U.S. Department of Justice

THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

2008 ANNUAL REPORT

SEPTEMBER 2008

TABLE OF CONTENTS

I. PRIVACY AND CIVIL LIBERTIES ACTIVITIES

A. NATIONAL SECURITY

This year, the Acting Chief Privacy and Civil Liberties Officer (CPCLO) worked to build out further the oversight regime to ensure that the Department of Justice and its components conduct national security investigations with due consideration of the privacy and civil liberties of individuals.

The Acting CPCLO instructed OPCL, through its Senior Counsel for National Security to work with different components of the Department to provide appropriate counsel concerning privacy and civil liberties safeguards for national security activities.

1. National Security Reviews ("NSRs")

a. Onsite Reviews

In the past, OPCL worked with OIPR and the FBI National Security Law Branch (NSLB) to examine FBI policies and procedures to ensure that appropriate protections and safeguards concerning U.S. person information were in place, taking into consideration the need of the FBI to acquire and share national security-related information. Additionally, beginning in June 2007, OPCL participated in onsite reviews conducted at selected FBI field offices throughout the country. A member of the OPCL staff, including, at times, the Acting CPCLO, participated in nine of the fifteen trips. During the first few trips, OPCL worked with OIPR and NSLB to determine the best means for assessing whether FBI agents routinely complied with the requirements of the NSL statutes and the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003) (NSIGs), or if any systemic compliance problems existed.

During the NSRs, the OPCL representative worked with review teams of NSLB and OIPR attorneys to analyze the information in selected national security investigative files and consider the privacy or civil liberties implications of certain procedural or statutory violations. The review process generally included an examination of whether FBI agents had the proper predication for

opening investigations; documented its collection of personally identifiable information; obtained the necessary authorizations for opening cases, closing cases and gathering information; applied the statutory requirements of the NSL provisions; and complied with the Attorney General Guidelines. OPCL, in particular, began to look at the internal mechanisms associated with information collected in the course of national security investigations to ensure the fair and equitable application of appropriate privacy and civil liberties safeguards to the collection, use, maintenance and dissemination of personally identifiable information handled in the course of a national security investigation. Depending on the size of the office and the number of national security investigations, the OPCL representative participated in each review for one to three days.

b. Creation of the NSD Office of Intelligence

In early 2008, the National Security Division announced the formal launch of the Office of Intelligence, which included three new sections dedicated to the NSD's three primary intelligence related functions – operations, oversight and litigation. These sections represent some new functionality for the Department as well as existing responsibilities that were formerly done through the Department's Office of Intelligence Policy and Review (OIPR).

Since the 9/11 terrorist attacks, OIPR had grown dramatically because of the steady increase in effort to oversee the increased national security activities of the Department. The creation of NSD in September 2006 brought OIPR under the umbrella of NSD and, because of the increased workload, presented an opportunity to review the structure and expanding mission of OIPR. Based on this review, the NSD decided to modify the organization of OIPR to meet the needs of a multi-faceted intelligence mission and developed the Office of Intelligence.

c. Current Process

By December 2007, it was determined that the process for assessing each field office's compliance with the then existing Attorney General Guidelines for National Security Investigations and the NSL statutory requirements had been

fine-tuned by the attorneys of OIPR and that onsite participation by OPCL was no longer necessary. As a result, the Acting CPCLO concluded that for the NSRs planned for calendar year 2008, OPCL's involvement in the NSR process should take place in the form of a briefing and review after each NSR trip was completed.

The process for OPCL participation is as follows: Approximately two weeks after the conclusion of an NSR, OPCL receives the draft case summaries prepared by NSD's Oversight Section (as successor to OIPR's oversight functions) that describe the attorneys' summary of findings from each of the national security investigation files reviewed during the NSR. Shortly thereafter, an OPCL representative meets with the lead NSD attorney responsible for managing the NSR for a post-review evaluation that includes a discussion of specific violations of policy or NSL statutes and an evaluation of the overall responsiveness of the FBI field office leadership in addressing any such violations. Significant privacy or civil liberties concerns raised by NSD are immediately directed to the attention of the Chief Privacy and Civil Liberties Officer for further consideration. Additionally, NSD has noted that the attorney preparing each NSR trip report will reference that OPCL has been consulted and will copy the Chief Privacy and Civil Liberties Officer on each of its final trip reports.

In this process, OPCL will continue to assist the Department in developing integrated policies and procedures that robustly promote privacy and civil liberties while at the same time enhance the work done by the FBI to identify threats and act upon them properly. Specifically, OPCL worked with NSD to add to NSR forms questions concerning the audit of closed 315 investigations to insure that FBI considers whether names should be removed from Terrorist Screening Database (TSDB).

2. National Security Letters

In March 2007, the Inspector General issued his initial report, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*. As part of that report, the Inspector General identified areas in the FBI's compliance mechanisms that required improvement. In light of this report, the then CPCLO

convened a working group to evaluate how NSL-derived information is used, stored, and disseminated. The NSL Working Group originally was chaired by the Chief Privacy and Civil Liberties Officer of the Department of Justice (DOJ) and the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (ODNI). It also included representatives from the National Security Division (NSD), Office of Legal Policy (OLP), the FBI Office of General Counsel (including the FBI Chief Privacy and Civil Liberties Officer), and the ODNI Office of General Counsel.

During 2007, the National Security Letter Working Group (Working Group) conducted initial research on the privacy issues associated with the FBI's use of NSLs and reviewed proposed minimization procedures that the FBI drafted for NSL-derived records. The Working Group prepared a recommendation memorandum to accompany the proposed minimization procedures and provided these materials to the Office of the Attorney General in September 2007. Due to the transition of the Attorney General, the recommendation memorandum was not signed by the Attorney General and was subsequently withdrawn for further consideration. The Working Group recognized the need for further consideration as a result of NSL-related concerns raised by, among others, independent privacy advocates. Those advocates were given an opportunity to discuss and comment on the proposed minimization procedures at a meeting called by the FBI General Counsel with the Acting CPCLO, FBI CPCLO, and the ODNI Deputy Civil Liberties Protection Officer.

Additionally, the Department's Inspector General referenced the Working Group's draft recommendation memorandum in his second NSL report, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, which was published in March 2008. Included in this report was a review of the existing work done by the Working Group and a recommendation for the Working Group to pursue further any privacy and civil liberties concerns that might be raised by the use, storage and dissemination of information obtained pursuant to NSLs.

In meeting to discuss the report in its draft form, the Working Group agreed with the Inspector General of the need to provide further guidance and

explanation for the FBI's proposed minimization procedures. It also saw value in documenting the research and analysis completed previously by the working group. In recognizing that the main focus of the effort would be on the internal development of policy that will impact DOJ and FBI operations and procedures, the ODNI CLPO took on a consultative role and the main research and policy development was done by DOJ and FBI.

In early 2008, the Working Group began field research to understand how FBI agents and analysts have applied the existing and new processes to safeguard privacy and civil liberties. The Working Group noted that both reports of the Inspector General on the use of NSLs acknowledged that investigators did not find specific acts that demonstrated deliberate or intentional misuse. Therefore, the Working Group believed that by examining existing procedures and practices, detailed procedures could be developed to cover any gaps and ensure appropriate implementation of the NSL authorities.

The Working Group met with analysts and agents in several field offices who use and manage all kinds of NSL-derived information. The Working Group met with representatives associated with the FBI's Telephone Applications system, the database into which the FBI enters telephone and subscriber related NSL-derived records. The Working Group examined the entire process of collecting, using, and managing NSL-derived information, from the initial collection from the responding party to ensure alignment with the NSL request, through to the access of information by agents.

The Working Group also met with financial analysts to understand better how the FBI processes information collected from a financial records NSL. As with all collections of NSL-derived information, the first step was for the FBI, either through the case agent or associated analyst, to ensure that the records received were responsive to the NSL request sent. If not, steps were followed to deal appropriately with the information to prevent unnecessary intrusions into an individual's privacy.

Additionally, the Working Group met with case agents and other personnel in order to understand better how information obtained through an NSL is handled upon receipt. The Working Group observed how agents

determined whether the information was responsive and how agents decided what information to disseminate. The Working Group observed that agents uploaded or disseminated only that information they determined might provide value to the investigation.

The Working Group also met with information technology personnel regarding the capabilities of the various databases to which NSL-derived information is uploaded. From these meetings, the Working Group determined areas where existing technology already serves to protect privacy interest and areas where technology could be utilized to enhance such interests.

From these observations, the Working Group began to formulate recommendations regarding the need, the utility, and the feasibility for additional policy and/or technology measures to protect privacy and civil liberty interests in the processing, use, and dissemination of NSL-derived information by the FBI. Specifically, the Working Group reviewed new detailed minimization procedures and provided guidance on improvements to FBI systems to safeguard privacy and civil liberties. The Working Group is drafting a memorandum for the Deputy Attorney General on these recommendations.

3. *Attorney General Guidelines*

The Attorney General, as part of his many duties, is entrusted with regulating federal law enforcement activities to ensure appropriate and legal actions are taken within the context of the Department's law enforcement mission and duties. To this end, the Attorney General issues guidelines for the FBI's activities. The FBI's current responsibilities require it to be both an agency that effectively detects, investigates, and prevents crimes and an agency that effectively protects the national security and collects and analyzes intelligence. Criminal law enforcement and national security have always been central to the FBI's functions, but the national security and intelligence aspects of its mission have increased in scope and importance since the September 11, 2001, terrorist attacks.

On September 29, 2008, the Attorney General issued new guidelines -- the Attorney General's Guidelines for Domestic FBI Operations -- which represent the culmination of the historical evolution of the FBI and the policies governing

its domestic operations in the period following the terrorist attacks. The new Guidelines reflect decisions and directives of the President and the Attorney General, inquiries and enactments of Congress, and the conclusions of national commissions, which recognized that the FBI's functions needed to be expanded and better integrated to meet contemporary realities. The critical measures directed or endorsed for this purpose have included improving coordination between criminal justice and national security activities, enhancing the FBI's intelligence gathering inside the United States, and completing the elimination of the old "wall" between foreign intelligence and domestic law enforcement, while recognizing at the same time that these tasks must be accomplished without sacrificing privacy and civil liberties and with respect for the rule of law.

To realize these objectives, the FBI has reorganized and reoriented its programs and missions, and the guidelines issued by the Attorney General for FBI operations have been extensively revised over the past several years. The completion of this process for the FBI's domestic activities involved work by the Department of Justice in the course of 2007 and 2008 to revise and consolidate the principal directives of the Attorney General governing the FBI's conduct of criminal investigations, national security investigations, and foreign intelligence collection. The new Guidelines issued in September 2008 integrate and harmonize standards to provide the FBI, as well as other affected Department components, with clearer, more consistent, and more accessible guidance in a single publicly available document that serves as the basic body of rules for the FBI's domestic operations.

The new Guidelines generally harmonize investigative standards and procedures, recognizing that responding to threats to the national security, including international terrorism and espionage, is likely to crosscut the FBI's authorities to investigate federal crimes, to protect the national security, and to collect foreign intelligence, and that there should not be arbitrary differences in applicable standards and procedures depending merely on how an activity is labeled. The new Guidelines also incorporate more comprehensive and adequate authorizations for the FBI to engage in intelligence analysis and planning, and to draw on lawful sources of information in doing so.

In addition, the new guidelines incorporate extensive oversight measures that involve many Department of Justice and FBI components in ensuring that all activities are lawful, appropriate, and ethical as well as effective.

The Office of Privacy and Civil Liberties participated in the review and drafting process of these new Guidelines, especially concerning the development of processes to ensure oversight and appropriate authorizations for activities surrounding the domestic operations of the FBI. This included a full examination of the Attorney General Guidelines in relation to the Privacy Act of 1974, especially with regard to Section 552a(e)(7) of Title 5 U.S.C., which provides that federal agencies shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

4. *Other Activities*

In addition to the matters discussed previously, OPCL met with members of NSD's Office of Intelligence Oversight Section to discuss the current NSD semi-annual audit of FBI Intelligence Oversight Board (IOB) violations and to set up procedures for working with the Chief Privacy and Civil Liberties Officer to obtain information about significant IOB violations in a timely and efficient manner.

OPCL worked with members of the Intelligence Community to provide legal review of requirements under the Privacy Act of 1974 and the operation of exemptions under the Privacy Act.

As a specific organization dealing with terrorism within the Department of Justice, OPCL worked with the Terrorist Screening Center (TSC) on a number issues to assist TSC in implementing appropriate and necessary protections for privacy associated with the collection, use, maintenance, and dissemination of personally identifiable information. In relation to national security investigation activities, OPCL worked with TSC and NSD to edit the form FBI uses to contact TSC about changes to information it handles to ensure that individuals' names are being removed when necessary so that redress procedures work correctly. Additionally, OPCL worked with TSC to follow up on a matter to consider

creation of uniform procedures for working with smaller government users of the TSDB that would ensure appropriate privacy protections.

5. Intelligence Community Coordination

Throughout these activities, the Acting CPCLO coordinated with the Civil Liberties Protection Officer for the Office of the Director of National Intelligence to ensure that the Department's activities designed to protect privacy and civil liberties met or exceeded standards being applied throughout the Intelligence Community. The Acting Chief Privacy and Civil Liberties Officer met regularly with the ODNI CLPO to discuss issues associated with the protection of privacy and civil liberties in the collection, use, maintenance, and dissemination of intelligence information.

B. INFORMATION SHARING

The Information Sharing Environment (ISE) Privacy Guidelines provide the framework for enabling information sharing while protecting privacy and other legal rights. To achieve this, the ISE Privacy Guidelines strike a balance between consistency and customization, substance and procedure, oversight and flexibility. These guidelines build upon existing resources within executive agencies and departments for implementation.

At the end of 2007, through the Program Manager for the Information Sharing Environment (PM_ISE), the ISE Privacy Guidelines Committee (ISE/PGC) co-chairs, the DOJ Acting CPCLO and the ODNI CLPO, released the ISE Privacy and Civil Liberties Implementation Guide to provide agencies with further guidance on the practical application of implementing the ISE Privacy Guidelines. A core tenant of the ISE is protecting privacy and civil liberties. The ISE Privacy Guidelines provide the framework for enabling information sharing while providing protections for information privacy and other legal rights. Balancing the need to share terrorism information with the need to remain vigilant about protecting Americans' privacy and civil liberties is challenging, yet vital to our way of life. Meeting the dual imperatives of protecting privacy and sharing information is at the core of the approach taken in the ISE. The ISE/PGC developed the ISE Privacy and Civil Liberties Implementation Guide

("Implementation Guide") to ensure uniform and deliberate application of needed safeguards in the development and use of the ISE.

Following the development of the Implementation Guide, the ISE/PGC created the ISE Privacy and Civil Liberties Implementation Manual ("the Manual"), which includes more detailed assistance and guidance to help agencies implement the ISE Privacy Guidelines.

Although implementation of the ISE Privacy Guidelines is mandatory, the co-chairs recognized that the manner in which each agency implements the ISE Privacy Guidelines may vary depending on existing agency practices, processes, and preferences. The Implementation Guide is not meant to be prescriptive, but rather to provide general guidance that can be applied in each agency's unique environment as it implements the ISE Privacy Guidelines. To be effective, the Implementation Guide addresses the realities of the many different environments in which it will be applied.

The framework in the Privacy Guidelines provides for

- identifying information that is subject to privacy protection,
- assessing applicable privacy rules,
- implementing appropriate protections, and
- ensuring compliance.

As each agency considers how to approach the implementation of the ISE Privacy Guidelines, each agency may use its existing processes or incorporate the process suggested in the Implementation Guide, in whole or in part. Further, the Manual is designed to be a "one-stop shopping" for resources an agency may need to implement Guideline 5.

Additionally, OPCL contributed substantially to other ISE/PM working groups established to handle ISE issues. These included the working group on Controlled Unclassified Information (otherwise known as Sensitive But Unclassified information) and the working group devoted to developing policy and procedures for Suspicious Activity Reporting.

C. INTERNATIONAL ACTIVITIES

The Office of Privacy and Civil Liberties continued to engage with the Department's international partners on privacy and civil liberties issues to provide a framework for privacy protections supporting the Department's already strong national security and law enforcement ties in the international arena.

1. *High Level Contact Group*

The Office of Privacy and Civil Liberties continued its privacy leadership by exercising leadership in the High Level Contact Group. In the framework of the EU-U.S. Justice and Home Affairs Ministerial Troika on November 6, 2006, it was decided to establish an informal high level advisory group to start discussions on privacy and personal data protection in the context of the exchange of information for law enforcement purposes as part of a wider reflection between the U.S. and the EU on how best to prevent and fight terrorism and serious transnational crime. This group is composed of senior officials representing the U.S. Attorney General, the Secretaries of the U.S. Departments of State and Homeland Security, the European Commission, and the European Council Presidency (supported by the Council Secretariat). The goal of the HLCG was to explore ways that would enable the EU and the U.S. to work more closely and efficiently together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed. This group's identification of the fundamentals or "common principles" of an effective regime for privacy and personal data protection was to be the first step towards that goal.

This goal builds on recent trans-Atlantic events in the Justice and Home Affairs area, which have included the conclusion of international agreements between the United States and the European Union governing Extradition and Mutual Legal Assistance and agreements governing personal data exchange between the United States and Europol and Eurojust.

At its third meeting on November 2, 2007 in Washington during the EU Presidency of Portugal, the HLCG concluded that good progress had been made and decided that the group should continue the exploratory talks with the aim of

trying to find as much common ground as possible. At the start of the Slovenian Presidency of the EU in January 2008, the group met in Brussels for two days of intensive negotiation focused on core data protection and privacy principles. At this meeting, the group was able to develop the foundation for the final twelve (12) common privacy principles. Work continued throughout the early part of 2008, with the group meeting via Digital Video Conference at number of times.

During the U.S.-EU Justice and Home Affairs Ministerial Troika in Brdo, Slovenia on March 12-13, 2008, the Ministers expressed a clear common will to continue working on the common principles, to identify options for future work, and to report on any outstanding issues. The Ministers also said that such reporting could take place in the context of the U.S.-EU Summit in June 2008.

U.S. and EU Ministers responsible for Justice and Home Affairs directed the HLCG to explore the commonalities of the laws, policies, and practices of each side and the potential efficiencies that could result from the development of common privacy principles. At the close of May 2008 prior to the June Summit, the HLCG delivered its "final report" on the twelve (12) common privacy principles for the protection of personal data and privacy.

These common principles define the following privacy and personal data protection requirements:

1. Purpose Specification/Purpose Limitation;
2. Integrity/Data Quality;
3. Relevant and Necessary/Proportionality;
4. Information Security;
5. Special Categories of Personal Information (sensitive data);
6. Accountability;
7. Independent and Effective Oversight;
8. Individual Access and Rectification;
9. Transparency and Notice;
10. Redress;

11. Automated Individual Decisions;

12. Restrictions on Onward Transfers to Third Countries.

Both sides agreed that an international agreement binding on both the U.S. and the EU to apply the agreed twelve (12) common principles in transatlantic data transfers is the preferred option in which both sides recognized the effectiveness of each other's privacy and data protection systems for the areas covered by these principles while providing the greater level of legal security and certainty.

In addition, both sides also agreed that the conclusion of a binding international agreement incorporating the twelve (12) common principles should provide every person in the EU and the U.S. with the greatest assurance that her or his personal data would be protected consistently and evenly at a high standard in both jurisdictions. Work is continuing on the framework for the negotiations for this agreement, but the benefits of concluding on the twelve (12) common principles have already been recognized in other data exchange negotiations and discussions with foreign partners.

2. *Preventing and Combating Serious Crime Agreements*

The Acting CPCLO lead the U.S. delegation to negotiate agreements to share information associated with criminal justice activities. In July 2008, the Department working with the Departments of State (State) and Homeland Security (DHS) began negotiations with a number of foreign government partners to enhance criminal law enforcement cooperation through the establishment of fingerprint matching processes, follow up procedures to provide additional information, and other information sharing procedures, entitled the "Preventing and Combating Serious Crime Agreement."

This agreement was based on the text of the agreement between the United States and Germany, done for similar purposes and modeled after the European convention known as the Prüm Treaty, as a starting point.

Prior to the start of the negotiations, the Acting CPCLO detailed to the interagency partners the specific legal restrictions for lawful use of criminal history record information (CHRI) making clear that CHRI may only be accessed

1) for a criminal justice purpose (as defined by 28 CFR § 20.3(b)) and 2) when fingerprints are collected from the individual for whom information is sought. Additionally, in order to ensure appropriate implementation at the border to prevent routine criminal background checks as part of the country admission process for travelers, the agreement requires that searches for CHRI shall only be done when border officials select an individual for secondary inspection because of a suspicion of criminal activity. This prevents the searching of CHRI available, for the U.S., through the FBI's Interstate Identification Index (III) and, for other countries, through their criminal information repository, for border screening purposes, because these processes were not authorized by law since they are for a non-criminal justice purpose.

Agreements were concluded with a number of countries, including the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Slovakia, and South Korea.

D. PRIVACY SENSITIVE TECHNOLOGIES

1. Biometrics

The Office of Privacy and Civil Liberties continued to promote the development of appropriate safeguards for privacy and civil liberties associated with the government's use and implementation of biometrics technology. OPCL remains co-chair of the Social, Legal, Privacy Issues Working Group of the Biometrics Subcommittee of the National Science and Technology Council.

Additionally, OPCL participated in the drafting process of the National Security Presidential Directive Number 59, Biometrics for Identification and Screening to Enhance National Security, to ensure the incorporation of protections for privacy and civil liberties into the operational processes to be developed under the Directive. Additionally, OPCL provided input into the drafting of the Action Plan required by the Directive to be completed by the Attorney General.

2. *Data Mining*

The Office of Privacy and Civil Liberties participated in the drafting and reviewed the Department's report concerning the Department's Data Mining activities as defined under Section 804 of the Implementing the Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53. Section 804 requires the heads of all agencies in the Federal government to submit, within 180 days of enactment of the Act and annually thereafter, a report regarding the organization and operations of every initiative engaged in "data mining," as defined in the statute.

For each such initiative, the head of the agency must provide: (1) a description of the data mining activity and its goals; (2) a description of the data mining technology that is being and how it is determined whether a particular pattern or anomaly is indicative of terrorist or criminal activity; (3) a description of the data sources that are being used; (4) an assessment of the efficacy or likely efficacy of the data milling activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity; (5) an privacy and civil liberties impact assessment of the data mining activity examining what actions that are being taken concerning appropriate protections of privacy and civil liberties; (6) a list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity; and (7) a description of the policies to protect the privacy and due process rights of individuals, including redress and integrity processes to ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, in order to guard against any harmful consequences of potential inaccuracies.

Data mining initiatives that analyze lawfully acquired information, including those Departmental activities in the report, provide important advanced analytical tools to support traditional investigative techniques. Nevertheless, such initiatives must be undertaken with deep respect for the privacy and civil liberties of Americans. The report demonstrated that all of the data mining initiatives undertaken by the Department meet both of these goals.

With regards to the protection of privacy and civil liberties, all of the initiatives are subject to existing processes and procedures to protect privacy and civil liberties, including those federal statutes and internal Department policies and procedures designed to mitigate potential privacy concerns. For example, Privacy Impact Assessments ("PIAs") completed by Department components pursuant to the E-Government Act of 2002 address the issue of the existing authority for the collection and advanced analysis of information. The goal of a PIA is three-fold: (1) to ensure that handling of information conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form via an electronic information system; and (3) to evaluate protections and alternative processes for handling information to mitigate potential privacy risks. OPCL is developing additional inquiries as part of the PIA process to provide greater insight and analysis about possible data mining activities. Once the new PIA guidance is reviewed on a Department-wide basis, these inquires will be incorporated into the standard PIA Template, and PIAs for applicable systems will be updated.

Moreover, the Department has long been subject to, and is diligent in complying with, the Privacy Act of 1974, 5 U.S.C. § 552a. The Privacy Act's requirements generally apply to records that identify and are about U.S. Citizens and legal permanent resident aliens and that are retrieved from a system by reference to an individual's name or other personal identifier. As a result, any information produced as a result of pattern-based data mining that meets these criteria is subject to the Act's requirements. It should be noted that while the Department, as a law enforcement agency, has exempted certain of its systems from subsections (e)(1) and (e)(5) pursuant to subsection (j)(2) of the Privacy Act, the Department nonetheless recognizes the need for relevant and accurate information in carrying out their law enforcement missions. Furthermore, an exemption cannot be claimed from (e)(4)(A)-(F) or (e)(6), (e)(7), (e)(9) and (e)(10), nor from subsection (b) of the Act, among others, the very core of the Act that prohibits disclosure of Privacy Act information except under certain circumstances.

The report identified and discussed a few specific risks in connection with the impact on privacy and civil liberties associated with data mining initiatives. One privacy risk associated with any pattern-based data mining initiative is whether the pattern-based data mining is undertaken for a legitimate purpose. A second privacy risk relates to the security of the information and how it is retained. In this regard, agencies that administer a pattern-based data mining initiative must ensure that the information is secure and that users utilize the particular tools only for authorized purposes. A third privacy risk relates to the security of information once the analysis has been undertaken. Protections required by FISMA and implemented in Departmental security policies, including strict access controls and audit capabilities, ensure that such data is not accessed by unauthorized users.

The report noted that the Department conducts a PIA for any associated system to evaluate the potential privacy risks noted above of a pattern-based data mining initiative and describe mitigation procedures that have been put in place to counter such potential risks. Further, OPCL is fully engaged in the development and analysis of any PIA on a major information system or national security system done by any component within the Department, providing additional insight into the potential privacy concerns at stake and potential for mitigating those concerns. Additionally, and perhaps most importantly, with regard to several of the Department's data mining initiatives, personal information is not forwarded to FBI investigators unless it is necessary for opening an investigation pursuant to the Attorney General's Guidelines. By minimizing the access to personal information, the risk of a security breach of this data is lessened.

Furthermore, leads generated by pattern-based data mining initiatives are not automatically accepted and acted upon, thus reducing the risk of "false positives." Rather, query results from these initiatives are independently evaluated by highly skilled analysts. The results are then passed along to investigators who also closely review results before taking any investigative action. These results are only used for lead purposes and no action is taken based solely on the analytic products produced by such pattern-based data mining initiatives. Internal Department and FBI procedures, including the

Attorney General Guidelines, set forth the Department's general policy that investigations should be undertaken by non-intrusive means prior to the use of more intrusive investigative means, and whether the aforementioned reviews determine further investigation using more intrusive means is relevant and appropriate.

In this way, no one is labeled a terrorist or a criminal simply because that individual appears in a database or appears as a result of some set of data mining queries. Moreover, the data mining initiatives discussed in this report do not preempt or abrogate other requirements investigators and analysts must satisfy in order to pursue more intrusive techniques. For example, investigators still must have sufficient probable cause in order to obtain a warrant. The Department realizes that there are privacy risks inherent in the use of pattern-based data mining initiatives, as there are with most law enforcement investigative techniques. As with all law enforcement techniques, the Department strives to mitigate such potential privacy risks through compliance with federal statutes and internal policies and regulations. Through such mitigation, the Department's agencies carry out their law enforcement and terrorism prevention missions while protecting the privacy and civil liberties of our nation's citizens.

II. PRIVACY COMPLIANCE OPERATIONS

A. PRIVACY ACT

The Office of Privacy and Civil Liberties continued its role of advising the Attorney General on the appropriate privacy protections relating to the collection, storage, use, disclosure and security of personally identifiable information held by the Department. To accomplish this, OPCL serves as the primary point of counsel for the Department on issues relating to the Privacy Act of 1974 and the application of the fair information principles throughout the Department.

In January 2008, the Attorney General signed an order designated the Chief Privacy and Civil Liberties Officer for the Department as the signing authority for all notices and regulations associated with the Department's

obligations under the Privacy Act of 1974. This order brought the last main privacy compliance component officially under the responsibility of the Office of Privacy and Civil Liberties.

1. *Maintaining "Systems of Records"*

In order to carry out the Department's important and varied law enforcement missions, the Department must handle and maintain a certain amount of information about individuals. The information that the Department maintains about individuals ranges from information within the federal prison system, to information related to cases in litigation, to investigative law enforcement files. The Privacy Act represents the embodiment of a code of fair information principles that governs the collection, use, dissemination, and maintenance of information about individuals that is maintained in "systems of records" by federal agencies. A "system of records" is a group or collection of records under the control of a federal agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

2. *Legal Counsel*

The CPCLO through OPCL oversees the Department's compliance with the Privacy Act of 1974 and plays an active role in ensuring that the Department's law enforcement, litigation, and anti-terrorism missions are carried out in accordance with its provisions.

OPCL provides Privacy Act guidance within the Department, both in response to specific inquiries raised by the components and through training programs, drawing on the expertise in Privacy Act case law and analysis that its staff brought to the Office. OPCL is routinely consulted for Privacy Act guidance in administrative matters, law enforcement initiatives, and litigation. OPCL is also continuing production and publication of the "Overview of the Privacy Act of 1974," a detailed analysis of Privacy Act case law that is heavily relied upon throughout the federal government.

As noted above, to more efficiently coordinate the Department's Privacy Act responsibilities, the Attorney General recently delegated authority respecting departmental systems of records under the Privacy Act to the CPCLO. (Atty.

Gen. Order No. 2940-2008.) Under the CPCLO's authority, OPCL works with the Department's components to promulgate rules to exempt Department of Justice records from provisions of the Privacy Act, to publish Federal Register notices of the existence and character of the Department's systems of records, to publish notices of routine uses, and to furnish reports to Congress and the Office of Management and Budget of proposals to establish or alter systems of records.

OPCL's Privacy Act expertise has also been particularly relied upon in connection with the Department's Law Enforcement Information Sharing Program, in which its staff has served a vital role in ensuring that information sharing initiatives carried out in the Department's effort to enforce the law are made in a manner that is consistent with the law. This has also led to OPCL's participation in various other federal information sharing initiatives in which the Department participates and in which OPCL is likewise relied upon for its Privacy Act expertise.

3. *Statutory Notices*

In addition to the wide-ranging general Privacy Act duties of OPCL, OPCL also assists components in developing appropriate language for the required notices to ensure compliance with the Privacy Act. The System of Records Notice (SORN), provides the public with the essential details about a system of records, including the purpose for its operations, the categories of individuals affected by its operations, the categories of information to be used and collected by the agency, where the agency maintains the information, what means of access and correction are available to the individual, what security measures safeguard the information, and, lastly, although very importantly, with what entities and under what conditions the agency will share the information in the system. OPCL counsel address issues related to both new systems and updates to existing systems to develop the appropriate notice to the public concerning Department of Justice systems of records.

In addition to its extensive work with SORNs, OPCL also provides input in connection with Privacy Act Statements, which are notices provided to the public when the agency collects personally identifiable information. These notices reiterate some of the information found in the SORN, but are designed to

provide an individual with certain information at the time he or she provides the information to the agency. The notices must inform the individual of the authority for the collection of the information and whether disclosure of such information is mandatory or voluntary; the principal purposes for which the information is intended to be used; the circumstances under which the information may be shared outside the agency; and the effects on the individual, if any, of not providing all or any party of the requested information. Additionally, if the collection involves Social Security Numbers, the Privacy Act, under Section 7, requires the agency to inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority the Social Security Number is solicited, and what uses will be made of it.

B. E-GOVERNMENT ACT, FISMA, AND SECTION 803

The Office of Privacy and Civil Liberties serves as the focal point for the privacy protections associated with the development of information technology systems and the handling of electronic personally identifiable information throughout the Department.

OPCL maintains the Department's approval process for Privacy Impact Assessments (PIAs), which is a highly collaborative process that includes working with the Department's Chief Information Officer, the privacy office of the component developing the technology, and the program office or official responsible for the deployment and implementation of the technology. The PIA process permits the Chief Privacy and Civil Liberties Office to have effective oversight of the implementation of appropriate policies and procedures for the protection of privacy and civil liberties, including appropriate training and auditing, to ensure the Department's compliance with privacy-related laws and policies, including Section 208 of the E-Government Act.

1. E-Government Act Activities

As discussed above, conducting a PIA at the Department is a highly collaborative process that incorporates the information technology know-how of the Office of the Chief Information Officer and the privacy compliance expertise of OPCL.

Additionally, OPCL redeveloped the Privacy Threshold Analysis (PTA) template into the Initial Privacy Assessment (IPA) to integrate the Department's E-Government responsibilities with its Privacy Act duties. Furthermore, the IPA will be used to capture the privacy issues associated with "micro" information technology systems. These are systems that would not necessarily be required to comply with the E-Government Act, either for privacy or information security purposes, but ones which the Department handles personally identifiable information. OPCL is currently in the process of updating the IPA template document and will follow with an update to the PIA guidance.

In the past year, OPCL worked with the Office of the Chief Information Officer to enhance further the Computer Security Awareness Training (CSAT) module that each employee or contractor with access to Department information technology resources must complete on an annual basis. This year's update to the training highlighted responsibilities, including those associated with OMB Memorandum M-07-16 (concerning data breach notification processes), Section 803 of the Implementing the Recommendations of the 9/11 Commission Act of 2007 (concerning personally identifiable information ("PII")), and updated the Rules of Behavior provided at the close of the training to emphasize the individual's as well as the Department's responsibility concerning the protection of PII.

2. *FISMA Activities*

OPCL continued to report quarterly in connection with FISMA on privacy issues. These reports review the Departmental processes concerning the handling of personally identifiable information and examine the PIAs and SORNs prepared by the Department. The reports help OPCL confirm the number of IT systems in the Department that handle personally identifiable information, that require PIA and Privacy Act documentation, and for which such documentation has been completed. To aid in the collection of this information, OPCL worked with OCIO to develop the capability within the software application that tracks FISMA compliance to capture relevant privacy information and documentation.

As in the past, the information in the quarterly FISMA privacy reports is also used by OPCL to determine the Department's and components' privacy compliance as measured by the President's Management Agenda scorecard. OPCL determines if a component will receive a passing grade, and if not, will inform the component what it must do to remedy the problem by the next quarter. Furthermore, OPCL also reviews and provides a score for the privacy portion of every Department OMB 300 business case before it is submitted to OMB.

3. *Section 803 Activities*

Following the enactment of the Implementing the Recommendations of the 9/11 Commission Act of 2007, OPCL began to report on a quarterly basis those activities associated with Section 803 of the Act.

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, 121 Stat. 266, 360 (August 3, 2007) imposes enhanced and periodic, but not less than quarterly, reporting requirements for the Department on certain privacy and civil liberties activities. The Chief Privacy and Civil Liberties Officer (CPCLO) for the Department is responsible for submitting these quarterly reports. Furthermore, Section 803 enumerated various privacy and civil liberties requirements for the Department. Likewise, the Department continues to review a wide variety of activities and procedures within the Department to find opportunities to enhance protections of the privacy and civil liberties of individuals.

The Department will report quarterly on its privacy and civil liberties activities on a schedule associated with the FISMA reporting and coordinated the development of this process with the Office of Management and Budget, as well as with a number of other federal agencies identified in the statute. The Department has developed a standard reporting framework and instructions to address Section 803 reporting requirements.

The OPCL submits consolidated reports for the Department, which include all privacy and civil liberties activities including data on the related reviews conducted, reference to the advisory guidance delivered, and information about written complaints received and their processing.

For each section 803 report, a review encompasses activities that are part of a systematic and repeatable process looking at privacy or civil liberties matters enumerated in controlling authorities, such as the Privacy Act of 1974; the Consolidated Appropriations Act of 2005; Office of Management and Budget (OMB) Circular A-130 (Appendix I); and OMB Memorandum M-07-16. Additionally, the report includes notice of the issuance of any formal written policies, procedures, guidance, or interpretations of privacy requirements for circumstances or business processes, which have 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. Lastly, the report incorporates information concerning written informal allegations regarding privacy or civil liberties protections submitted to or through the CPCLO. This will not include any filing of litigation against the Department or Freedom of Information Act/Privacy Act requests made to the Department. For each type of privacy or civil liberties issue reported received by OPCL during each quarter, OPCL will report the number of complaints (1) that the agency was able to assist in resolving; (2) that the agency referred out; and, (3) that the agency was unable to assist in resolving.

III. OUTREACH AND INTERGOVERNMENTAL ACTIVITIES

To further its mission, OPCL conducted numerous outreach activities explaining the impact of its activities on privacy and civil liberties. OPCL interacted with outside organizations, including privacy and civil liberties advocates and organizations. Additionally, OPCL worked with individuals to address issues concerning the impact that Departmental activities had on privacy and civil liberties.

A. PRIVACY LEADERSHIP

In addition to internal interactions, OPCL works with different governmental groups on multiple levels to help build an understanding of the government's responsibility in ensuring the privacy and civil liberties of individuals. This work extends not only to collaborating with other federal agencies, but with international, state and local entities and officials.

1. The Federal CIO Council Privacy Committee

Since its inception in May 2007, the DOJ CPCLO has served as the co-chair with the Administrator of E-Government and Information Technology from the Office of Management and Budget of the Privacy Committee of the Federal CIO Council.

The Privacy Committee serves as the interagency coordination group for Senior Agency Officials for Privacy in the federal government to provide a focal point for the development and harmonization of privacy policy and protections. The Privacy Committee works to promote adherence to the letter and the spirit of laws advancing privacy, including the Privacy Act of 1974 and the E-Government Act of 2002, as well as widely accepted concepts of fair information principles and practices. Additionally, it looks to ensure widely available education and outreach efforts to create a culture of privacy and to enhance the respect for fair information principles across the federal government. These activities of the Privacy Committee help the Senior Agency Officials for Privacy ensure that their agency appropriately minimizes the impact on the individual's privacy, particularly the individual's personal information and dignity, in the design, development, and operation of agency collections of data.

2. High Level Contact Group Experts Panel

As noted above, the Acting CPCLO served as the head of the U.S. delegation of experts designated to work with their EU counterparts to develop common privacy principles.

3. Information Sharing Environment Privacy Guidelines Committee

At the end of 2006, the President approved for issuance and implementation, and the Information Sharing Environment Program Manager (ISE/PM) released to the public, the Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment, also known as the "ISE Privacy Guidelines." Following the issuance of the ISE Privacy Guidelines, the Program Manager for the Information Sharing Environment (PM/ISE) asked the Attorney General and Director of National Intelligence to each designate senior officials to

serve as co-chairs of ISE Privacy Guidelines Committee (ISE/PGC), which, according to the ISE Privacy Guidelines, consists of the ISE Privacy Officials of the departments and agencies comprising the Information Sharing Council (ISC). The Attorney General and Director of National Intelligence designated, respectively, the DOJ CPCLO and ODNI CLPO as co-chairs of the ISE/PGC.

4. Federal Enterprise Architecture Security and Privacy Profile Working Group

The Acting CPCLO served as the lead privacy expert on the Federal Enterprise Architecture Security and Privacy Profile Working Group (FEA SPP WG) with Ron Ross, senior computer scientist and information security researcher at the National Institute of Standards and Technology (NIST), and Scott Bernard, deputy CIO and chief enterprise architect at the Federal Railroad Administration, lead the team examine the development of a scalable and repeatable methodology for addressing information security and data privacy requirements from a business-centric perspective at the enterprise, segment, and solution levels of an agency's enterprise architecture. The FEA-SPP supports the identification and evaluation of security and privacy requirements throughout the architecture using the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and the FEA-SPP Tool both of these support the development and implementation of security and privacy controls using NIST procedures and FEA guidance.

5. Federal Interagency e-Discovery Privacy Working Group

The Acting CPCLO coordinated the development of a working group made of senior agency official who develop or implement policy concerning privacy, data protection, or discovery issues. This working group formulated a response, delivered by the Acting CPCLO, to an inquiry from Dr. Alexander Dix, the Data Protection Supervisor for Berlin, Germany, in Dr. Dix's role as the chair of a working group of the EU Article 29 Working Party looking into issues surrounding the release of new U.S. federal discovery rules and the transnational flow of personally identifiable information.

6. Global Privacy and Information Quality Working Group

The Acting CPCLO participates on the Global Privacy and Information Quality Working Group of the Global Justice Information Sharing Initiative to ensure privacy and civil liberties safeguards become embedded in the framework of information sharing concerning the sharing of law enforcement information.

B. PRIVACY AND CIVIL LIBERTIES COMPLAINTS

The Office of Privacy and Civil Liberties addresses various complaints received concerning privacy and civil liberties in association with the Department's handling of personally identifiable information. As noted above, following the enactment of the Implementing the Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, OPCL implemented the reporting requirements concerning the handling of complaints.

OPCL facilitated general requests for assistance by directing individuals to the appropriate component or program that either held the information sought by the individual or operated the program or system that impacted the individual. To that end, OPCL developed close relationships with different offices throughout the Department and in particular with the Civil Rights Division through OPCL's participation in the bimonthly meetings that Division holds with members of various communities impacted by the Department, government, or law enforcement activities.

C. EVENTS AND TALKS

The Acting Chief Privacy and Civil Liberties Officer spoke at a number of events describing the integration of privacy and civil liberties protections into the mission of the Department. Such events included speaking to the Global Privacy and Information Quality Working Group (GIPIQWG) on Privacy Issues Across Federal Partners and to the American Society of Access Professionals, on security and associated privacy issues from an information technology perspective.

This outreach extended to the international arena. The Acting Chief Privacy and Civil Liberties Officer participated as an observer at the fall 2007 meeting of global privacy and data protection commissioners. Although this

conference has closed sessions for only those commissioners providing oversight over all of their country's activities, including commercial data protection, the Acting Chief Privacy and Civil Liberties Officer was granted observer status to all closed sessions in recognition of OPCL's impact on privacy and civil liberties issues. The international outreach continued with participation at the European Commission Directorate General for Justice, Freedom, and Security; Conference on Data Sharing and Protection in Brussels, Belgium on the Information Sharing Environment Privacy Guidelines.

IV. CONCLUSION

The Office of Privacy and Civil Liberties successfully "operationalized" privacy throughout the Department in the past year both in terms of re-structuring OPCL and the further development of processes, training, and reporting. The Department of Justice stands as a defender of the rights of individuals including the safeguarding of privacy and civil liberties in the handling of personally identifiable information in connection with its operational mission.

The protection of privacy and civil liberties is core to the mission of the Department of Justice. As noted by Attorney General Michael Mukasey in his memorandum covering the release of the new consolidated Attorney General Guidelines, one key objective of the new Guidelines was "[to conduct] all activities ... in a lawful and reasonable manner that respects liberty and privacy." OPCL will continue to move forward together and achieve the Department's mission of protecting and defending the lives and way of life of the people of this Nation.