Privacy Impact Assessment
for the

Innocence Lost Database

11/15/2007

Contact Points
IA [redacted]
Crimes Against Children Unit
Criminal Investigative Division
Federal Bureau of Investigation
[redacted]

b6
b7C

[redacted] Unit Chief
Crimes Against Children Unit
Criminal Investigative Division
Federal Bureau of Investigation
[redacted]

Reviewing Official
David C. Larson
Privacy and Civil Liberties Officer
Office of the General Counsel
Federal Bureau of Investigation

Vance Hitch
Chief Information Officer
Department of Justice
(202) 514-0507

Approving Official
Kenneth Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 252-8878

Introduction

The Federal Bureau of Investigation (FBI) exercises jurisdiction and investigative responsibility pursuant to several federal statutes covering crimes against children, including the White Slave Traffic Act-Sexual Exploitation of Children and White Slave Traffic Act-Domestic Trafficking of Children/Prostitution. To carry out its responsibilities, the Office of Crimes Against Children (CAC) Program was established to: develop a nationwide capacity to provide a rapid and effective investigative response to reported federal crimes involving the victimization of children; reduce the vulnerability of children to acts of sexual exploitation and abuse; and strengthen the capabilities of federal, state and local law enforcement through training programs and investigative assistance. The CAC Program strategy is implemented by using multi-disciplinary and multi-agency resource teams to investigate and prosecute crimes against children that cross legal, geographical and jurisdictional boundaries and by promoting and enhancing interagency sharing of intelligence information. Implementing the CAC Program strategy is the primary mission of the FBI's Crimes Against Children Unit (CACU), which was created to address the significant crime problems that exist with respect to the victimization of children and to provide a focal point for government and public awareness of the FBI's increased jurisdiction in this critical area of law enforcement.

To facilitate the interagency sharing of intelligence information necessary to combat child prostitution, a national child prostitution database is required to record biographical information regarding suspected pimps and victim prostitutes. Such a database is necessary because of the interstate nature of child victimization crimes. Although local law enforcement agencies independently collect and gather intelligence on prostitution activities in their areas, analysis of the crime problem indicates that individuals and organizations involved in this type of crime are highly likely to be implicated in this criminal activity in other cities, states and regions. Because of the enterprise nature of this type of crime, centralizing the intelligence gathered from local law enforcement will facilitate the effective investigation and prosecution of crimes against children that cross legal and geographical jurisdictional boundaries and ultimately help combat the domestic trafficking of children.

A national child prostitution database will act as the central storage medium for information regarding the activities and locations of suspected pimps and victim prostitutes. In addition to being able to search for information on suspected pimps and victim prostitutes, the database will be used to confirm the identity of victim prostitutes and to provide a common communications environment for investigators working/interfacing with the same suspected pimps and victim prostitutes. The national child prostitution database will allow for the national collection of intelligence regarding prostitution and the national analysis of pimp and prostitute networks and activities. Such analysis will allow the CACU to determine trends, patterns and most importantly, develop cases which are national in scope.

Development of this database will ultimately allow for more effective investigations to be initiated, more missing children to be located and more offenders to be prosecuted.

Section 1.0
The System and the Information Collected and Stored within the System.

1.1 What information is to be collected?

Biographical information and intelligence will be collected on suspected pimps, co-conspirators and victims. This information, to the extent it is available, will include:

b7E

1.2 From whom is the information collected?

Information will be collected from local, state and federal law enforcement officers who investigate child prostitution matters and from non-governmental organizations that provide assistance to law enforcement officers. These officers and organizations collect this information from suspected pimps, co-conspirators, witnesses and victims.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

The FBI will utilize this information to collaborate with state and local law enforcement agencies to identify suspected pimps and victims in child prostitution investigations; to identify criminal enterprises and the geographical locations having a high incidence of child prostitution; and to assist law enforcement officers with identifying and recovering child victims.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The FBI is legally authorized to collect this information pursuant to its investigative mission. A listing of the federal statutes pertaining to crimes against children for which the FBI has jurisdiction can be found at www.fbi.gov/hq/cid/cac/federal.htm.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The information is collected from law enforcement agencies at all levels of government that have it as a result of encounters with individuals engaged in child prostitution. A significant portion of the information in this system will identify juveniles. This information is particularly sensitive under federal law (e.g., 18 U.S.C. § 3509 (d)) and the laws of most states that protect the confidentiality of the identities of child victims as well as juvenile perpetrators of crime. Accordingly, under FBI policy, it should be afforded a high degree of protection.

Although there are risks that, by collecting the identities of minors on a national basis, some of them may be inadvertently compromised or exposed, those risks are heavily outweighed by the increased opportunities that this database will provide, nation-wide, to identify and apprehend the perpetrators of the crimes against and by children. Furthermore, to mitigate these risks and protect this sensitive information, the FBI has promulgated policies restricting access to case sensitive information for authorized investigative purposes, which are described in regard to this system in Section 8.5. In addition, authority for non-FBI entities to access the information will be controlled by the FBI through a password protected encrypted system, subject to FBI management approval and in compliance with pre-established disclosure agreements. An audit mechanism will also be in place to detect improper access to or use of database information so that appropriate corrective action can be taken.

Section 3.0
Uses of the System and the Information.

3.1 Describe all uses of the information.

The database will act as the central storage medium for information regarding the activities and locations of suspected pimps and victim prostitutes. The database will be utilized to search for information on suspected pimps and victim prostitutes, to confirm the identity of victim prostitutes (who often provide false names when interacting with

law enforcement), and to provide a common communications environment for investigators working/interfacing with the same suspected pimps and prostitutes. The database will allow for the national collection of intelligence regarding prostitution and the national analysis of pimp and prostitute networks and activities. Such analysis will allow the CACU to determine trends, patterns and most importantly, develop cases which are national in scope.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

The system will allow for the national analysis of known data about suspected pimp and child prostitution networks and activities. Queries are based on names or other known data elements; therefore the system does not allow for "data mining" as described. Investigators will be able to use the database to search for common terms in a case specific environment in order to obtain for known data a more complete and accurate picture of what information is available. This type of analysis may lend itself to the development of cases that potentially are national in scope and whose resolution will help reduce the incidence of child prostitution.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The information will be submitted by law enforcement officers currently working child prostitution investigations. Because it is critical that accurate information be maintained, there is a built-in incentive to ensure the veracity of the records. Added to this incentive, system rules will require that submitters provide information updates as they become available. As multiple records are collected on the same individual or individuals suspected of being the same individual, the submitting agencies will be contacted by the CACU data steward[1] or other CACU personnel to verify which information is accurate. This can be accomplished in one of two ways. With records that are entered into the database and then modified by a subsequent entry, the owner of the original record maintains the ability to accept or reject changes to the information it has shared. In the event of conflicting reports entered simultaneously or nearly so, the CACU data steward retains final authority to deconflict the information, based on consultations with the record owner and the submitter(s). Separately, conflicts in the data will be ascertained by means of an automated "smart query" that will be run on a daily basis.

[1] The CACU has named an Intelligence Analyst as steward of the Innocence Lost database to ensure oversight and accountability for the database. The data steward will have the ultimate authority to approve access to the data and the level of access an individual may be afforded, and the data steward will ensure that the rules for participating in the database are strictly enforced.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Under the current statute of limitations, individuals responsible for the sex trafficking of children may be prosecuted throughout the life of the victim. Substantive FBI information in the database is covered by the existing records schedule for the FBI's Central Records System, where the records are maintained. While certain of the records are considered permanent, most case files are destroyed after the expiration of 20 years from the time of case closure. To the extent that queries of the database and other administrative activities result in electronic records that must be retained, the FBI will work with the National Archives and Records Administration to develop an appropriate retention schedule.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The Innocence Lost database will be maintained in Law Enforcement Online (LEO), which is a secure controlled-access communications and information sharing repository accessible to authorized law enforcement users through a password-protected system. LEO operates as an SBU network and is certified and accredited under the Federal Information Security Management Act. LEO systems employ several different data encryption devices that encrypt data across a Wide Area Network (WAN) or Internet links. These devices prevent unauthorized access to or reading of data as it passes over the links. The FBI will be the sole agency to authorize the end users of the Innocence Lost database. In addition, an FBI data steward from the CACU will ultimately be responsible for the database and, through oversight, will ensure adherence to database rules.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

4.1 With which internal components of the Department is the information shared?

In addition to being shared within the FBI with those who have a need to know for analytical or operational purposes, the information in the Innocence Lost database may be made available to Trial Attorneys working child prostitution matters at the DOJ/Child Exploitation and Obscenity Section and to Assistant United States Attorneys (AUSAs) for prosecution as appropriate.

4.2 For each recipient component or office, what information is shared and for what purpose?

FBI Intelligence Analysts and agents will utilize the information to identify the networks involved in the trafficking of children. Additionally, the information will be utilized to identify unknown victims. Trial attorneys and AUSAs will use the data for prosecutions.

4.3 How is the information transmitted or disclosed?

The information will be accessible to end users through the FBI LEO encrypted system. End users will have varying levels of read/write access based on their involvement in Innocence Lost Child Prostitution Task Forces. End users will access the secure site via a secure socket layer (SSL) web connection employing username and password access controls and utilize a search screen to locate information needed for on-going investigations, based on their particular role.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Sharing personally identifiable information carries with it a risk of improper access and/or improper use. Because the system relies on role-based access and because users within the FBI and Department of Justice must be certified by the data steward as having a demonstrated need for access, these risks will be mitigated. In addition, system access rules will be enforced through periodic audits, which will permit anomalous activity to be flagged and referred for investigation. Rules of Behavior will be placed at the login screen specifying the conditions for access and that the information contained in the database is law enforcement sensitive and for law enforcement use only. This will serve as a reminder to users that the database contains sensitive information and that access and use of the data will be strictly monitored to ensure compliance with system rules.

Section 5.0
External Sharing and Disclosure

5.1 With which external (non-DOJ) recipient(s) is the information shared?

The information may be shared with local, state and federal law enforcement officers who actively investigate missing children cases and/or child prostitution cases. In addition, information from the database may be provided to NCMEC in an effort to identify missing children and obtain additional details about subjects of interest.

NCMEC is a private, non-profit Section 501(c)(3) organization with a Congressional mandate which includes, but is not limited to, serving as a clearinghouse of information about missing and exploited children and providing technical assistance to law enforcement, including the FBI, in the prevention, investigation, prosecution, and treatment of cases involving missing and exploited children.

5.2 What information is shared and for what purpose?

Information will be shared with local, state and federal law enforcement officers who are attempting to solve crimes involving the sex trafficking of children. In order to ensure that only those with a need to know can access the database, permission to use the database will be granted by the FBI data steward and log-on to the database will only be permitted after a user has reviewed Rules of Behavior describing the proper utilization of the information. In addition, access to particular data elements will be based on role.

Users will be able to employ the database to determine the true identity of victims of prostitution who frequently utilize false identification. Similarly, the information will be utilized to assist in identifying child prostitution enterprises. The information will be used to link together investigations across the nation targeting common suspects and to act as a central storage medium for a highly mobile crime problem. Intelligence Analysts and law enforcement personnel will utilize the information to identify the networks involved in the trafficking of children. Additionally, the information will be utilized to identify unknown victims.

5.3 How is the information transmitted or disclosed?

The information will be accessible to end users through the FBI LEO encrypted system. End users will have varying levels of access based on their involvement in Innocence Lost Child Prostitution Task Forces. End users first access the LEO secure site and then must access the database through a Special Interest Group (SIG) established for that purpose. Membership in the SIG is controlled by the data steward. Once a user has been validated, he or she will access the secure site to input new records and utilize a search screen to locate information needed for on-going investigations, but any access to the data will be based on role.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

When a user logs onto the SIG in LEO to access information from the database, Rules of Behavior will be posted that must be reviewed before a query is permitted. These rules will indicate the sensitivity of the data to be accessed and the procedures that should be followed in order to perform queries. To protect the security and privacy of the data, the system only permits twenty-five records or fewer in response to queries. This

helps to limit accessibility to the data and ensures that information to be provided is targeted to meet a particular query. In addition, the information that is returned is formatted at Hypertext Markup Language (html), which facilitates information sharing in a controlled and secure manner. Search screens will contain a cautionary statement that the information contained herein is "law enforcement sensitive," the property of the FBI and cannot be disseminated outside the receiving agency without the FBI's permission. All generated reports and accessed screens will be marked "For Official Use Only – Law Enforcement Sensitive."

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

Access to the database requires user agreement with specific and comprehensive rules of behavior that address security, data handling and personal responsibility by the user to keep his or her eligibility for membership updated by reconfirming it on a yearly basis with the data steward (or terminating when appropriate). The rules also require users to refrain from uploading certain types of information, and to ensure that any information that is added to the database has been legally obtained and can be legally shared. Because database users are expected to be personnel whose primary responsibility is in the area of crimes involving child victimization, it is expected that they will be sensitive to the nature of the information in the database and appreciate the restrictions that are imposed on the data. Nevertheless, users of the information must be able to demonstrate to the satisfaction of the data steward a bona fide need for access in the performance of their official duties.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

Yes. The database will be housed on LEO, which has its own procedures and devices for intrusion detection and which uses an audit reduction tool to detect intentional misuse of the system. The log generated by the audit reduction tool is monitored daily and a report is provided to the data steward, who can review the report for anomalous activity entries and pursue appropriate follow-up action.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The information to be shared currently exists and is shared by law enforcement agencies upon request. The privacy risk created by this database is that the sharing may be more robust and that connections among data elements that were previously not apparent may become obvious. This database will facilitate connections among law enforcement officers and allow for a more direct and efficient exchange of case-related

information at the discretion of the investigating agency. The privacy risks from this enhanced sharing are mitigated by oversight of the database by the data steward and by strong audit controls at the user and system levels. In addition, users will have access based only on the level of permission assigned by the FBI, giving a measure of control to the access that is provided

Section 6.0
Notice

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Because information is collected in connection with law enforcement activities, no individual notice is given. Nonetheless, when an individual interacts with law enforcement and is aware that he or she is interacting with law enforcement, that individual should be aware that any information collected at that time will be used for law enforcement purposes. General notice concerning the collection of FBI information used in this system, however, is provided through the System of Records Notice for the Central Records System maintained by the FBI (63 FR 8671).

6.2 Do individuals have an opportunity and/or right to decline to provide information?

N/A. See previous answer.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

N/A. See answer to question 6.1.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy risk identified would be the failure of persons to know their information may be collected and to know how it will be used. In mitigation of this risk, the FBI has published a Privacy Act System of Records Notice (SORN) for its

investigative records. The notice includes information about entities with which and situations when FBI may share investigative records. No other notice is provided, and no other notice is required to be provided because the information in this system is collected during law enforcement investigations and it is not practicable for any other notice to be given during these investigations.

Section 7.0
Individual Access and Redress

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Applicable regulations found in 28 CFR Part 16, Subparts A and D, which have been issued pursuant to the Freedom of Information and Privacy Acts, govern requests for access to information in FBI files.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

28 C.F.R. 16.41 and 16.46 provide information on individual access and amendment to records.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

See previous response.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

If an individual believes he or she is the subject of records maintained by the FBI, the procedures established in 28 C.F.R. 16.46 are available for contesting the information. Although FBI records are generally exempt from Privacy Act access and amendment procedures, the FBI, of course, strives to maintain accurate information and will, in its discretion, consider amendment requests. To ensure data integrity, updates of information are required from data contributors and smart queries will be used to harmonize conflicting data.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system?

Law enforcement officers, analysts and attorneys from local, state and federal agencies who are charged with investigating crimes against children and specifically child prostitution matters will have access to the system. Additionally, select employees from the NCMEC will have access.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

No.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes (see below)

8.4 What procedures are in place to determine which users may access the system and are they documented?

The users are required to apply for LEO membership and additionally request access to the Child Prostitution Special Interest Group (CP SIG). The FBI CACU approves and denies membership to the CP SIG and will be responsible for assigning each user to one of six access levels to the database.

- System Administrator - LEO Computer Technicians responsible for the operational management of the database. Full access to test and monitor.
- Data Steward - Limited CACU personnel responsible for granting membership access and setting permissions for all users; merging, updating, and deleting records. Full access to test and monitor.
- HQ Full Access: Full Access to query, add, update, and search on all data.
- Field Access: Identified Special Agents, Analysts and Innocence Lost Task Force members working cases. Access to add new entries, query and read. Ability to update owned records only. Limited Read based on non-owned records.
- Limited Law Enforcement User: Access to add new reports, limited query access, and limited read access. Use by non-Task Force Members to identify missing children.
- No Access - Access to Special Interest Group only, no access to database.

A user's access can also be revoked at any time for disclosure, procedural or user policy violations.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Users will complete an application with a justification for the requested access. A database administrator, assigned to the FBI CACU approves or denies membership to the CP SIG and will be responsible for assigning each approved user to one of six access levels to the database. Members will be required to re-enroll on a periodic basis in order to ensure that only those who ought to have access to the database actually are members of the SIG.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

There will be an auditing function in the database that identifies users who accessed specific records or ran particular queries. Audit logs will be subject to LEO procedures for detecting anomalous uses and a daily report of any such uses will be reviewed by the data steward for purposes of taking corrective action. All users must agree to a user agreement before being permitted access to the database. In addition, search screens will contain a cautionary statement that the information contained herein is "law enforcement sensitive," the property of the FBI and cannot be disseminated outside the receiving agency without the FBI's permission. All generated reports and accessed screens will be marked "For Official Use Only – Law Enforcement Sensitive."

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

FBI employees receive annual privacy training as part of required Information Security training. In addition, a tutorial must be completed before passwords are granted to individuals who have been approved by the data steward for access to the database.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The LEO Program Office maintains Certification and Accreditation for the system. The last full C&A was performed in November 2006; a modification was approved in November 2007.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The database is subject to oversight by the data steward, role-based access, and oversight through LEO, where it is maintained. All of these attributes should help mitigate privacy concerns related to access and security. Potential privacy risks occasioned by access to the data have been mitigated through the user application process and the assignment of one of the six levels of access, depending on an individual user's role. Additionally, the system contains a strong audit function that can be used to detect improper use and/or access. If anomalous behavior or other misuse of the database is uncovered, appropriate sanctions will be applied, up to and including denial of access and elimination of privileges.

Section 9.0 Technology

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

There were no existing systems in place which stored this national information and met the needs of the end user.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The CACU sought the most secure environment to host the database and chose the LEO system, which is an encrypted network and which requires membership for access. The CACU has devised six additional membership levels for end users, which limits access based on role, in order to protect the privacy and security of the data. System configuration will be changed as appropriate if experience indicates a problem with data integrity, privacy or security, and appropriate modifications will be made in this PIA.

9.3 What design choices were made to enhance privacy?

It was determined that a web-based system would best serve the requirements for sharing law enforcement information about child prostitution. Other techniques were deemed inapposite. Design choices, as detailed above, were made to control access and dissemination of information obtained from the system to ensure information is utilized for legitimate law enforcement purposes.

Conclusion

The Innocence Lost database will facilitate investigations to help locate and recover victims of child prostitution, to identify and apprehend pimps responsible for their exploitation, and to assist federal, state and local law enforcement agencies with investigating and identifying child victims. In recognition of the sensitive nature of the data to be maintained in the database, the Crimes Against Children Unit has developed system attributes to protect the privacy and integrity of the information while still enabling it to be useful for resolving crimes, through the use of role-based access, dual sign-on requirements, strong rules of behavior, a data steward to exercise oversight and audit controls at the database and host level.

Responsible Officials

10/25/06 <<Sign Date>>

[redacted]

Unit Chief
Crimes Against Children Unit
CID - Violent Crimes Section

b6
b7C

[redacted]

2/2/07 <<Sign Date>>

Patrick W. Kelley
Privacy and Civil Liberties Officer
Federal Bureau of Investigation
Department of Justice

2/1/08 <<Sign Date>>

Kenneth P. Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice