U.S. Department of Justice

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

PRIVACY AND CIVIL LIBERTIES ACTIVITIES SEMI-ANNUAL REPORT

SECOND SEMI-ANNUAL REPORT, FY 2015

APRIL 1, 2015 – SEPTEMBER 30, 2015

United States Department of Justice

Semi-Annual Section 803 Report

Message from the Chief Privacy and Civil Liberties Officer

I am pleased to present the Department of Justice's (Department or DOJ) Semi-Annual Privacy and Civil Liberties Report, in accordance with Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2012). This report covers the period from April 1, 2015, through September 30, 2015.

Specifically, Section 803 requires federal agency semi-annual reports related to the discharge of certain privacy and civil liberties functions of the agency's Senior Agency Official for Privacy (SAOP). The Department's Chief Privacy and Civil Liberties Officer (CPCLO) in the Office of the Deputy Attorney General serves as the SAOP for the Department, and as the Attorney General's principal advisor on privacy and civil liberties matters. The Department's Section 803 reports include the following information:

- The number and types of privacy reviews undertaken by the CPCLO (including reviews of legislation and testimony, initial privacy assessments, privacy impact assessments, system of records notices, Privacy Act exemption regulations, reviews required by OMB Circular A-130, data breach incidents, Privacy Act amendment appeals);
- The type and description of advice and outreach undertaken by the CPCLO and the Department's Office of Privacy and Civil Liberties (OPCL); and
- The number and nature of privacy complaints received by the CPCLO and OPCL for alleged violations.

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

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

Erika Brown Lee

Chief Privacy and Civil Liberties Officer

U.S. Department of Justice

I. INTRODUCTION

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2014) (hereinafter Section 803), requires designation of a senior official to serve as the Attorney General's principal advisor on privacy and civil liberties matters and imposes reporting requirements of such official on certain activities. The Department's CPCLO in the Office of the Deputy Attorney General serves as the principal advisor to the Attorney General and is supported by the OPCL. Specifically, Section 803 requires periodic reports[1] related to the discharge of certain privacy and civil liberties functions of the Department's CPCLO, including information on: the number and types of privacy reviews undertaken by the CPCLO; the type of advice provided and the response given to such advice; the number and nature of 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 such officer. Many of these functions are discharged, on behalf of the CPCLO, by the Department's OPCL. To provide a standard reportable framework, the Department has coordinated with the Office of Management and Budget (OMB) in order to tailor the report to the missions and functions of the Department's CPCLO.

Accordingly, the Department submits its second Semi-Annual Report for Fiscal Year 2015 on such activities of the Department's CPCLO and OPCL.

II. PRIVACY REVIEWS

The Department conducts privacy reviews of information systems and programs to ensure that privacy issues are identified and analyzed in accordance with federal privacy laws enumerated in controlling authorities such as the Privacy Act of 1974, 5 U.S.C. § 552a (2012), the privacy provisions of the E-Government Act of 2002, 44 U.S.C. § 3501 (note) (2012), as well as federal privacy policies articulated in OMB guidance, including OMB Circular A-130.[2]

A privacy review for purposes of this report encompasses activities that are part of a systematic and repeatable process such as those listed below:

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

Proposed legislation, testimony, and reports are reviewed for any privacy and civil liberties issues by OPCL and the CPCLO.

---

[1] On July 7, 2014, the statute was amended to require semi-annual submissions of the periodic reports rather than quarterly submissions. *See id.* § 2000ee-1(f) (2014), Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014).

[2] *See* OMB Circular No. A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6428 (Feb. 20, 1996), *as amended*, 65 Fed. Reg. 77,677 (Dec. 12, 2000), *available at*: http://www.whitehouse.gov/omb/circulars_a130.

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

An IPA is a privacy compliance tool developed by the Department as a first step to: facilitate the identification of potential privacy issues; assess whether privacy documentation is required; and ultimately ensure the Department's compliance with applicable privacy laws and policies.[3] IPAs are conducted by Department components with coordination and review by OPCL. For purposes of this report, this number represents IPAs that have been reviewed and completed by OPCL.

3. **Privacy Impact Assessment (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.[4] For purposes of this report, this number represents PIAs that have been reviewed, approved and completed by OPCL, and signed by the CPCLO.

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

A SORN is a notice document required by the Privacy Act of 1974 which 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.[5] The SORN is published in the Federal Register. For purposes of this report, this number represents SORNs reviewed and approved by OPCL and the CPCLO that result in a published SORN for which the comment period has exhausted.

5. **Privacy Act Exemption Regulation:**

The Privacy Act provides that agencies may exempt some systems of records from certain provisions of the Act. A Privacy Act exemption regulation is the regulation promulgated by an agency and published in the Federal Register that provides the reasons why a system of records maintained by the agency is exempt from certain provisions of the Act.[6] For purposes of this report, this number represents exemption regulations that have been reviewed and approved by OPCL and the CPCLO that results in a final regulation for which the comment period has exhausted.

---

[3] For further information about the Department's IPA process, *see* http://www.justice.gov/opcl/privacy-compliance-process.

[4] *See* OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A, Section II.A.6 (Sept. 26, 2003), *available at*: http://www.whitehouse.gov/omb/memoranda_m03-22.

[5] *See* 5 U.S.C. § 552a(e)(4).

[6] *See id.* § 552a(j), (k).

6. **Information Collection Notice:**

An information collection notice is a notice to individuals as required by subsection (e)(3) of the Privacy Act.[7] 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 purpose for which the information is intended to be used; the routine uses of the information; and the effects on the individual, if any, of not providing all or any of part of the requested information. For purposes of this report, this number represents reviews of information collection notices conducted by OPCL to ensure that they fully meet the requirements of subsection (e)(3) of the Privacy Act.

7. **OMB Circular A-130:**

OMB Circular A-130 reviews include assessments of the following: SORNs to ensure that they are accurate and up to date; routine uses to ensure that they are still required and compatible with the purpose for which the information was collected; record practices and retention schedules to ensure that they are still appropriate; exemption regulations to ensure that they are still necessary; contracts to ensure that appropriate Federal Acquisition Regulation language is used to bind the contractor to provisions of the Privacy Act; Computer Matching programs to ensure compliance; civil or criminal violations of the Privacy Act to assess concerns; and agency programs for any privacy vulnerabilities.[8] For purposes of this report, this number represents the systems of records that have been reviewed in accordance with the requirements of OMB Circular A-130 by Department components and submitted to OPCL. These reviews are conducted on an annual basis in coordination with the Federal Information Security Management Act (FISMA)[9] reviews. Specific details of such FISMA reviews are submitted through the SAOP portion of the annual FISMA report.

8. **Data Breach or Incident:**

A data breach or incident includes intentional or inadvertent losses of personally identifiable information (PII) in the control of the Department or its contractors who process, store, or possess DOJ PII.[10] For purposes of this report, this number includes data breaches and incidents that have been formally reviewed by the Department's Core Management Team (DOJ's organizational team co-chaired by the CPCLO and the Chief Information Officer, which convenes in the event of a significant data breach involving PII).

---

[7] *See id.* § 552a(e)(3).

[8] *See* OMB Circular No. A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6428 (Feb. 20, 1996), *as amended*, 65 Fed. Reg. 77,677 (Dec. 12, 2000), *available at:* http://www.whitehouse.gov/omb/circulars_a130.

[9] 44 U.S.C. § 3541 *et seq.* (2014).

[10] The Department's Instruction titled "Incident Response Procedures for Data Breach" is *available at* http://www.justice.gov/opcl/breach-procedures.pdf.

9. **Privacy Act Amendment Appeal:**

A Privacy Act amendment appeal is an appeal of an initial agency action regarding a request from an individual to amend their information that is maintained in a Privacy Act system of records.[11] For purposes of this report, this number represents the number of appeals that have been adjudicated and closed by OPCL.

PRIVACY REVIEWS	
Type of Review	**Number of Reviews**
Legislation, testimony, and reports	164
Initial Privacy Assessments	11
Privacy Impact Assessments	3
System of Records Notices – • JUSTCIE/DOJ-017, "Giglio Information System" • JUSTICE/DOJ-016, "Debt Collection Enforcement System"	2
Privacy Act Exemption Regulation – • JUSTCIE/DOJ-017, Giglio Information System	1
Data breach and/or incident reviews	3
(e)(3) Notices – • Justice Management Division – "Phased Retirement Agreement" and "Phased Retirement Mentoring Certification Inventory" Forms • Justice Management Division – "DOJ Rent Management System User Request" Form • Office of Inspector General – "Investigations Data Management System" Public Complaint Online Portal	3
Privacy Act Amendment Appeals	9

III. PRIVACY IMPACT ASSESSMENTS

The Department is committed to ensuring the appropriate protection of privacy and civil liberties in the course of fulfilling its missions. PIAs, which are required by Section 208 of the

[11] *See* 5 U.S.C. § 552a(d)(2), (3).

E-Government Act of 2002, are an important tool to assist the Department in achieving this objective. Below are executive summaries of DOJ's PIAs published for public review for this period, along with a hyperlink to the full text.

- **Justice Management Division (JMD) Justice Communication Center**

JMD's Justice Communication Center (JCS) combines messaging systems used by participating Department components into a single enterprise infrastructure. Specifically, this system provides email, instant messaging, and collaboration services using commercial off-the-shelf software (COTS). Component messaging systems will be migrated into JCS in a phased approach. The purpose of the system is to meet the messaging and collaboration requirements of participating components and to increase standardization of such functionality within the Department. Information about non-DOJ individuals is also captured by this system, even though users of the system are limited to DOJ personnel. For example, if a non-DOJ individual communicates with a DOJ user via email, the email address of the non-DOJ individual, as well as any information transmitted through the email message, will be captured. In addition, in the performance of their duties, DOJ users may transmit information about non-DOJ individuals via this system, such as in the course of civil or criminal litigation. This PIA has been published on OPCL's website and is located at: http://www.justice.gov/file/441446/download.

- **Federal Bureau of Investigation's (FBI) Facial Analysis, Comparison, and Evaluation (FACE) Services Unit**

The Facial Analysis, Comparison, and Evaluation (FACE) Services Unit of the Biometric Services Section, Criminal Justice Information Services (CJIS) Division provides investigative lead support to FBI Field Offices, Operational Divisions, and Legal Attachés by comparing the facial images of persons associated with open assessments and investigations against facial images available in state and federal face recognition systems. In limited instances, the FACE Services Unit provides face recognition support for closed FBI cases (*e.g.*, missing and wanted persons) and may offer face recognition support to federal partners.

In its support of FBI agents and analysts, the FACE Services Unit accepts unclassified photographs of subjects of, and persons relevant to, open FBI assessments and investigations. These photographs are called "probe photos." The FACE Services Unit only accepts probe photos that have been collected pursuant to applicable legal authorities as part of an authorized FBI investigation, and in a future expansion of the program, other federal agency investigations. Upon receipt of a probe photo, the FACE Services Unit uses face recognition software to compare the probe photo against photos contained within government systems, such as FBI databases (*e.g.*, FBI's Next Generation Identification), other federal databases (e.g., Department of State's Visa Photo File, Department of Defense's Automated Biometric Identification System), and state photo repositories (*e.g.*, select state Departments of Motor Vehicles). By using face recognition technology to search probe photos for matching candidate photos, the FACE Services Unit provides unique and specialized value to the FBI's mission to fight crime

and terrorism. In many instances, face recognition results in information that is not available with any other investigative method. This PIA will be made available here: https://www.fbi.gov/foia/privacy-impact-assessments.

- **FBI's Next Generation Identification (NGI) Interstate Photo System (IPS)**

The Next Generation Identification (NGI) system is a replacement for the FBI's Integrated Automated Fingerprint Identification System (IAFIS). The FBI's CJIS Division, which operated and maintained IAFIS, continues to advance biometric identification services with NGI's new functionalities and improvements to existing capabilities. One of NGI's updated services is the Interstate Photo System (IPS). IPS is a face recognition service that allows law enforcement agencies to search photographs of criminals to assist with investigative leads. NGI and IPS are expected to significantly enhance the speed and accuracy of law enforcement identifications, while sufficiently protecting privacy and civil liberties. This PIA will be made available here: https://www.fbi.gov/foia/privacy-impact-assessments.

IV. SYSTEM OF RECORDS NOTICES AND EXEMPTION REGULATION

During this reporting period, one modification to an existing SORN[12] and one new SORN with accompanying exemption regulation went into effect.. First, the Department modified SORN JUSTICE/DOJ-016 titled, "Debt Collection Enforcement System," on March 19, 2015 (80 Fed. Reg. 14407). The Department modified DOJ-016 by adding a new routine use which allows information from the Debt Collection Enforcement System to be disclosed to Federal or state agencies for the purpose of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state in a state-administered, federally funded program. This transfer of information is authorized pursuant to the following authorities: Improper Payments Elimination and Recovery Act of 2010, as amended by the Improper Payments Elimination and Recovery Improvement Act of 2012; Executive Order 13520 (dated November 20, 2009); and Presidential Memorandum—Enhancing Payment Accuracy Through a "Do Not Pay List" (dated June 18, 2010). These authorities require agencies to review existing databases known collectively as the "Do Not Pay List" before the release of any Federal funds. The purpose of the "Do Not Pay List" is to help prevent, reduce, and stop improper payments from being made, and to identify and mitigate fraud, waste, and abuse. This modification is available at: http://www.gpo.gov/fdsys/pkg/FR-2015-03-19/pdf/2015-06335.pdf.

Second, the Department published a new SORN titled, "Department of Justice, Giglio Information Files", JUSTICE/ DOJ-017 (79 Fed. Reg. 28774), on March 19, 2015. This system

[12] A system of records is defined by the Privacy Act of 1974 as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5). Agencies are required to publish in the Federal Register notice of any new use or intended use of the information in the system of record.

of records contains potential witness impeachment information, including records of disciplinary actions. Potential impeachment information has been generally defined as impeaching information which is material to the defense of a federal criminal prosecution. It also includes information that either casts substantial doubt upon the accuracy of any evidence, including witness testimony, the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence.

The purpose of this system of records is to ensure that the Department's prosecutors and investigative agencies receive sufficient information to meet their obligations under *Giglio* v. *United States,* 405 U.S. 150 (1972). This system of records enables the Department's prosecuting offices and investigative agencies to collect, maintain, and disclose records of potential impeachment information that is material to the defense of federal criminal prosecutions. The new SORN is available at: http://www.justice.gov/file/438541/download. In conjunction with the SORN, the Department amended its Privacy Act regulations applicable to the SORN on June 15, 2015 (80 Fed. Reg. 34051-02) by amending 28 C.F.R. 16.81 to remove and reserve paragraphs (g) and (h), and add 28 C.F.R. 16.136 to subpart E.

V. ADVICE AND OUTREACH

Formal advice encompasses the issuance of formal written policies, procedures, guidance, or interpretations of privacy requirements for circumstances or business processes. This advice has been drafted or authorized by the CPCLO and approved as official agency policy by Department leadership to respond to issues or concerns regarding safeguards for privacy and civil liberties. Examples of formal advice and responses to advice provided may include issuance of regulations, orders, guidance, agreements, or training.

As part of the Department's Continuous Monitoring Working Group's monthly meeting in July, a group spearheaded by the Office of the Chief Information Officer, OPCL staff trained information technology (IT) system managers on implementing Appendix J, *Privacy Control Catalog*, of the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* To assist Department components in implementing privacy-enhancing controls into their IT systems, OPCL recently developed tailored resources and guidance for the Department to adopt the privacy controls found in Appendix J. These controls will help ensure that each Department IT system has in place the appropriate administrative, technical, and physical safeguards to protect and ensure the proper handling of PII.

Also, in an effort to enhance the Department's privacy compliance process, OPCL revised its privacy compliance documentation, including the Department's IPA and PIA templates, and introduced a new Administrative PIA template. Also, the CPCLO updated the Department's PIA Guidance. These updated compliance documents are available here: http://www.justice.gov/opcl/privacy-compliance-process. In addition, to increase transparency and better educate the public on the work of the CPCLO and OPCL, changes were made to OPCL's website to include a "Frequently Asked Questions" section that details OPCL's mission, structure, and statutory and administrative authorities. Available here: http://www.justice.gov/opcl/faq.

Further, in July, OPCL released the 2015 edition of its legal treatise on the Privacy Act of 1974 (5 U.S.C § 552a (2012)), *Overview of The Privacy Act of 1974*. This legal treatise provides reference to, and legal analysis of, court decisions discussing the Privacy Act, including its disclosure prohibitions, access and amendment obligations, and agency recordkeeping requirements. *Overview of the Privacy Act of 1974* is viewed as the leading Privacy Act resource for the federal government. This treatise is available to the public on its website, available here: http://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

In August, a joint memorandum was issued from the CPCLO and the Department's Chief Information Officer (CIO) reminding all Department employees of the privacy protections that apply to PII maintained in the Department's systems. Department employees were also reminded of their continuing obligations related to the safeguarding of sensitive PII, including their responsibilities to minimize the use of Social Security Numbers (SSNs), and when using SSNs is absolutely necessary, to redact or mask the data to the extent feasible. The CPCLO also worked with Department leadership in addressing the effect of the OPM data breach incident on the Department. [13]

Finally, the CPCLO and OPCL have also continued to engage stakeholders in the privacy community. They have conducted outreach to the privacy advocacy community and participated in a number of speaking engagements to promote transparency of the Department's policies, initiatives, and oversight with respect to the protection of privacy and civil liberties. The following activities highlight some of the CPCLO and OPCL's efforts:

- The CPCLO and OPCL continued to meet with the European Delegation regarding E.U.-U.S. Data Protection and Privacy Agreement (DPPA) negotiations.
- The CPCLO and OPCL have been participating in meetings with the White House, the Privacy and Civil Liberties Oversight Board (PCLOB), and other federal agencies to discuss ways to improve the Department's privacy and civil liberties reports, including the privacy and cybersecurity assessment required by Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. Discussions on improving such reports are still ongoing.
- The CPCLO and OPCL have also worked with the PCLOB and OMB to address privacy concerns, as well as ways to improve agency outreach. Moreover, the CPCLO and OPCL have met with other federal agencies to improve inter-agency coordination, and to

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

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

- The CPCLO also submitted to the White House a description of the conferences and in-person meetings provided by the Department in 2014 in order to enhance collaboration and information sharing about privacy best practices among state and local law enforcement agencies receiving federal grants. This privacy outreach is ongoing, and occurs regularly throughout the country.
- On June 9, 2015, the CPCLO participated in an International Association of Privacy Professionals (IAPP) event, titled "Privacy: An Equal Playing Field for Women and Men". This panel discussed leading women in privacy in this emerging profession, where success is based on experience and merit.
- On July 20, 2015, OPCL met with civil society representatives on the National Action Plan (NAP) regarding surveillance activities.
- On July 23, 2015, the CPCLO attended a meeting with other Federal Government Chief Privacy Officers hosted by the PCLOB.
- On August 12, 2015, the CPCLO presented on a panel entitled "A facilitated dialogue concerning the pros and cons of non-public safety UAS operations and their impact on privacy" as part of the "The National Institute of Justice's Unmanned Aircraft Systems Expert Convening" event.
- On September 11, 2015, the CPCLO participated in a Policymaker Roundtable hosted by The Privacy Salon, and participated on a panel discussing "Big Data and the Internet of Things."

VI. COMPLAINTS

A privacy complaint encompasses a written allegation (excluding complaints filed in litigation against the Department) concerning a violation of privacy protections in the administration of the programs and operations of the Department that is submitted to or through the CPCLO and/or OPCL. Complaints directly received by components without notice to the CPCLO and/or OPCL are handled by components and are not counted for purposes of this report. Privacy complaints are separated into three categories:

1. Process and procedural issues (such as appropriate consent, collection, and/or notice);
2. Redress issues (such as misidentification or correction of PII, which are outside of the Privacy Act amendment process); and
3. Operational issues (inquiries regarding general privacy, including Privacy Act matters).

A civil liberties complaint encompasses a written allegation (excluding complaints filed in litigation against the Department) for a problem with or violation of civil liberties safeguards

concerning the handling of personal information by the Department in the administration of Department programs and operations that is submitted to or through the CPCLO and/or OPCL.

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

PRIVACY AND/OR CIVIL LIBERTIES COMPLAINTS[14]				
Type of Complaint	**Number of Complaints**	**Disposition of Complaint**		
		Closed-Responsive Action Taken	**Referred to Office of Inspector General**	**Referred to another Component or Agency for review**
Process and Procedure	1[15]	1	0	0
Redress	0	0	0	0
Operational	0	0	0	0
Civil Liberties Complaints	0	0	0	0
Total	1			

[14] For the Second Semi-Annual Report for Fiscal Year 2015, OPCL received 281 inquiries in the form of phone calls, emails, or letters from members of the public, non-federal entities, and within the Department. 280 of these inquiries did not qualify as a privacy and/or civil liberty complaint because the matters raised in those inquiries either fell outside the purview of the Office (e.g., the complaints were against private entities or other non-DOJ entities) or did not raise issues concerning privacy and/or civil liberties matters.

[15] After a thorough review, OPCL determined that one of the inquiries received qualified as a privacy and/or civil liberty complaint against the Department, which involved the interpretation of a Department memorandum regarding the use of PII.