrorism efforts.[5] 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[6] ("Privacy Act"), and Section 208 of the E-Government Act of 2002.[7]

1. Department CPCLO (A), Peter Winn, speaks at the Privacy Summit held at DOJ headquarters, June 2024.

Moreover, the CPCLO serves as the Senior Agency Official for Privacy (SAOP) for the Department. The role and responsibilities of an SAOP are outlined in Office of Management and Budget (OMB) policies applicable to Executive Branch agencies. OMB's overarching objectives are to maximize the quality and security of U.S. government information systems, while ensuring that agencies manage information systems in a way that addresses and mitigates security and privacy risks, addressed in OMB Circular No. A-130, *Managing Information as a Strategic Resource*.[8] OMB first established the requirement that agencies designate a SAOP in 2005, and expanded on those requirements in

[3] *See id*.; *see also* Implementing Recommendations of the 9/11 Commission Act of 2007 § 803, 42 U.S.C. § 2000ee-1 (2018).
[4] 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." *See* DOJ Order 0601, *Privacy and Civil Liberties* (May 14, 2020).
[5] *See* 28 U.S.C. § 509 note; *see also* 42 U.S.C. § 2000ee-1 (2018).
[6] 5 U.S.C. § 552a (2018).
[7] 44 U.S.C. § 3501 (2018).
[8] Off. of Mgmt. & Budget, Exec. Office of the President, OMB Circular No. A-130, Managing Information as a Strategic Resource (1996).

2016, pursuant to the requirements of Executive Order 13719, Establishment of the Federal Privacy Council, and OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 15, 2016). Taken together, these authorities require the SAOP for each agency to be responsible for all privacy issues in their agencies.[9]

During the reporting period, the CPCLO's work in international data protection and privacy has been increasingly important, particularly in representing the Department in international negotiations designed to harmonize high standards in privacy related laws, policies, and practices related to the Department's mission. This includes international engagement with organizations such as the United Nations (UN), the Organization for Economic Cooperation and Development (OECD), the Council of Europe, EU-U.S. Trade and Technology Council, UK-U.S. Data and Technology, Global Privacy Assembly (GPA), G7 Data Protection Authority Roundtable, and Freedom Online Coalition. The CPCLO also has a key role in implementing the Judicial Redress Act, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), and other key international agreements and arrangements, such as the Data Protection and Privacy Agreement, also known as the "Umbrella Agreement," and the EU-U.S. Data Privacy Framework, as discussed further below.

2. CPCLO, Peter Winn, speaks at 45th Global Privacy Assembly, Bermuda, 2023.

Peter Winn has been the Department's CPCLO (Acting) since 2017 and is an experienced attorney in the career Senior Executive Service, with demonstrated expertise in privacy law, policy, and compliance.[10]

2. THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

The Office of Privacy and Civil Liberties (OPCL) was established 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.

[9] Most courts in the United States give OMB guidelines and regulations, such as Circular A-130, the same deference they give interpretations of an agency that has been charged with the administration of a statute. *See Sussman v. Marshals Serv.*, 494 F.3d 1106, 1120 (D.C. Cir. 2007) ("Congress explicitly tasked the OMB with promulgating guidelines for implementing the Privacy Act, and we therefore give the OMB Guidelines 'the deference usually accorded interpretation of a statute by the agency charged with its administration.'").
[10] U.S. Dep't. of Just., *Staff Profile, Peter A. Winn* (2024), https://www.justice.gov/opcl/CPCLO.

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.[11] Additionally, OPCL is comprised of a team of experienced attorneys and analysts, with each OPCL attorney and analyst responsible for a defined set of Department components, and specializing in certain subject areas of federal privacy and civil liberties law.

OPCL supports the CPCLO by providing advice on new domestic or international 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 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 its programs and information systems.

OPCL accomplishes its mission by:

- Reviewing legislative, regulatory and policy proposals pertaining to privacy and civil liberties issues arising from the Department's operations;
- Serving on interagency and intra-agency committees and working groups and developing policies, guidelines, and procedures to support the Department's mission, including for law enforcement and national security operations;
- Advising the Department in connection with information sharing agreements and arrangements with state, local, tribal, and territorial authorities, as well as with foreign governments;
- Advising Department leadership and components concerning international data protection and privacy laws and policies, participating in international organizations charged with addressing data protection and privacy issues, and representing the Department in international negotiations designed to harmonize high standards in privacy laws, policies, and practices;
- Developing and providing guidance to Department components to help ensure they comply with federal privacy laws, regulations, and policies;
- Reviewing the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties and appropriately minimize risks;
- Overseeing the Department's response to data breaches in coordination with the Justice Management Division Office of the Chief Information Officer (JMD OCIO), consistent with applicable laws and policies;
- Reviewing and facilitating finalization of 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;

[11] U.S. Dep't. of Just., *Staff Profile, Katherine Harman-Stokes* (2024), https://www.justice.gov/opcl/staff-profile/acting-director-office-privacy-and-civil-liberties.

- Assisting the CPCLO in adjudicating appeals of DOJ component denials of requests 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 redressing and 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, and Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005.

In addition, OPCL provides administrative support to the Data Protection Review Court (DPRC), the second layer of a two-layer independent and binding redress process, a critical pillar in the EU-U.S. Data Privacy Framework established in 2023, as discussed further below.[12]

3. SENIOR COMPONENT OFFICIALS FOR PRIVACY

OPCL supports the CPCLO with overseeing each Department component's compliance with privacy laws, regulations, and policies. Pursuant to DOJ Order 0601, "Privacy and Civil Liberties" (May 14, 2020), each component designates a SCOP, who is accountable and responsible for the component's privacy program. The SCOPs, in turn, coordinate their components' privacy issues and concerns with OPCL, the CPCLO, and Department leadership. The Department's SCOPs have varied resources. Some components, such as the Federal Bureau of Investigation (FBI), have privacy and civil liberties units with multiple experienced attorneys dedicated only to privacy and civil liberties issues; 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. In addition, OPCL provides annual role-based training programs focused on the responsibilities of the SCOPs and has developed resources that detail the SCOPs responsibilities, actions, and action deadlines in response to a privacy data breach.

II. 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 accomplishes these missions, the Department must fulfill its interrelated responsibility to manage and protect the PII it collects about individuals. On July 28, 2016, OMB

[12] U.S. Dep't. of Just., *Data Protection Review Court* (2024), https://www.justice.gov/opcl/redress-data-protection-review-court.

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 several 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. Agency privacy programs now have explicit responsibilities in the assessment and authorization process for information systems.

During this reporting period, OPCL and OCIO completed implementation and updated the Department's Security and Privacy Assessment and Authorization Handbook (SPAA Handbook) to version 10. [13] The SPAA Handbook assists the Department with meeting the requirements of OMB Circular A-130, and adopts the National Institute of Standards and Technology's Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* and NIST 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.[14] The Handbook embeds privacy assessments and controls into the system design and development lifecycle. It outlines the process, documentation requirements, and automated tools essential to performing the successful security and privacy assessment and authorization of all DOJ information systems. The SPAA Handbook serves as the foundation for assessing privacy controls and authorizing the operation of DOJ information systems. OPCL also worked closely with Department procurement and contracting specialists to incorporate an analysis of privacy-related requirements into the procurement process, and to mandate that certain procurement and contract documents incorporate specific privacy-protective terms and conditions.

The governance framework overall requires component information technology, mission, and privacy experts to draft an initial privacy assessment, which describes the project and asks key threshold questions to determine necessary compliance requirements and controls. OPCL works with the SCOP and approves the next steps, then the component team works on a comprehensive privacy impact assessment, Privacy Act compliance documents, privacy controls outlined in the SPAA Handbook and NIST standards, and takes other next steps, when required, to ensure legal compliance and appropriately minimize privacy risks. Once these steps have been completed and OPCL or the SCOP concurs with OCIO that risks have been properly mitigated, the SCOP and component authorizing official may authorize the system to operate. 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 privacy-related processes. The Department established the Initial Privacy Assessment (IPA) template, which consolidates questions regarding various threshold privacy-related compliance requirements into a single, unified, and comprehensive process. The IPA template consists of questions designed to

[13] Off. of Mgmt. & Budget, Exec. Office of the President, OMB Circular No. A-130, Managing Information as a Strategic Resource (1996).

help components and OPCL determine whether a particular information system requires further privacy assessment and/or documentation (e.g., completion of a Privacy Impact Assessment (PIA), or 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.

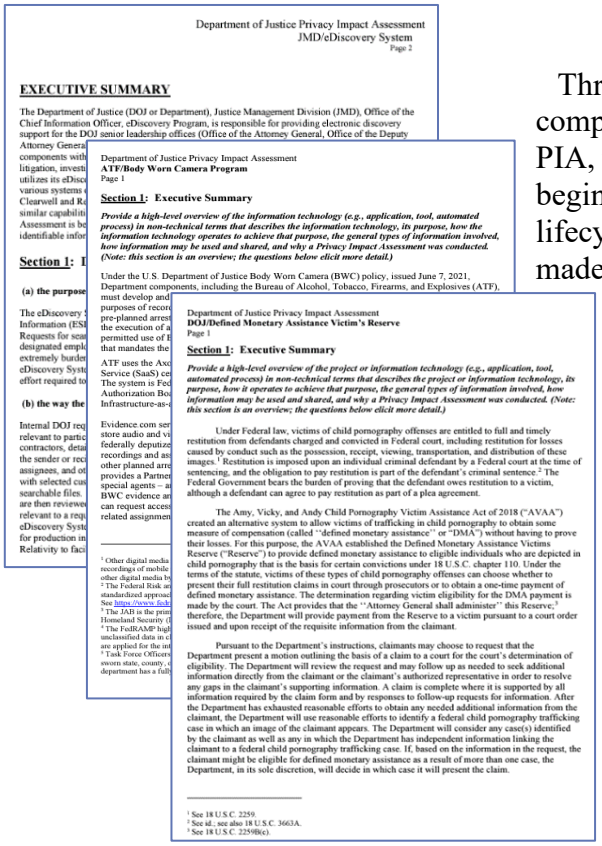
The Department has incorporated the IPA process into the Department's risk management framework outlined in the SPAA Handbook, including in the IT information system Authorization to Operate (ATO) security authorization process, and utilizes a software application managed by OCIO to track components' compliance with applicable federal and Department privacy and security requirements for IT systems. 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 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. The IPA process is well-established throughout the Department, and the IPA template is updated regularly to address new compliance or other requirements. For example, OPCL appended its IPA template with a privacy assessment for information collection requests in accordance with Paperwork Reduction Act requirements. Also, because of OPCL's leadership on the Department's Emerging Technology Board, the Department will leverage the IPA process for emerging technologies. OPCL began updating the IPA template to ask threshold questions that will identify uses of AI or machine-learning requiring further assessment.

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.[15] 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.[16]

[15] *See* E-Gov't. Act of 2002, Pub. L No. 107-347, §208 (b)(1)(A)(ii).
[16] *See* Off. of Mgmt. & Budget, Exec. Office of the President, 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.


Department of Justice Privacy Impact Assessment
JMD/eDiscovery System
Page 2

EXECUTIVE SUMMARY

Department of Justice Privacy Impact Assessment
ATF/Body Worn Camera Program
Page 1

Section 1: Executive Summary

Department of Justice Privacy Impact Assessment
DOJ/Defined Monetary Assistance Victim's Reserve
Page 1

Section 1: Executive Summary

Through the IPA process, OPCL determines if 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 appropriate 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 authorized to operate. A system may not be authorized to operate without the CPCLO, OPCL Director, or the SCOP's concurrence.

The Department also maintains an alternative PIA template for components, known as the "Admin PIA" template, designed for administrative systems as opposed to law enforcement systems or systems supporting other mission functions. PIAs appropriate for publication can be found on OPCL's website.[17]

3. SOCIAL SECURITY NUMBER FRAUD REDUCTION ACT

OPCL worked with components to ensure compliance with the Social Security Number Fraud Reduction Act of 2017 (SSN Act). The SSN Act requires agencies to 1) submit to Congress an initial report detailing documents physically mailed by the agency during the previous year that contain a full SSN, with annual updates for 5 years; 2) 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; and 3) issue regulations implementing the agency's plan by 2022.[18]

OPCL has amended 28 CFR part 16, subpart D to include instructions that define the term "necessary" to include only those circumstances in which a component would be unable to comply, in whole or in part, with a legal, regulatory, or policy requirement if prohibited from mailing the full SSN. The regulations also include instructions for the partial redaction of SSNs where feasible; and require that SSNs not be visible on the outside of any package sent by mail. Unless

[17] U.S. Dep't. of Just., *DOJ Privacy Impact Assessments* (2024), https://www.justice.gov/opcl/doj-privacy-impact-assessments.
[18] SSN Act, 42 U.S.C. § 405 note.

the Attorney General directs otherwise, the CPCLO is authorized to assist components in interpreting these requirements. In addition, OPCL has satisfied its reporting requirements to Congress under the Act.

OPCL enhanced its training initiatives to help ensure that component officials are fully aware of the requirements and 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.

4. SYSTEM OF RECORDS NOTICES

Under the Privacy Act, agencies must assess their handling of certain information about individuals and ensure the collection, maintenance, use, disclosure, and safeguarding of such information is appropriate and lawful.[19] 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 is comprised of the Federal Register notice(s) that identifies the system of records, the purpose(s) of the system, the legal authority for maintenance of the records, the categories of records maintained in the system, the retention and disposal of records, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, how individuals may request access and amendment of records, and additional details about the system.[20] The Department of Justice maintains many systems of records. The SORNs for these systems can be found on OPCL's website.[21]

Through the IPA process, OPCL advises the Department's components on the proper maintenance of information in systems of records to ensure compliance with the numerous Privacy Act requirements that govern such information. For example, once OPCL determines, via an IPA, 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.[22] As part of this work, OPCL assists components in reviewing routine uses included in SORNs to ensure that each routine use contemplated is compatible with the purpose for which the information was collected.

During this reporting period, OPCL provided to components guidance on and review of SORNs and exemption regulations. In addition to facilitating publication of SORNs and regulations, OPCL advises components on preparing other Privacy Act documents, such as Privacy

[19] *See* 5 U.S.C. § 552a.
[20] *See id.* § 552a(e)(4); Off. of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* (2016).
[21] U.S. Dep't. of Just., *DOJ Systems of Records* (2024), https://www.justice.gov/opcl/doj-systems-records (Stating there may be several subsystems of records that are covered by the same SORN).
[22] The Attorney General delegated the authority to carry out these responsibilities to the CPCLO by order in January 2008.

Act consent forms and Privacy Act notice statements, which provide actual notice to an individual about an agency's collection authority and the possible uses of their information.[23]

5. JUDICIAL REDRESS ACT IMPLEMENTATION

Over the reporting period, OPCL assisted 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.[24]

6. PRIVACY ACT AMENDMENT REQUEST APPEALS

Under the Privacy Act, individuals have certain rights to access records about themselves and amend records, correcting records that are not accurate, relevant, timely, or complete, with certain exemptions for law enforcement and national security systems.[25] Individuals may request access and amendment through Department components. The components decide whether access or amendment are appropriate under the law and the facts. The OPCL Director (pursuant to delegation by CPCLO) adjudicates all appeals of denials by Department components of requests to amend records. 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 request appeals.

7. PRIVACY AND CIVIL LIBERTIES INQUIRIES AND COMPLAINTS

OPCL receives numerous inquiries and complaints from members of the public by mail, email, and phone, and has an established process to review such inquiries or complaints in a timely manner. Such inquiries and complaints may concern questions about the Department's handling of PII or requests to correct inaccurate PII consistent with the objective of maintaining data quality, as well as other issues involving the proper handling of PII, including when PII, such as biometric information, is collected through technological means. For inquiries, OPCL acts as an ombudsman, referring such inquiries to the appropriate Department component, to ensure that inquiries are properly reviewed, and responses are properly provided and/or appropriately referred. If an individual is not satisfied with the response received from the component, OPCL can provide additional review. For this reporting period, OPCL received numerous inquiries from members of the public. "Inquiries" are different from "complaints," however.

During the reporting period, OPCL received zero complaints, either privacy or civil liberties related, during FY21 and FY22. In this context, a *privacy complaint* encompasses a written allegation (excluding complaints filed in litigation against the Department) concerning a violation of privacy protections in the administration of the programs and operations of the Department that is submitted to or through the CPCLO and/or OPCL. A *civil liberties complaint* encompasses a written allegation (excluding complaints filed in litigation against the Department)

[23] *See* 5 U.S.C. § 552a(b); *see id.* § 552a(e)(3).
[24] *See* U.S. Dep't of Just., *Judicial Redress Act of 2015 & U.S.-EU Data Protection and Privacy Agreement* (2022), https://www.justice.gov/opcl/judicial-redress-act-2015.
[25] *See* 5 U.S.C. § 552a(d); *see also* U.S. Dep't of Just., *Privacy Act Requests* (2022), https://www.justice.gov/opcl/doj-privacy-act-requests.

of a problem with or violation of civil liberties safeguards concerning the handling of personal information by the Department in the administration of Department programs and operations that is submitted to or through the CPCLO and/or OPCL.

8. COMPUTER MATCHING AGREEMENTS AND THE DOJ DATA INTEGRITY BOARD

Throughout the reporting period, OPCL and the CPCLO ensured that the Department complied with the Computer Matching and Privacy Protection Act of 1988, as amended.[26] These activities included coordinating the review of all Computer Matching Agreements that were either established, re-established, or renewed with JMD. The CPCLO serves on the DOJ Data Integrity Board and is one of the stakeholders responsible for reviewing and approving Computer Matching Agreements entered on behalf of the Department. OPCL assisted JMD in preparing the Annual Computer Matching Activity Reports, in compliance with OMB Circular A-108.[27] [28] These activities included coordinating the review of all Computer Matching Agreements that were either established, re-established, or renewed with JMD. The CPCLO serves on the DOJ Data Integrity Board and is one of the stakeholders responsible for reviewing and approving Computer Matching Agreements entered on behalf of the Department. OPCL assisted JMD in preparing the Annual Computer Matching Activity Reports, in compliance with OMB Circular A-108.[29]

9. INFORMATION COLLECTION REQUEST PRIVACY ASSESSMENTS

In 2018, 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 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.

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 notice under 5 U.S.C. §552a(e)(3). To assist DOJ components in answering these questions, OPCL developed an assessment tool, called an "Information Collection Request – Privacy Assessment" (ICR-PA). The ICR-PA helps components decide whether an information collection instrument submitted to OMB

[28] Pub. L. No. 100-503, 102 Stat. 2507 (1988), (codified at 5 U.S.C. § 552a).
[29] DOJ Annual Computer Matching Activity Reports can be found at: https://www.justice.gov/opcl/computer-matching-agreements-and-notices; *see supra* note 20 (re A-108).

OIRA as part of an ICR must include Privacy Act-required notices to the individual about whom information is being solicited.

10. BUDGET, ACQUISITION, CONTRACTORS, AND THIRD PARTIES

Designing a new technology to minimize privacy risks often starts with a procurement or other agreement or contract with a third party. OMB Circular A-130 directs agencies to impose conditions in written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding, that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII.[30] In 2019, OPCL began working with the Department's OCIO Policy and Planning Staff to integrate privacy into the Department's existing IT investment review process. Beginning in early 2020, OPCL began participating in meetings of the IT Acquisition Review Board, which is tasked with reviewing acquisitions between $500K-$5M, and the Department Investment Review Council, which reviews acquisitions over $5M and provides monitoring, oversight, and facilitation of major IT program investments. OPCL's goal is to help flag proposed acquisitions which trigger privacy concerns and resolve any identified or suspected privacy risk.

In September 2021, OPCL finalized the Department's Contractor Privacy Requirements Clause, DOJ-02, which was published under Acquisition Procurement Notice (APN) 21-07. Contracting Officers are required to include the clause in all new contracts, orders, Blanket Purchase Agreements, Basic Ordering Agreements, or other procurement vehicles involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII, whether that PII relates to Federal employees or contractors, or members of the public. DOJ-02 satisfies the agency's requirements for ensuring that terms and conditions in written agreements involving Federal Government information incorporate security and privacy requirements, including OMB Circular A-130, and enables agencies to meet federal and agency-specific requirements pertaining to the protection of Federal information. The clause is available in the Department's Unified Financial Management System and automatically populates in the procurement vehicle templates unless the Contracting Officer attests that the procurement does not involve PII.

DOJ-02 was last updated by APN 21-07A in January 2022. Since the publication of DOJ-02, OPCL has provided numerous trainings across the Department and the Federal Government on the implementation of the Contractor Privacy Requirements clause and third-party risk management in federal contracting. In addition, OPCL performs quarterly audits of Department component procurement vehicles to ensure the clause is being appropriately applied to engagements involving PII.

[30] *See* OMB Circular A-130, Appendix I § 3(d).

11. INCREASING TRANSPARENCY OF PRIVACY POLICIES

OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services* 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.[31] These and related efforts in updating OPCL's central resource page dedicated to the Department's privacy program, increase transparency and better educate the public on the work of the CPCLO and OPCL. [32] Specifically, during the reporting period, OPCL:

- Updated the list and provided links to all Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f);[33]
- Regularly updated OPCL's public homepage[34] and "Frequently Asked Questions" page.[35]

12. DATA BREACHES

During the reporting period, OPCL continued to perform its responsibilities for reviewing and coordinating responses to data breaches of PII in accordance with DOJ Instruction 0900.00.01, *Reporting and Response Procedures for a Breach of Personally Identifiable Information* and the successor DOJ Policy Statement 0904.02, *Incident and Breach Response Playbook*. [36]

In performing these responsibilities, OPCL coordinated closely with OCIO and SCOPs to ensure breaches were reported rapidly, and that components completed their response activities

[31] Off. of Mgmt. & Budget, Exec. Off. of the President, OMB M-17-06*, Polices for Federal Agency Public Websites and Digital Services* (Nov. 8, 2016).
[32] *See* U.S. Dep't of Just., *Privacy* (2024), https://www.justice.gov/privacy.
[33] *See* U.S. Dep't of Just., *DOJ Privacy Act Regulation* (2022), https://www.justice.gov/opcl/doj-privacy-act-regulations.
[34] U.S. Dep't of Just., *Office of Privacy of Civil Liberties* (2024), https://www.justice.gov/opcl.
[35] U.S. Dep't of Just., *Frequently Asked Questions* (2024), https://www.justice.gov/opcl/faq.
[36] U.S. Dep't of Just., *Reporting and Response Procedures for A Responsibilities for Managing Breach of Personally Identifiable Information* (Feb. 16, 2018), https://www.justice.gov/opcl/file/1036466/dl?inline=.

and complied with requirements under OMB Memorandum M-17-12, successor memoranda, and other applicable laws, policies and regulations.

a. Policy Statement 0900.00.01 to 0904.02

On November 17, 2023, the Department issued DOJ Policy Statement 0904.02, which updated Instruction 0900.00.01 based on new standards, as well as Department experience in responding to breaches— "lessons learned" and best practices. The Policy Statement establishes DOJ's notification procedures and policies for responding to suspected or confirmed incidents or breaches. OPCL lead the drafting, coordination, and implementation of the Policy Statement.

The policy statement establishes the Department's notification procedures and policy for responding to suspected or confirmed incidents and breaches including those involving National Security Information (NSI) and other DOJ information. It also identifies the DOJ Core Management Team (CMT), co-chaired by the CPCLO and CIO, as the primary advisor to the Attorney General and Deputy Attorney General for making determinations regarding planning, response, oversight, and notice to the public for incidents and breaches.

b. Reported Breaches

During the reporting period, the Department experienced three breaches that rose to the level of a "Major Incident," as defined under applicable law, policies, and standards.

- An intrusion into the Department's Microsoft O365 email environment was discovered on December 24, 2020.
- A U.S. Marshals Service system containing law enforcement sensitive information was attacked by a threat actor using ransomware on February17, 2023.
- A company that provided case data analysis support to several United States Attorney's Offices reported to the Department on June 2, 2023, that it was attacked by a threat actor using ransomware.

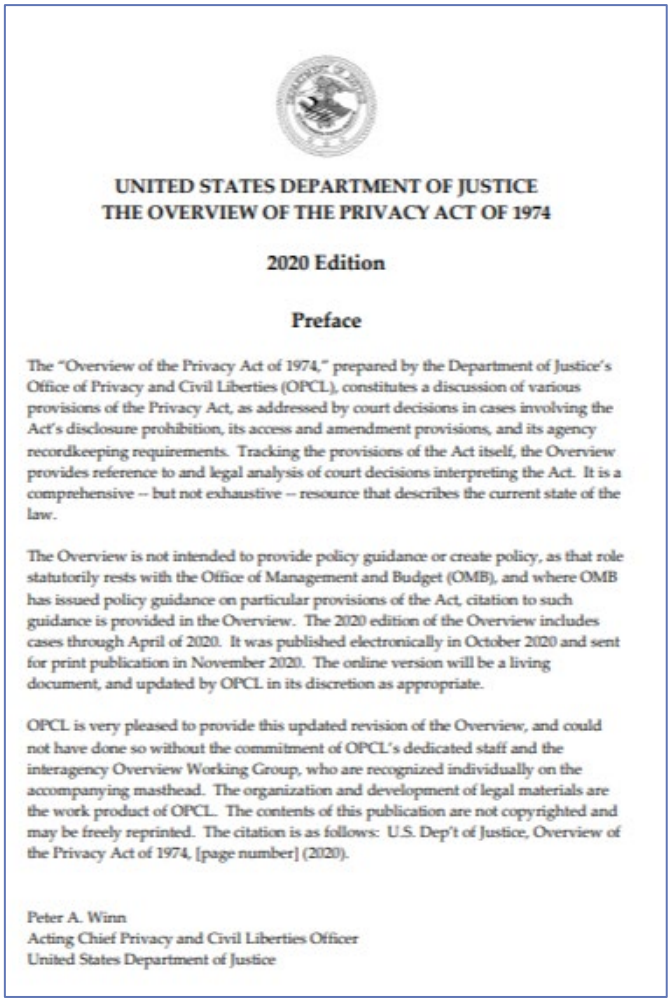
Each of these breaches was treated as a Major Incident and resulted in notification to Congress. The CPCLO and OPCL were involved in coordination and execution of the response and remediation activities for each.

c. Breach Response Program Development

OPCL executed a number of actions to ensure compliance with the Department's obligations under 0904.02, including the creation of a central register to track feedback, proposed changes, and draft versions; a new internal webpage to assist DOJ stakeholders in understanding 0904.02 and its new requirements; a streamlined Initial Risk of Harm Assessment template to ready it for possible automation, publishing a role-based actions and deadlines matrix for participants in the breach response process, and documenting needed changes to the incident response ticketing software.

III. LEGAL GUIDANCE AND TRAINING

OPCL provides legal advice and guidance to Department leadership and components on federal privacy compliance requirements, policies, and initiatives. In this capacity, OPCL advises components about the applicability and requirements of federal 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

1. PRIVACY ACT OVERVIEW

In October 2020, OPCL published an updated *Overview of the Privacy Act of 1974* (*Overview*).[37] 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 a valued resource and is widely used throughout the Federal Government for guidance in this field.

2. OPCL TRAINING

OPCL conducts a comprehensive and meticulous training program to ensure that personnel are well-trained to spot privacy 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 Policy Instruction 0904.02 (Incident and Breach Response Playbook) and issue-specific training as requested by SCOPs.

[37] *See* U.S. Dep't. of Just., *Overview of the Privacy Act of 1974 (2020 Edition)* (2020), https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition.

3. OPCL Senior Counsel, Michelle Ramsden, provides real-time role-based training through the DOJ media center.

During the reporting period, OPCL completed the development of role-based training modules for Department employees engaged in law enforcement or litigation functions, among other critical functions, and began required compliance checks for training. The CPCLO and OPCL continued participating in several training-related initiatives within the Department, hosting LearnDOJ training, hosting semi-annual virtual or in-person training events for DOJ personnel and Federal Government privacy practitioners, and, where feasible, publishing videos of those events more broadly.[38]

The CPCLO and OPCL also continued updates to several training modules about the use of encryption technology and other cybersecurity topics in partnership with OCIO. Those training modules are available on the DOJ Intranet and on LearnDOJ. Finally, the CPCLO and OPCL assisted the Federal Privacy Council in developing government-wide privacy training for privacy-adjacent personnel, including contracting and IT professionals, which will serve as the backbone of a future DOJ "Privacy Bootcamp." The CPCLO and OPCL also supported DOJ-wide training initiatives by participating actively in the DOJ Mentoring Program, developing learning assignments for and hosting participants in the Department's LEAP program, and joining in the U.S. Department of Justice Annual Cybersecurity Symposium. As examples, an OPCL attorney spoke on "Data Privacy and Security" in DOJ's weekly internal training sessions for Cybersecurity Awareness Month. In May 2024, the CPCLO and OPCL Senior Counsel spoke on "Federal Privacy Foundations: Transparency, Trust, and Protection" and privacy in AI systems at the U.S. Department's 15th Annual Cybersecurity Symposium.

[38] Learn DOJ is an internal to DOJ online training portal for DOJ employees.

4. OPCL Senior Counsel, Christina Baptista, and Privacy Analyst, Christopher Hicks, provide training at the Privacy Summit held in DOJ headquarters, June 2024.

OPCL also provides training on privacy-adjacent topics to Department components, other federal agencies, international partners, and related organizations at their request, in addition to providing presentations as discussed below.

From 2021-2024, 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 National Institute of Standards and Technology (NIST) Special Publications, and privacy considerations in unique circumstances, such as coordinating with victims and witnesses of crime.

The CPCLO and OPCL personnel also regularly provide training or other presentations in U.S. and international forums.[39]

3. TRAINING RECEIVED BY OPCL

To provide effective guidance to the privacy audience, it is imperative that the CPCLO and OPCL staff remain informed of current privacy issues, particularly new U.S. and international laws, regulations, policies, and standards. During the reporting period, the CPCLO and OPCL staff attended virtual or in-person iterations of: the Federal Privacy Council (FPC) Boot Camp and the Annual Summits; International Association for Privacy Professionals (IAPP) training, including IAPP's Global Privacy Summit, Privacy, Security and Risk Conference, and Europe Data Protection Congress; Privacy Law Scholars Conferences; ForumGlobal Data Privacy Conference; Privacy Laws & Business

5. OPCL personnel Kiran Natarajan, Hannah Mayer, Michelle Ramsden, and Jay Sinha, and former OPCL privacy analyst Jamie Huang attend an international privacy summit held in Washington, D.C., April 2024.

[39] *See* Appendix 1 for detail concerning speaking engagements during this reporting period.

International Conference; Regulation of AI, Internet and Data (RAID) fall and spring conferences; Privacy+Security Academy fall and spring conferences; American Bar Association conferences focused on antitrust, cybersecurity, and privacy; and Intelligence Community Legal Conferences. OPCL attorneys completed additional training in ethics, privacy, cybersecurity, and topics in their specialty areas to meet all mandatory, annual continuing legal education licensing requirements of their respective state bar associations.

4. CPCLO/OPCL LEGAL AND POLICY REVIEW AND GUIDANCE

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

- **Proposed legislation, policies, testimony, and Executive Branch department/agency reports:**
  OPCL and the CPCLO review proposed legislation, policies, testimony, and reports for privacy and civil liberties issues. These reviews have dramatically increased, from approximately 200 requests for review in FY2020, to 484 requests for review in FY2022, and 370 requests in FY2023.

- **Initial Privacy Assessments (IPA):**
  As explained above, an IPA is a privacy compliance tool developed by the Department to facilitate the identification of potential privacy issues, assess whether additional privacy documentation and controls are needed, and ultimately ensure the Department's compliance with applicable privacy laws and policies.[40] IPAs are conducted by Department components with oversight 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.[41]

- **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.[42] Each SORN is published in the Federal Register.

[40] For further information about the Department's IPA process, *see* U.S. Dept. of Just., *Privacy Compliance Process* (Oct. 5, 2023), https://www.justice.gov/opcl/privacy-compliance-process.
[41] *See* Off. of Mgmt. & Budget, Exec. Off. of the President, OMB M-03-22*, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (2002).
[42] *See* 5 U.S.C. § 552a(e)(4).

- **Privacy Act Exemption Regulations:**
  With certain conditions, the Privacy Act allows agencies to exempt systems of records from certain provisions of the Act by promulgating and publishing a regulation in the Federal Register that explains the basis for the exemption(s).[43]

- **Privacy Act Notices:**
  A Privacy Act Notice is a notice to individuals as required by subsection (e)(3) of the Privacy Act.[44] 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 part of the requested information.

- **Assessments required by OMB Circular A-130:**
  On July 28, 2016, OMB released an update to OMB Circular A-130 titled, *Managing Information as a Strategic Resource*.[45] 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 requirements for agencies to integrate their privacy programs into their Risk Management Framework (in accordance with NIST 800-37), including but not limited to, the selection, implementation, and assessment of the SP 800-53 Rev. 5 privacy and security controls (formerly Appendix J privacy controls). OPCL and OCIO have incorporated these requirements into the Department's SPAA Handbook.[46]

  OMB Circular A-130 requires assessments of the following, among others: 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 acquisition language, including the Contractor Privacy Requirements clause, DOJ-02, is used to impose privacy requirements, including those under the Privacy Act and OMB Circular A-130, on written agreements; Computer Matching programs to ensure compliance with computer matching requirements outlined in the Privacy Act; and agency programs for any privacy vulnerabilities.[47] These reviews are generally conducted annually along with the

[43] *See id.* § 552a(j), (k).
[44] *See id.* § 552a(e)(3).
[45] *See supra* note 8.
[46] U.S. Dept. of Just., *SPAA Handbook* (Nov. 30, 2023), https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/3-DOJ_Handbooks_Guides_Plans/DOJ-Security-Privacy-Assessment-and-Authorization-Handbook-v10_Final.pdf.
[47] *See supra* note 8.

Federal Information Security Modernization Act (FISMA)[48] reviews. FISMA review details are submitted through the annual FISMA report.[49]

- **Privacy Act Amendment Appeals:**
  Under the Privacy Act, individuals may request amendment of records about themselves, and if that request is denied, they may appeal. OPCL adjudicates the appeals of the denial of amendment requests.[50] During the Reporting Period, OPCL adjudicated 28 amendment request appeals.[51]

- **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 certain matters, such as the FISMA privacy audit and significant data breach situations. In addition, OPCL periodically receives requests for advice on questions of privacy law and policy.

- **FBI Whistleblower Redaction Reviews:**
  Pursuant to Deputy Attorney General direction, the Department has begun an effort to publish decisions regarding FBI whistleblower claims of unlawful reprisal. OPCL plays a key role in reviewing these decisions to facilitate appropriate publication.

IV. OPCL DOMESTIC LEADERSHIP AND ENGAGEMENT

The CPCLO and OPCL continued to lead or participate in a number of different internal and external working groups, committees, task forces, and other groups established for collaboration and coordination to advance agency missions.

1. ENGAGEMENT WITHIN THE DEPARTMENT

Within the Department, OPCL led or actively participated in the following working groups, committees, and other collaborative bodies within the Department. The CPCLO and OPCL also had various speaking engagements with Department components for training and guidance, as detailed in Appendix 1, CPCLO and OPCL Speaking Engagements:

- **Open Government:**
  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

[48] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).
[49] *See infra* text accompanying note 83.
[50] *See* 5 U.S.C. § 552a(d)(2), (3).
[51] U.S. Dep't. of Just., *Reports*, https://www.justice.gov/opcl/reports/reports.html.

CPCLO have committed to enhance transparency of federal use of investigative technologies.

- **OPEN Government Data Act:**
  In January 2019, Congress passed the Foundation for Evidence-based Policymaking Act of 2018.[52] 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).[53] 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 continues to coordinate and facilitate the implementation of Department-wide processes and standards, and for addressing common issues affecting Component data programs and resources.

- **AI, FRT, Data Brokers, and ETB:**
  OPCL engages in Artificial Intelligence (AI), Facial Recognition Technology (FRT), and Data Brokers working groups, and the recently established Emerging Technologies Board (ETB). In particular, the CPCLO and OPCL have a critical role in the Department's development of AI assessment processes pursuant to Executive Order 14110 and OMB Memorandum 24-10, co-chair the FRT and Data Brokers working groups, including leading the drafting and updating of associated policies and procedures, actively participate in ETB meetings and subgroups, and 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 these and other emerging technologies;[54]

  - Further, OPCL has actively participated in the White House's AI Equity IPC and has consulted with other government agencies on the EU AI Act's impact on the U.S.
  - As detailed further below, OPCL serves as a member of the U.S. delegation to the Council of Europe for the Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.

- **Crime Victims and Witnesses Attorney General Guidelines Working Group:**
  The CPCLO and OPCL worked to update Attorney General guidelines to provide stronger privacy protections to crime victims and witnesses as a matter of DOJ policy and have since served on the Department's Standing Committee for Crime Victims and Witnesses matters.

[52] The Foundation for Evidence-based Policymaking Act of 2018, Pub.L. 115–435, Stat. 2.14.
[53] *Id*.
[54] Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 14, 2019) (OPCL follows policies consistent with Executive Order 13859, Maintaining American Leadership in Artificial Intelligence); Exec. Order No. 13960, 85 Fed. Reg. 78939 (Dec. 8, 2020).

- **IT Acquisition Review and Department Investment Review Council:**
  The CPCLO and OPCL participate in DOJ IT Acquisition Review and Department Investment Review Committee meetings to ensure Department investments are privacy compliant and aligned with existing Department privacy policy.

- **Learning Development Committee (LDC):**
  The CPCLO and OPCL participate in the Department's learning advisory groups, including the LDC, its Mandatory Training Advisory Sub-group, and the Leadership Development Executive Board. Through these groups, OPCL provides feedback on the Department's training processes and ensures the effective inclusion of privacy considerations in training programs.

- **DOJ-wide Unmanned Aircraft Systems (UAS) Working Group:**
  OPCL advises the Department on privacy and civil liberties-related aspects of the development of UAS and Counter-UAS policies.

- **National Law Enforcement Accountability Database**:
  As directed by Executive Order 14074,[55] the Attorney General established the National Law Enforcement Accountability Database (NLEAD), to make policing safer and more effective by strengthening trust between law enforcement officers and the communities they serve, and to promote new and strengthened practices in the hiring, promotion, and retention of law enforcement officers. The NLEAD houses official records of federal law enforcement officer misconduct, commendations, and awards. The CPCLO and OPCL worked with stakeholders both within the Department and at other federal agencies to ensure that the objectives of Executive Order 14074 were achieved consistent with federal privacy laws and policy. The CPCLO serves on the Executive Board of the NLEAD.

- **Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act):**
  In November 2020, CASES was enacted and required each agency to accept electronic identity proofing and authentication processes for the purposes of allowing an individual to provide prior written consent for the disclosure of the individual's records, or access the individual's records, in accordance with the Privacy Act.[56] OPCL chairs the Department's CASES Act compliance working group, which is responsible for assessing the feasibility of solutions that, if adopted, would support the Department's compliance with the CASES Act's requirements for remotely identity-proofing end users seeking government services. During this reporting period, the CPCLO and OPCL, in coordination with the Office of Information Policy and the Justice Management Division, began efforts to implement the CASES Act requirements.

[55] *See* Exec. Order No. 14074, 87 Fed. Reg. 32945 (May 25, 2022).
[56] Pub L. No. 116-50, 133 Stat. 1073, 5 U.S.C. § 552a note.

- **Insider Threat:**
  OPCL participates in the Department's Insider Threat Council[57], advising Department and component leadership regarding insider threat issues. Insider Threat is defined in EO 13587 as "the threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of Departmental resources or capabilities."[58] Additionally, OPCL serves as a member of the Insider Threat Prevention and Detection Program (ITPDP) which prevents, deters, detects and mitigates insider threats. As a member of ITPDP, OPCL advises ITPDP on any privacy issues that may arise during an investigation, as well as assisting ITPDP with developing Privacy Act-compliant information collection or investigative techniques.

- **Use of Social Media:**
  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, 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 to ensure that the Department's uses of social media 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.[59] OPCL worked directly with components to review proposed uses of social media for privacy concerns and provided approval and compliance documentation for those requests; launched a working group with OPA and JMD OCIO to update the security requirements that Component social media account managers must adhere to.

- **COVID-19 Pandemic Response**:
  In response to M-21-15 COVID-19 Safe Federal Workplace: Agency Model Safety Principles (January 24, 2021), and M-21-25 Integrating Planning for A Safe Increased Return of Federal Employees and Contractors to Physical Workplaces with Post-Reentry Personnel Policies and Work Environment (June 10, 2021), OPCL worked closely with JMD to develop Department-wide policies and procedures to ensure appropriate compliance, and protect personnel from unwarranted risk of infection and harm while protecting individual privacy.[60]

[57] The Insider Threat Council is the successor to the Insider Threat Working Group, which was established by EO 13587, https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.
[58] Exec. Order No. 13587, 76 Fed. Reg. 63811 (2011).
[59] U.S. Dep't. of Just., *Social Media* (2024), https://www.justice.gov/social.
[60] *Id*.

2. ENGAGEMENT IN INTER-AGENCY WORK

The CPCLO and OPCL also engage in leadership roles or otherwise participate in inter-agency efforts, i.e., in collaborative working groups, task forces, committees, and councils, at times led by the Executive Office of the President, including the National Security Council and National Economic Council. OPCL participates in multiple Inter-Agency Policy Committees on various subjects that raise privacy and civil liberties concerns. OPCL also engages with federal privacy community and have developed and participated in events aimed at educating and engaging the federal workforce, the advocacy community, the public, and foreign officials on privacy-related topics. They also have consistently provided presentations to inter-agency audiences, as addressed on Appendix 1. Examples of such engagement include:

- **Federal Privacy Council:**
  On February 12, 2016, the President signed an Executive Order 13719 establishing the FPC.[61] 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.

- **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.[62] 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.[63] The CPCLO was responsible for reviewing this assessment, in which OPCL provided legal research, writing, and strategic assistance.

- **Cybersecurity Information Sharing Act of 2015 (CISA):**
  On December 8, 2015, President Obama signed CISA, including the Privacy and Civil Liberties Guidelines, into law.[64] It requires the Attorney General and the Secretary of Homeland Security to jointly develop, submit to Congress, and make publicly available interim and final guidelines relating to privacy and civil liberties, which govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with activities authorized in CISA.[65] During the reporting period, OPCL led

[61] Establishment of the Federal Privacy Council, 81 Fed. Reg. 7687 (Feb. 16, 2016).
[62] Cybersecurity Information Sharing Act of 2015, 81 Fed. Reg. 39061 (June 15, 2015).
[63] *Id*.
[64] Cybersecurity & Infrastructure Sec. Agency, *Privacy and Civil Liberties Guidelines: Cybersecurity Information Sharing Act of 2015* (Dec. 8, 2015), https://www.cisa.gov/resources-tools/resources/privacy-and-civil-liberties-guidelines-cybersecurity-information-sharing-act-2015#:~:text=Establishes%20privacy%20and%20civil%20liberties.
[65] *Id*.

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 guidelines were finalized in 2016, updated in June 2018, and then again in January 2021 and November 2022.[66]

- **National Vetting Center:**
  OPCL continued its longstanding work collaborating with other DOJ components as well as other departments and agencies on various terrorist and transnational organized crime watchlisting policies and processes, including as part of the Privacy, Civil Rights, and Civil Liberties Working Group reviewing the activities of the Center pursuant to National Security Presidential Memorandum-9.

3. ENGAGEMENT WITH PRIVACY ADVOCATES AND COMMUNITY STAKEHOLDERS

The CPCLO and OPCL staff meet with privacy advocates, business organizations, and academics regularly to discuss issues of concern to them. As an example, OPCL assisted in establishing the Department's JusticeAI Initiative and Privacy and Consumer Protection Roundtable in August 2024, with members of the public, e.g., civil society, academics, local government, and industry chief privacy officers. This roundtable was focused on AI's potential to magnify and accelerate risks to privacy and consumer rights, and opportunities for AI to advance the Department's mission to protect the rights of consumers.[67] OPCL also supported the Civil Rights Division's assistance to MASSAH communities (Muslim, Arab, Sikh, South Asian, and Hindu communities) and Jewish stakeholders.

V. OPCL LEADERSHIP AND ENGAGEMENT ON INTERNATIONAL PRIVACY MATTERS

Cross-border data flows are the lifeblood of the modern global economy – critical not only for large technology companies, but for big and small firms across all sectors, including manufacturing and agriculture. These data flows are also instrumental to international cooperation on health, finance, scientific research, and law enforcement and national security. While the increase in digitalization has spurred innovation and opportunities, it has also led to higher demands for effective data privacy frameworks given the risks associated with the improper use or sharing of personal data, data breaches, and indiscriminate government access to data. Consumers, businesses, and civil society are all demanding effective data privacy protections that also uphold democratic principles and the rule of law.

---

[66] *See* U.S. Dep't. of Just., *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (Jan. 4, 2021), https://www.cisa.gov/sites/default/files/publications/CISA_PCL_Guidelines_Periodic_Review_2020_final.pdf.

[67] *See* U.S. Dep't. of Just., *Update on Deputy Attorney General Lisa Monaco's Justice AI Convenings* (Aug. 16, 2024) https://www.justice.gov/opa/pr/update-deputy-attorney-general-lisa-monacos-justice-ai-convenings-0#:~:text=This%20week,%20Deputy%20Attorney%20General.

Although the key data protection and privacy principles are common among like-minded democracies, because of different cultures, histories, and legal regimes, the language and implementation of those principles can differ, at times creating inconsistencies between countries and conflicts of law that pose challenges to public and private organizations transferring data across borders. The CPCLO and OPCL are deeply involved in multilateral and bilateral efforts designed to harmonize data protection and privacy legal frameworks, to ensure that the Department has the personal data needed to advance its missions and protect the public. The CPCLO and OPCL personnel regularly provide presentations and engage in international workshops and other forums to support harmonization of legal frameworks, collaboration, and coordination with foreign partners.[68] They also have been instrumental on U.S. delegations in negotiating international agreements and arrangements. They support the Department of State and Department of Commerce in developing interoperable approaches to data governance and privacy based on democratic values and rule of law, with the goal of bringing additional like-minded countries into U.S.-supported legal frameworks. Ensuring that effective data privacy protections are consistent with the U.S. approach to open data flows is critical for advancing democratically aligned technology development, upholding our shared values of openness, and protecting human rights and fundamental freedoms, including privacy.

6. OPCL Director, Katherine Harman-Stokes, and Senior Counsel, Hannah Mayer, speak at the Privacy Symposium in Venice, Italy, June 2024.

1. U.S.-EU DATA PRIVACY FRAMEWORK

For several years, the CPCLO and OPCL have worked closely with colleagues at the Office of the Director of National Intelligence (ODNI), the Department of Commerce, and other Federal departments and agencies as a part of the comprehensive effort to negotiate a new data privacy framework between the United States and the European Union (EU).

On March 25, 2022, President Biden and European Commission President von der Leyden announced that the United States and the EU have committed to a new U.S.-EU Data Privacy Framework.[69] The Framework is designed to foster trans-Atlantic data flows and address the

[68] *See* Appendix 1 for detail concerning speaking engagements during this reporting period.
[69] *See* Press Release, White House, *United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework* (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/#:~:text=The%20United%20States%20and%20the%20European.

concerns raised by the Court of Justice of the European Union in its *Schrems II* decision of July 2020 concerning the impact of U.S. signals intelligence activities on the privacy of EU data transferred to the United States, and which invalidated an important pre-existing basis in EU law, based on the EU-U.S. Privacy Shield Framework, for transfers of personal data from the EU to the United States relied on by thousands of companies in the United States and Europe.[70]

On October 7, 2022, President Biden signed Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities."[71] The Executive Order bolsters an already rigorous array of privacy and civil liberties safeguards for U.S. signals intelligence activities and created a two-layer independent and binding mechanism enabling individuals in qualifying states and regional economic integration organizations, as designated under the order, to seek redress if they believe their personal data was collected through U.S. signals intelligence in a manner that violated applicable U.S. law. Under the first layer of the redress mechanism, the Civil Liberties Protection Officer in the Office of the Director of National Intelligence (CLPO) will conduct an initial investigation of qualifying complaints received to determine whether the order's enhanced safeguards or other applicable U.S. law were violated and, if so, to determine the appropriate remediation. The order also establishes that the CLPO's decision will be binding on the Intelligence Community, subject to the second layer of review, and provides protections to ensure the independence of the CLPO's investigations and determinations.

As a second layer of review, the order authorized and directed the Attorney General to establish the DPRC to provide independent and binding review of the CLPO's decisions, upon an application from the individual or an element of the Intelligence Community. The Attorney General issued regulations establishing the DPRC on October 7, 2022.[72] Judges on the DPRC are appointed from outside the U.S. Government, have relevant experience in the fields of data privacy and national security, review cases independently, and enjoy protections against removal. Decisions of the DPRC regarding whether there was a violation of applicable U.S. law and, if so, what remediation is to be implemented, are binding on the Intelligence Community. To further enhance the DPRC's review, the order provides for the DPRC to select a special advocate in each case who will advocate regarding the complainant's interest in the matter and ensure that the DPRC is well-informed of the issues and the law regarding the matter.

On June 30, 2023, the Attorney General designated the European Union and the European Economic Area as "qualifying states" for purposes of implementing the redress mechanism established in Executive Order 14086.[73] This designation became effective on July 11, 2023, after the European Commission's adoption on July 10, 2023, of an adequacy decision for the United States as part of the EU-U.S. Data Privacy Framework. The European Commission's adequacy decision relied, in part, on the establishment of the DPRC in determining that the United States provided an adequate level of protection for personal data transferred under the EU-U.S. Data

[70] *Id.*
[71] 87 Fed. Reg. 62283 (Oct. 7, 2022).
[72] *Id*.
[73] *See* Attorney General Designations of the European Union, Iceland, Liechtenstein, and Norway as "Qualifying States," 88 Fed. Reg. 44844 (June 30, 2023).

Privacy Framework.[74] Subsequently, on September 18, 2023, the Attorney General designated the United Kingdom (UK) as a "qualifying state" for purposes of implementing the redress mechanism established in Executive Order 14086.[75] This designation became effective on October 12, 2023, when the UK regulations implementing the data bridge for the UK Extension to the EU-U.S. Data Privacy Framework entered into force. On June 7, 2024, the Attorney General designated Switzerland as a "qualifying state" for purposes of implementing the redress mechanism established in Executive Order 14086.[76] That determination became effective on September 15, 2024, when the corresponding amendment to the Swiss Data Protection Ordinance entered into force.[77]

Under the Attorney General's regulations, OPCL provides administrative support to the DPRC. Throughout the reporting period, the CPCLO and OPCL worked to establish the DPRC and ensure that it is equipped to process applications for review of the CLPO's determinations when received. This has included supporting the Attorney General with consultations regarding DPRC judges and Special Advocates, and on-boarding those DPRC judges and Special Advocates selected by the Attorney General.[78] The CPCLO and OPCL also have requisitioned equipment and classified facilities for the DPRC's use and provided recordkeeping and public communications support. In January 2024, the Court issued detailed Frequently Asked Questions, detailing information about the Court.[79]

2. ORGANIZATION FOR ECONOMIC DEVELOPMENT AND COOPERATION (OECD) DECLARATION ON GOVERNMENT ACCESS

The CPCLO and OPCL were part of the U.S. delegation in drafting and negotiating the OECD Declaration on Government Access to Personal Data Held by Private Entities. This effort stemmed from a concern about the absence of principles specifying privacy protections that OECD members follow when governments access personal data; the 1980 OECD Privacy Principles do not cover government access to data for national security and law enforcement. The Declaration developed seven core principles for government access to fill that gap and to address the growing concern about countries accessing data inconsistent with rule of law and democratic principles.

To succeed in drafting the Principles and build trust among democracies—distinguishing the U.S. and like-minded countries from authoritarian regimes—the principles needed to accurately identify the current safeguards in place, i.e., current laws, and how those laws are implemented. It was critical to have practitioners and experts, especially national security experts,

---

[74] *See* Commission Implementing Decision of 10.7.2023, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (July 10, 2023), at ¶¶ 175-176, 184-192.
[75] *See* Attorney General Designation of the United Kingdom as a "Qualifying State," 88 Fed. Reg. 65405 (Sept. 18, 2023).
[76] Attorney General Designation of Switzerland as a "Qualifying State," 89 Fed. Reg. 50377 (June 7, 2024).
[77] *See* Press Release, Swiss Fed. Council, *Swiss-US Data Privacy Framework: Certified US companies offer adequate protection for personal data* (Aug. 14, 2024) https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-102054.html.
[78] *See, e.g.*, Press Release, U.S. Dep't. of Just., *Attorney General Merrick B. Garland Announces Judges of the Data Protection Review Court* (Nov. 14, 2023) https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[79] *See* U.S. Dep't. of Just., *DPRC Resources* (2024), https://www.justice.gov/opcl/dprc-resources.

involved in the discussion. These experts have the insight and experience to facilitate identifying and drafting meaningful and accurate principles, in sufficient detail, that highlight shared values. Previously, much of the data protection debate was solely focused on transatlantic data flows. With the OECD effort, the debate shifted to a global debate and, importantly, an exchange of accurate information. During the reporting period, over thirty-five countries had agreed to follow the Declaration.

3. THE FINANCIAL ACTION TASK FORCE (FATF)

In late 2021, the U.S. Department of Treasury requested that OPCL co-chair a project organized by the Financial Action Task Force (FATF) to promote information sharing between financial institutions to improve detection and investigation of money laundering and terrorist financing, while also complying with data protection and privacy laws, regulations, and policies. The FATF is the global money laundering and terrorist financing watchdog—an inter-governmental body that sets international standards to prevent these illegal activities and the harm they cause to society.

With current technology, a single financial institution has only a partial view of transactions and sees one small piece of what is often a large, complex puzzle. It is increasingly difficult for individual financial institutions to detect these illicit activities. By using collaborative analytics, bringing data together, and developing other sharing initiatives in responsible ways, financial institutions seek to build a clearer picture of the puzzle, to better understand, assess, and mitigate money laundering and terrorist financing risks.

8. OPCL Director, Katherine Harman-Stokes, speaks at the Financial Action Task Force plenary in June 2022.

OPCL accepted the role of co-chair, with support from the DOJ Criminal Division and National Security Division, Treasury, and Financial Crimes Enforcement Network (FinCEN). OPCL and the other co-chair, the Netherlands financial intelligence unit (FIUs), held multiple focus groups with financial institutions, financial regulators, FIUs, and privacy regulators in a dozen countries, including Germany, Estonia, Netherlands, United States, and Singapore. Each focus group addressed a specific information sharing initiative, how the initiative was designed to comply with data protection and privacy requirements, the collaboration between financial and privacy regulators and financial institutions, and best practices, concerns, and what to avoid. This work resulted in a report, Partnering in the Fight Against Financial Crime: Data Protection, Technology, and Private Sector Information Sharing, adopted by the FATF Plenary and published on July 20, 2022.[80] The report aims to help jurisdictions responsibly enhance, design and implement information collaboration initiatives

[80] *See* Fin. Action Task Force, *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing* (2022), https://www.fatf-gafi.org/publications/digitaltransformation/partnering-in-the-fight-against-financial-crime.html?hf=10&b=0&s=desc(fatf_releasedate.

among private sector entities, in accordance with privacy requirements, so that the risks associated with increased sharing of personal data are appropriately taken into account.

4. ADDITIONAL INTERNATIONAL LEADERSHIP AND ENGAGEMENT

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.

- **Council of Europe, Cybercrime Convention, Second Additional Protocol**:
  The U.S. continued and concluded its negotiations in the Council of Europe on the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence on behalf of the U.S. government. OPCL participated as a member of the delegation advising on issues related to personal information and data protection matters. This strengthening and expansion of the multilateral international treaty commonly called the Budapest Convention is part of the United States' steadfast commitment to helping nations, including the United States, fight cybercrime by obtaining access to needed electronic evidence within a privacy-protective legal framework. The Department's delegation in the negotiations from OPCL and the Criminal Division received an Attorney General's Award for Distinguished Service, the Department's second highest recognition for employee performance.

- **Council of Europe, Convention on AI:**
  The U.S. joined the negotiations in the Council of Europe on the Convention on Artificial Intelligence, Human Rights, and the Rule of Law. OPCL joined the U.S. delegation, advising on issues related to personal information and data protection matters as applied in the context of artificial intelligence.

- **CLOUD Act:**
  The U.S. continued and concluded its negotiations with Australia on a CLOUD Act Executive Agreement,[81] and is supporting Criminal Division in negotiations with European Union. The CPCLO and OPCL continued to assist the Department in meeting many of its disclosure obligations under the CLOUD Act. The CLOUD Act authorizes bilateral agreements between the United States and trusted foreign partners that will make both nations' citizens safer, while at the same time ensuring a high level of protection of those citizens' rights.

- **Global Privacy Assembly (GPA),** *f/k/a, International Conference of Data Privacy and Protection Commissioners (ICDPPC):*
  The CPCLO consistently has been accredited as an observer and, along with the OPCL Director, attended the annual meetings of the Global Privacy Assembly (GPA) in 2021, virtually, and in 2022 and 2023, in person. In 2023, they were joined by the

[81] *See* U.S. Dep't. of Just., *Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime* (Dec. 15, 2021), https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-and-australia.

OPCL Senior Counsel dedicated to the Data Protection Review Court (DPRC). 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.

- **G7 Data Protection Authority Roundtable:**
  The CPCLO and OPCL actively participate in the Group of 7 (G7) Data Protection Authorities Roundtable. They attended the annual meetings in 2022 in Bonn, Germany; 2023 in Tokyo, Japan; and 2024 in Rome, Italy, and they consistently contribute to Roundtable working groups. Through the Roundtable, the G7 DPAs collaborate and share knowledge on key global data protection and privacy issues, such as privacy safeguards in AI and other emerging technologies, international enforcement cooperation, advancing "Data Free Flow with Trust" initiatives, working towards interoperability of cross-border data transfer tools to facilitate transfers and achieve a high level of data protection, and promoting trusted government access, including their support for the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities.

9. OPCL Director, Katherine Harman-Stokes, participates in G7 Data Protection Authority Roundtable in Bonn, Germany, 2022.

- **EU-U.S. Trade and Technology Council**:
  OPCL led the Department's engagement with EU-U.S. Trade and Technology Council working groups addressing artificial intelligence, tech platform governance, and mitigating the misuse of technology, including disinformation and the arbitrary or unlawful use of surveillance technology by undemocratic governments.

- **Efforts Through the United Nations**:
  The CPCLO and OPCL have engaged with United Nations Officials and the U.S. Department of State, advising regarding revisions to resolutions and other material concerning privacy and civil liberties matters, including issues raised by other countries or international organizations such as the Freedom Online Coalition, Human Rights Council, and the Red Cross and Red Crescent Movement.

- **Financial Stability Board**:
  As part of a G20 workstream, the Financial Stability Board (FSB) is focused on minimizing "friction" in payment data chains, which includes addressing challenging, at times conflicting, cross-border data protection and privacy requirements. During this reporting period, the FSB began leveraging existing data protection and privacy forums to work toward harmonizing cross-border privacy legal frameworks. OPCL assisted the Department of Treasury and the FSB in connecting with the Global Privacy Assembly (GPA) and OECD Digital Policy Committee. OECD's adoption of the Declaration on Government Access to Personal Data Held by Private Sector Entities could provide a useful roadmap for the FSB, potentially with OECD support, to identify common principles in like-minded countries that impact international financial payments.

In addition, OPCL engaged with foreign officials in dialogues pertaining to the U.S. sectoral privacy regime and comparative systems around the world and participated often in international panels and other speaking engagements which enabled OPCL to support the approach of both the Department and the U.S. to privacy law and policy. OPCL contributed to the Department's review of international laws and regulations significantly impacting privacy and provided substantive comments on the impact of those laws on information governance in the U.S. and by the U.S. Government. The CPCLO and OPCL attorneys also provided training to the interagency on international privacy laws, regulations, and policies and advised on data protection questions that impact the Department and interagency.

VI. ACCOUNTABILITY AND REPORTING

The CPCLO and OPCL are responsible for issuing and contributing to numerous Department privacy reports, including: this Report, i.e., 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 section of annual reports in accordance with the FISMA; and annual reports required by the Social Security Number Fraud Reduction Act of 2017 (SSN Act). Certain reports from this reporting period that have been approved by OMB and transmitted to Congress can be found on OPCL's webpage.[82]These reports are described in more detail below:

[82] U.S. Dep't. of Just., *Reports*, https://www.justice.gov/opcl/reports/reports.html.

- **Federal Information Security Modernization Act of 2014 (FISMA) Annual Report:** Federal agencies are required to submit annual reports to OMB, Congress, and the Government Accountability Office (GAO) regarding their privacy programs in accordance with the FISMA and OMB guidance implementing the FISMA.[83] The annual report requires OPCL to report 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 breach response activities, SSN reduction efforts, as well as programmatic aspects of the Department's privacy program, such as training, workforce development, budget and acquisition.

  The Department's Inspector General (IG) also conducts its own audit of the Department's information security and privacy programs. OMB has selected a core group of metrics that must be evaluated annually, which include the NIST 800-53 privacy controls. The remainder of the controls are evaluated on a two-year cycle as identified by OMB. OPCL coordinates with the IG on these FISMA control assessments and remediates any privacy control deficiencies identified as a result of the audit.

- **Privacy and Civil Liberties Activities Semi-Annual Section 803 Reports:** The CPCLO continues to submit 803 Reports to Congress and the PCLOB, now on an annual basis due to recent statutory requirement change. The content of the 803 Reports includes 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.

- **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 a DOJ Privacy Policy, available on its central website.[84] 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 comply with Federal and DOJ content policies and guidelines. Included in the quarterly submission is a certification that the component is meeting DOJ Privacy Policy requirements.

---

[83] *See* 44 U.S.C. § 3544(c) (2014); *see also* Off. Of Mgmt. & Budget, Exec. Off. Of the President, M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* (Dec. 4, 2023).
[84] U.S. Dep't. of Just., *Privacy Policy* (2024), https://www.justice.gov/doj/privacy-policy.

- **Report for the Social Security Number Fraud Reduction Act of 2017 (SSN Act):** The SSN Act requires federal agencies to cease the mailing of documents containing full SSNs by September 15, 2022, unless the head of the agency deems such mailings necessary, by which time the agencies must promulgate regulations specifying the circumstances under which inclusions of full SSNs in mailings are necessary. In addition, the Act requires a series of annual reports to Congress for five years, including an inventory of the types of documents containing full SSNs that the agency used and information regarding the agency's plan to achieve full compliance with the Act. The Department has submitted its Initial, First, Second, Third, and Fourth and Fifth Annual Reports on the Department's implementation of the Act's restrictions on the mailing of SSNs and provided an inventory of all the documents in which the inclusion of SSNs is necessary. Upon submission of its Fifth annual report, the Department has satisfied its reporting requirements under the SSN Act.

APPENDIX 1 - CPCLO AND OPCL ADDITIONAL SPEAKING ENGAGEMENTS

The CPCLO and OPCL attorneys and analysts provided training within the Department and to other U.S. Government agencies. With their expertise and experience in U.S. and international privacy law, they also have been invited to speak or have had their proposals accepted to speak at conferences, symposiums, summits, workshops, and meetings with U.S. and foreign officials, associations, and the public. These speaking engagements advance the Department's mission. They provide significant opportunities for the CPCLO and OPCL to reinforce the United States' commitment to protecting privacy and civil liberties; inform others about privacy and civil liberties safeguards in the U.S. legal framework, in particular to support cross-border data transfers; learn from other officials and experts; and often help shape the privacy and civil liberties legal frameworks within the United States and around the world.

The CPCLO and OPCL attorneys and analysts have repeatedly presented at conferences and programs hosted by the following organizations[85]:

10. OPCL Director, Katherine Harman-Stokes, speaks at the Privacy Symposium, Venice, June 2024.

- American Bar Association (ABA): In February 2023, the CPCLO spoke about protecting the public trust through privacy oversight frameworks at an ABA conference. He also spoke on OECD Declaration on Government Access to Personal Data Held by Private Entities, and the DPF, at the ABA Consumer Protection & Data Privacy Conference in San Diego, California.

- Biometrics Institute: The CPCLO and OPCL attorneys regularly speak at Biometrics Institute conferences and programs. For example, in June 2022, OPCL's Law Enforcement & National Security Unit Chief spoke at the Biometrics Institute as the keynote speaker on biometrics and public trust, and several OPCL Senior Counsel have spoken in later programs about facial recognition technology and AI.

- Brookings Institution: The CPCLO has spoken several times at Brookings Institution events, e.g., in October 2022, the CPCLO spoke on the EU-US Data Privacy Framework.

- Department of Commerce, Global Cross-Border Privacy Rules (CBPR) Forum: An OPCL Senior Counsel has been a key expert and advisor in the Global CBPR Forum capacity-

[85] The reference to private and public organizations, and conferences or events hosted or sponsored by such organizations, is solely to provide information about CPCLO or OPCL activity and does not imply endorsement by the Department of Justice, CPCLO, or OPCL personnel.

building workshops, presenting on U. S. and other legal frameworks, to help authorities in other countries build their own data protection and privacy legal frameworks and help harmonize different legal frameworks to advance DOJ's mission. She has participated in workshops in London, UK, and Egypt, Germany, Argentina, Kenya, and other countries.

11. OPCL Senior Counsel, Hannah Mayer, participates in the Global Cross-Border Privacy Rules (CBPR) Forum Workshop in Buenos Aires, Argentina, June 2023.

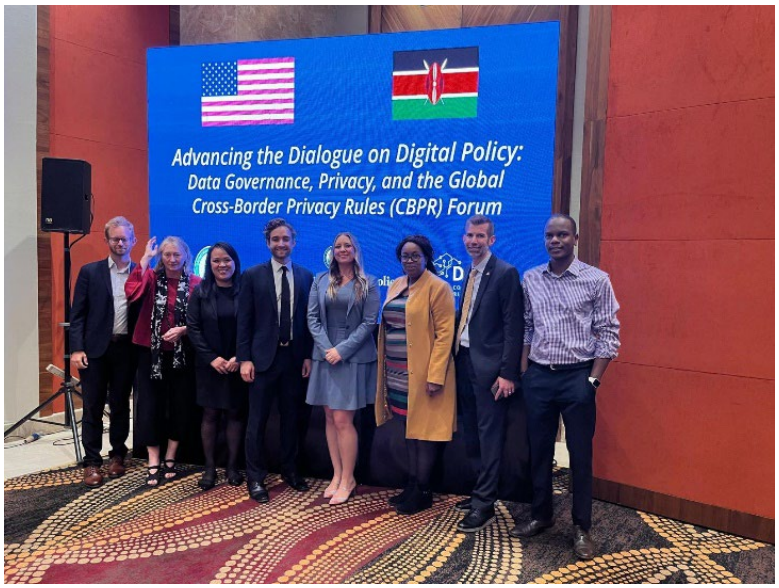
- Council of Europe: In addition to participating in the U.S. delegation negotiating various Council of Europe (CoE) international treaties and other instruments, as explained above, in November 2022, the CPCLO spoke on the DPF at a CoE program in Strasbourg, France, and in January 2023, an OPCL Senior Counsel spoke about AI at the CoE Plenary in Strasbourg.

- Federal Privacy Council: The CPCLO and OPCL actively participate in the U.S. Federal Privacy Council (FPC),[86] the principal interagency forum to improve the privacy practices of agencies. The FPC works to strengthen protections of information about individuals and privacy rights across the Federal Government. The CPCLO is a member of the FPC Executive Committee, OPCL attorneys and analysts support and often lead FPC committees and working groups, and they provide training on a variety of issues. As examples, the CPCLO and OPCL attorneys and analysts participated as speakers at the: 2020 FPC Summit, discussing the Overview of the Privacy Act of 1974, 2020 Edition; at the January 2023 FPC Summit, on "Exploring International Privacy Issues," "Emerging Trends in AI Governance," and providing a "Privacy Case Law Update"; at the January 2024 FPC Summit, on "Ensuring Privacy Compliance in Third-Party Contracts," and "Data Breach Best Practices." They also regularly give presentations in FPC Agency Implementation Committee programs and have served on the faculty of the FPC "boot camp" since 2016, when that training program for federal privacy professionals began. This includes presentations on privacy compliance in vendor contracts, compliance when addressing commercially available information, responding to data breaches, and "Emerging Trends in AI Governance."

- Financial Action Task Force (FATF): In March 2021, the Director of OPCL spoke at the FATF roundtable discussion on "Data Pooling, Analysis and Data Protection," and spoke on related issues at a "Roundtable on Data Protection Issues" with the U.S. Department of Treasury. In June 2022, the Director spoke at five different FATF meetings/conferences to discuss the "Fight Against Financial Crime: Data Protection, Technology, and Private Sector Information Sharing," and the focus groups and report adopted at the FATF Plenary, "Partnering in the Fight Against Financial Crime: Data Protection, Technology, and Private

[86] *See* Federal Privacy Council, https://www.fpc.gov/.

Sector Information Sharing." In August 2022, the Director of OPCL spoke at the Privacy Enhancing Technology (PET) FinCrime Challenge, and an OPCL Senior Privacy Analyst participated in the demonstrations of PETs that won the U.S.-U.K. Prize Challenge on detecting financial crime while strengthening privacy safeguards.



12. OPCL Senior Counsel, Hannah Mayer, participates in the Global CBPR Forum Workshop in Nairobi, Kenya, August 2023.

- Forum Europe/Forum Global: In September 2021, the CPCLO spoke at Forum Europe/Forum Global's Third Annual Data Privacy Conference USA on "Data Privacy, AdTech, Antitrust and implications for a fair, trustworthy, competitive and innovative digital ecosystem." He also discussed privacy ethics on a different panel at the conference. In September 2022, the CPCLO spoke on "Lawful Access to Data and Privacy Considerations" at Forum Global's 4th Annual Data Privacy Conference USA in Washington D.C.

- Global Privacy Assembly (GPA) (f/k/a International Conference of Data Protection and Privacy Commissioners (ICDPPC)): As noted above, the CPCLO is accredited as an observer at the GPA, and along with the OPCL Director, has attended each GPA annual meeting during the reporting period. The CPCLO and OPCL are consistently engaged with GPA meetings, programs, committees, and working groups. In addition, they have given presentations at the open and closed government-only sessions at the GPA annual meeting. For example, they hosted and led a roundtable discussion on biometrics; in October 2022, the CPCLO spoke on International Data Flows in the opening session in Istanbul, Turkey; and in October 2023, the CPCLO and Director of OPCL spoke at the Global Privacy Assembly Annual Meeting in Bermuda.

- George C. Marshall Center, European Center for Security Studies: In June 2021, an OPCL Senior Counsel spoke in the "Military and National Security Data & Information Protection Online Workshop," and in June 2022, the OPCL Director and an OPCL Senior Counsel discussed the Trans-Atlantic Data Privacy Framework, in an engagement titled "Upcoming EU-US Privacy Shield 2.0 – Overview on the Current Status" at the Military and National Security Data and Information Protection Online Workshop hosted by the George C. Marshall European Center for Security Studies. In June 2023, an OPCL Senior Counsel spoke to the Data Protection Workshop in Berlin, Germany. In June 2024, an OPCL Senior Counsel spoke at the latest Data Protection Workshop in The Hague, Netherlands.

- State Bar of Georgia: An OPCL Senior Counsel speaks regularly at Georgia Bar conferences and programs. As examples, in 2022, she discussed how to break into the field of privacy law; in March 2023, she gave a presentation on "International Data Transfers." In March 2024, several OPCL staff spoke at a Georgia Bar two-day conference. A Senior Counsel spoke about the DPF and DPRC; two OPCL Senior Counsel spoke on emerging technologies, including AI, and on online safety issues; and a Senior Counsel and Senior Privacy Analyst spoke on a panel about Privacy-Enhancing Technologies (PETs).

- International Association of Privacy Professionals (IAPP): The CPCLO and OPCL attorneys and analysts regularly speak on panels at IAPP conferences and other programs, including the IAPP Global Summit; IAPP Data Protection Congress, held annually in Brussels; IAPP Privacy, Security, Risk program; KnowledgeNet and other programs. This includes: June 2021, the OPCL Director discussed the importance of "Creating Privacy Protections for Government Requests Across Borders"; in November 2022, the CPCLO spoke on the EU-U.S. Data Privacy Framework (DPF); in December 2022, the CPCLO spoke on OECD Declaration on Government Access to Personal Data Held by Privacy Entities and the DPF; April 2022, the CPCLO spoke on "Government Access to Data for National Security and Law Enforcement Purposes: Convergence for the EU and U.S. Approaches?"; April 2023 and April 2024, the CPCLO spoke on panels at the IAPP Global Privacy Summit, providing updates on the DPF and Data Protection Review Court (DPRC). In addition, OPCL attorneys presented on the DPF at separate IAPP KnowledgeNet sessions in May and September 2023. The discussions, which included panelists from the private sector, focused on the DPF and the DPF's new independent and binding redress mechanism under Executive Order 14086, with additional focus on the DPRC.

13. OPCL Senior Counsel, Michelle Ramsden, speaks at Privacy Laws & Business Conference, Cambridge, UK, July 2024.

- Organization for Economic Development and Cooperation (OECD): The CPCLO and OPCL consistently have been engaged in OECD work and have actively participated in negotiations of international instruments, as discussed further above. In addition, in December 2022, the CPCLO spoke on legal framework governing the use of AI by Federal Government agencies and spoke on the "Trusted Government Access Principles" at the OECD Ministerial in the Canary Islands, Spain. In April 2022, the OPCL Director spoke at an OECD meeting about the FATF "Partnering in the Fight Against Financial Crime" report.

- Privacy Laws & Business: In July 2023, an OPCL Senior Counsel spoke on the DPF and DPRC, and in July 2024, another Senior Counsel participated in a panel, "Online Privacy Invasion and its Impact on Women."

- Regulation of AI, Internet, and Data (RAID): October 2022, the OPCL Director spoke on a RAID panel in Brussels, Belgium, entitled "Come Together: Regulatory Convergence"; in May 2023, the Director spoke on "Tackling Global Challenges Together," and also gave presentations in September 2023, May 2024, and September 2024.

14. OPCL Director, Katherine Harman-Stokes, speaks on a panel at RAID, 2024.

- Spanish Association for the Promotion of Information Security (ISMS): The CPCLO spoke at the ISMS Privacy Forum, Data Privacy Institute (DPI) Forum, in February 2021, 2022, and 2023, for example, speaking on "Privacy Governance" and on the DPF at the 15th Privacy Forum of ISMS in Spain.

- Privacy Symposium: The Privacy Symposium is hosted by Ca' Foscari University, Venice, Italy, and organized in collaboration with the CoE, European Centre for Certification and Privacy, European Cyber Security Organization, and additional partners. In April 2022, both the CPCLO and the Director of OPCL spoke at the Privacy Symposium. The CPCLO spoke on the "Outlook on Data Protection Evolution Across the World (Beyond the European Union)" and provided the closing remarks, and the Director spoke on "Data Protection in Practice." In April 2023, and June 2024, the CPCLO, OPCL Director, and OPCL Senior Counsel spoke about the DPF and DPRC, the OECD Declaration on Government Access to Personal Data Held by Private Entities, AI and other emerging technology, and cross-border data transfers and efforts to harmonizing different privacy legal frameworks.

Additional speaking engagements, chronologically:

- October 2020: The CPCLO participated in a panel at a Gruter Institute program.

- March 2021: The CPCLO participated on a panel hosted by the Open Group entitled "Information Governance & Digital Transformation: A New Approach to Data Protection and Privacy."

- March 2021: The CPCLO spoke about privacy governance at a program hosted by the Cross Border Data Forum.

- March 2021: The CPCLO discussed the importance of "Data Protection and Privacy Crisis" at a program hosted by the U.S. Department of Health and Human Services (HHS) Privacy Committee.

- April 2021: The CPCLO participated on a panel discussing "System of Trust" held by LegalWeek 2021.

- July 2021: The CPCLO discussed "The Future of Data: Privacy Foundations and Legislative Approaches" at the Internet Governance Forum USA 2021.

- October 2021: The OPCL Director participated in a privacy panel at the Annual Cyber Security & Privacy Month at a 2U Conference.

- December 2021: The CPCLO spoke to the Iraq Delegation on "The Impact of Data Protection Regulation on the Digital Economy."

- December 2021: An OPCL Senior Counsel participated in the 2021 Internet Governance Forum, speaking on Open Forum #57 "The Role of Regulation in a Post Pandemic Context."

- February 2022: The CPCLO spoke at Uniform Law Commission, National Conference of Commissioners on Uniform State Laws, on the topic of the Uniform Personal Data Protection Act.

- March 2022: The Director of OPCL spoke at a symposium hosted by the Future of Financial Intelligence Sharing (FFIS) and the Royal United Services Institute (RUSI) on "U.S. High-Level Roundtable on 314(b) Effectiveness." She also spoke at a program hosted by FFIS on the topic "Collaboration in Combatting Economic Crime."

- May 2022: The Director of OPCL spoke at the Computers, Privacy and Data Protection Conference (CPDP), on "The Future of Global Data Flows," in Brussels, Belgium.

- June 2022: The OPCL Director spoke at a program on cross-border data sharing to combat financial crime hosted by FFIS, in conjunction with presentations at the June 2022 Plenary of the Financial Action Task Force (FATF), discussed above.

- June 2022: An OPCL attorney participated in the Atlantic Council's Digital Forensics Research Lab, 360/Open Realities Summit, and EU-U.S. Trade and Technology Council bilateral events around the misuse of technology and disinformation in Brussels, Belgium.

- July 2022: An OPCL attorney spoke at the National Academy of Science on "Facial Recognition Current Capabilities Future Prospects and Governance Meeting: Key Legal and Policy Considerations in Facial Recognition Systems."

- September 2022: The OPCL Director spoke and participated in the three-day EU-U.S. Expert Workshop on "Legal Gateways in the Fight Against Terrorism Financing," in Lyon, France. This program was part of the EU-funded BeCaNet project, an international

initiative against terrorism financing supported by authorities in Germany, France, Spain, the U.S., and Europol.

- October 2022: An OPCL attorney spoke on the "Intersection of Privacy and Antitrust Law" at the Mexican Federal Telecommunications Institute (IFT).

- November 2022: The CPCLO spoke on a panel discussing Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities," and the related Attorney General regulation on the "Data Protection Review Court," both of which served as the foundation of the EU-U.S. Data Privacy Framework, discussed above, at the International Intelligence Oversight Forum (IIOF).

- November 2022: The CPCLO spoke at a workshop organized by the EU-U.S. Tech and Data Governance Working Group on freedom of expression and constitutional limits in the Federal Government's ability to protect personal data and ensure appropriate moderation of content on internet platforms.

- January 2023: The Director of OPCL moderated a breakout session discussing the EO 14086 at the 6th Annual Intelligence Community (IC) Civil Liberties, Privacy and Transparency (CLPT) Summit.

- February 2023: The CPCLO spoke on cross-border data sharing at a Chatham House taskforce meeting.

- March 2023: The CPCLO spoke at the Data Protection Conference in Lyon, France.

15. OPCL Senior Counsel, Hannah Mayer, speaking on a panel with a senior official from France and others at the Privacy Laws and Business Conference at Cambridge University, UK, July 2023.

- April 2023: The OPCL Director spoke, virtually, at the German-American Data Protection Day held in Berlin.

- May 2023: The Director of OPCL spoke on a panel at the Privacy+Security Forum in Washington, D.C.

- June 2023: At RightsCon, held in San Jose, Costa Rica, the OPCL Director spoke on "Promoting Trust in Law Enforcement and National Security: International Developments in Safeguards, Oversight, and Redress"; an OPCL Senior Counsel spoke on "Human Rights; Online Harms, Violence Against Women."

- April 2024: An OPCL Senior Counsel spoke about current data privacy challenges at the W&M Data Privacy & Cybersecurity Legal Society at William & Mary School of Law in Williamsburg, Virginia (webinar).

- May 2024: An OPCL Senior Counsel spoke at the Privacy and Security Academy at George Washington University.

- June 2024: An OPCL Senior Counsel spoke at the Video Game Bar Association Summit 2024 in Los Angeles, California on "Insights from DOJ OPCL – EU-U.S. Data Privacy Framework, Breach Response Trends, and More."

- June 2024: An OPCL Senior Counsel, Privacy Analyst, and the CPCLO spoke at the FedID conference in Baltimore, Maryland. The panels were titled "Privacy and Security: Managing Risks Associated with Biometric ID Systems" and "Select Privacy and Legal Considerations in Federal Identity: CAI, FRT, Biometrics and CASES Act."

- June 2024, an OPCL Attorney spoke at the George C. Marshall Center Data Protection Workshop in The Hague, Netherlands.

16. OPCL Senior Counsel, Michelle Ramsden, speaks at the George C. Marshall Center, Data Protection Workshop, at the Hague, Netherlands, June 2024.

- July 2024: An OPCL Senior Counsel spoke on elements of the EU-U.S. Data Privacy Framework in light of the relevant caselaw of the Court of Justice of the European Union (CJEU) and the European Convention Human Rights (ECHR), and to raise broader observations about the concept of essential equivalence. This was at the invitation of the U.S. Commerce Department and the law firm of August DeBouzy in Paris, France.

- August 2024: An OPCL Senior Counsel spoke about Privacy 101 at the USTP OIT Conference.