Federal Bureau of Prisons

Privacy Impact Assessment
for the
Forensic Laboratory

Issued by:
Sonya D. Thompson,
Senior Component Official for Privacy,
Sr. Deputy Assistant Director/CIO

Approved by: Erika Brown Lee, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [November 18, 2014]

Section 1: Description of the Information System

The Federal Bureau of Prisons (BOP) protects society by confining offenders in the controlled environments of prisons, and community-based facilities that are safe, humane, and appropriately secure, and which provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens.

In accordance with sound correctional security practices, the BOP uses various security methods to detect and deter the use of unauthorized cell phones in its prisons. When such contraband is confiscated, retrieved cell phones are sent to the BOP's Forensic Laboratory (Lab) in Washington, D.C. for analysis. The Lab was established to assist BOP staff in recovering information from unauthorized cellular phones in order to determine if criminal or illegal activity has or is occurring. The original lab was first developed and implemented in 2009 pursuant to 18 U.S.C. § 1791, which was later updated in 2010 when Congress passed the Contraband Cell Phone Act of 2010, Pub.L. 111-225, 18 U.S.C. § 1791. This Act prohibits the possession of cell phones in prisons by unauthorized persons, including visitors providing a cell phone to an inmate, or for an inmate to possess a cell phone.

When a cellular device is retrieved at an institution, the cellular device is sent to the Lab whereby lab technicians use various forensic software tools to extract information, including incoming and outgoing phone numbers dialed from and to the phone, and text messages and images stored on the phone's memory (internal and SD card). In addition, artifacts are produced from such analysis, such as metadata (e.g., subscriber information, device type, serial numbers, cell towers, location base via GPS and all other data that can identify the device specifically to providers), email contents, and local applications use and content, including web browsing history, remote/cloud activity, SMS, Skype, WIFI connections and Social networking Services (SNS). The Lab also performs forensic analysis of other types of mobile devices (e.g., tablets), as well as computer forensics of laptops and workstations, when required.

Extracted data from the device is compiled into a report at the Lab and sent back electronically to the forwarding institution for further investigation by local intelligence staff. BOP intelligence staff use this extracted information to determine if illicit or criminal activity is occurring and who was potentially responsible for smuggling the cell phone into the institution. Further, such information may be shared with other components within the Department of Justice, in addition to federal, state and local law enforcement agencies, for purposes of criminal investigation.

The Lab's IT system is a stand-alone infrastructure consisting of workstations (hardware), software and local Network-attached storage, in order to share data among forensic workstations and BOP Lab staff. The only individuals with physical access to the Lab and to the equipment and software therein are staff assigned to the Central Office Intelligence Section, which includes BOP staff forensic analysts. The Lab is physically secured inside BOP's headquarters using a Personal Identity Verification (PIV) card which is controlled and enabled via use of a Physical Access Control System. Workstations are secured by requiring individuals to log in with user identification (userID) and password authentication. Data stored on any external hard drives is encrypted. The Lab's workstations are not interconnected to any other BOP system.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card	X		
Other identifying numbers (specify): Inmate federal register number; other identifying numbers, such as credit card numbers may be recovered inadvertently when data is extracted during the analysis process.					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth		Financial info	
Alias	X	Home address	X	Medical information	
Gender		Telephone number	X	Military service	
Age	X	Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify): Data found on the phone may include information pertaining to third-parties.					

Work-related data					
Occupation		Telephone number	X	Salary	
Job title		Email address	X	Work history	
Work address		Business associates			
Other work-related data (specify): Data found on the phone may include information pertaining to third-parties.					

Distinguishing features/Biometrics					
Fingerprints		Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures	X	Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): Voice mail and scars, marks and tattoos may be recovered from media (photos, audio, etc.) captured from and/or stored on the cell phone.					

System admin/audit data							
User ID	X	Date/time of access	X	ID files accessed			
IP address	X	Queries run	X	Contents of files	X		
Other system/audit data (specify):							

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	
Telephone	X	Email	X		
Other (specify): Cell phone Texts: Short Messaging Service (SMS), Multimedia Messaging Service (MMS), Social Network Services (SNS); Call history logs.					

Government sources					
Within the Component		Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify):					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify): Publicly-available sources: Reverse Phone Number Lookup Database, Internet Service Provider IP Addresses, People Search Database (Pipl)					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Improper physical access to the Lab and technological access to its IT systems and infrastructure are the primary threats to privacy that exist in light of the information collected. Unlike traditional computer forensics where data collection analysis can be used for only specific artifacts like email or pictures, the technology used by BOP for forensic extraction on mobile devices is designed to retrieve all artifacts on the device. As a result, BOP takes significant steps to ensure that privacy protections are followed for the sensitive information stored therein. The Lab's IT infrastructure is a stand-alone

network with physical and electronic access only assigned to forensic examiners in the Lab. Access is role-based and in accordance with security clearances as noted in Section 3.5. The network is protected by a firewall and Active Directory Domain. Access to the network, and data stored therein, requires a userID and password. Additional system security is provided at the data storage level through the use of disk encryption.

Further, as described in Section I, physical access to the Lab requires authorization through a PIV-card, controlled and enabled via use of a Physical Access Control System. These measures mitigate unauthorized physical access to the Lab and its IT infrastructure. Highly-sensitive data extracted from the phones, contained in hard-copy documents and reports, is stored in a locked safe within the Lab. Combinations are known only by the examiners assigned to the Lab. In case of an emergency, the Correctional Service Administrator (CSA) can override the combination with a key that is stored offsite in a safe protected by another PIV-controlled access system. The CSA does not have direct access to the Lab with his or her PIV-card. All visitors and non-Lab BOP staff must sign in and be escorted at all times.

Also, there is a privacy risk related to the inadvertent disclosure of sensitive information to persons not authorized to receive it. To mitigate this risk, sensitive data retrieved from confiscated phones is only shared with intelligence staff and Chief Executive Officers (CEOs) at the site where the phone was retrieved for further investigation. All BOP staff members, including lab technicians, are annually trained on how to properly handle sensitive information. Access to any relevant data is limited to those persons who have an appropriate security clearance which is regularly reviewed.

In general, information is safeguarded in accordance with BOP rules and policies governing security of and access to information systems. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification to access the system.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities		For civil enforcement activities
X	For intelligence activities		For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
X	To conduct analysis to identify previously unknown areas of note, concern, or pattern (e.g., a possible source for introduction of contraband; an identified security breach or vulnerability within a particular institution).		For administering human resources programs
	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The BOP uses the information collected from confiscated phones to determine if criminal or illegal activity has or is occurring. The BOP also uses the information extracted from the device to identify the responsible party who smuggled the cell phone into the institution, and who has used the device since its introduction into the institution. The information is used for internal intelligence activities associated with the safe and orderly operation and security of BOP institutions. The BOP also may share data on a case-by-case basis with external federal law enforcement task forces for criminal investigations and intelligence gathering.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	18 U.S.C. §§ 3621, 4042, 4082 and 5003 (state inmates), Section 11201 of Pub. L. 105-33; 111 Stat. 740 (DC felons); 18 U.S.C. §1791 (Pub. L. 111-225).
	Executive Order	
X	Federal Regulation	28 C.F.R. §§ 553.12 and 553.13.
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Data retrieved from the mobile device is temporarily stored on the Lab's IT network until a referral report has been sent back to the institution where the mobile device was retrieved. The confiscated device remains at the Lab. If retained for further investigation, the file retention period is temporary. The Lab destroys all of its files and data, including the reports, the metadata extracted from the phone, and the devices themselves, when no longer needed for legal evidence or investigative purposes or four years, whichever is later. The applicable authority has been approved by NARA (Authority # N1-129-09-11).

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Forensic analysis of contraband mobile devices often contains information on inmates as well as third-parties associated with the inmates. This information can be financial and/or personal in nature. To ensure this information cannot be inadvertently disclosed to unintended parties, all artifacts are stored within the Lab's IT network and protected by physical and electronic access controls described above. All reports are assigned an internal Lab tracking number (TRK) that is cross-referenced with an Evidence Control Number (ECN) that is assigned by the facility's BOP Special Investigative Agent (SIA) when an investigation is opened. The ECN numbers are assigned by the requesting SIA based on the facility where they are assigned. All reports are sent only to the relevant and specified SIA's electronic mailbox (which is accessible only by Intelligence staff) and the CEO/Warden, unless another disclosure is specifically authorized by the SIA and/or Warden. Reports are only sent to internal DOJ components or outside federal law enforcement agencies once approved by the relevant SIA and/or the BOP's Office of Internal Affairs. The internal DOJ component or outside law enforcement agency must provide the Lab with the BOP Lab's TRK number or ECN number prior to receiving the requested forensics reports. This measure ensures that BOP SIA communications are secure within the internal DOJ component or outside agency prior to requesting information from the Lab.

Further, BOP has put into place additional restrictions that prevent physical access to the Lab and to the data stored within the IT system and work stations within the Lab. Physical access to the Lab and data stored within its IT network is limited to those persons who have an appropriate security clearance and are authorized to review such information for their official duties. User access privileges are regularly reviewed by the Correctional Services Administrator. Information in the system is safeguarded in accordance with BOP rules and policies governing information systems security. Staff receives periodic and annual training on information security and handling of sensitive information.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X			
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities	X			

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

To ensure information cannot be inadvertently disclosed to unintended parties, all artifacts are stored within the Lab and protected by physical and electronic access controls described above. As discussed above, all reports are assigned an internal Lab tracking number (TRK) that is cross-referenced with an Evidence Control Number (ECN) that is assigned by the facility's BOP Special Investigative Agent (SIA) when an investigation is opened. The ECN numbers are assigned by the requesting SIA based on the facility where they are assigned. Reports are only sent to internal DOJ components or outside federal law enforcement agencies once approved by the SIA and/or the BOP's Office of Internal Affairs. The internal DOJ component or outside law enforcement agency must provide the Lab with the BOP Lab's TRK number or ECN number prior to receiving forensic reports. This measure ensures that BOP SIA communications are secure within the internal DOJ component or outside agency prior to requesting information from the Lab.

Information retrieved from confiscated phones is shared within BOP to authorized persons for additional investigation. Information may also be shared with certain components within the Department of Justice including EOUSA, Criminal Division, and the FBI or with federal law enforcement task forces. These entities receive data on a case-by-case basis electronically or the information may be printed and provided to such offices in hard copy. Some data may also be shared with Department of Homeland Security for purposes of criminal investigation. State and local law enforcement may be provided information in relation to a criminal investigation. All information that is covered by the Privacy Act is disseminated in accordance with the Privacy Act's disclosure rules.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
X	No, notice is not provided.	Specify why not: Information is collected and retrieved as part of BOP's forensic examination of confiscated cell phones. No notice can be provided to individuals, whose information is potentially contained on the confiscated cell phones, since their identity is unknown at the time of collection and extraction.

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Information is collected and retrieved as part of BOP's forensic examination of confiscated cell phones. No notice can be provided to individuals, whose information is potentially contained on the confiscated cell phones, since their identity is unknown at the time of collection and extraction. Thus, individuals do not have the opportunity to decline to provide such information.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Individuals do not have the opportunity to provide consent to disclosures since their identity is unknown at the time of collection, extraction, and use of their information.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Because the identity of the individuals are not known at the time the cellular devices are confiscated, actual notice cannot be provided at the time the devices are collected. However, notice of the information maintained is provided by the applicable System of Records Notice BOP-001, "Prison Security and Intelligence Record System," 67 FR 41449 (06/18/02); 72 FR 3410 (01/25/07). Individuals are not provided the opportunity to provide consent to collection or use of the information since the identity of the individual is unknown at the time of cell phone confiscation, and subsequent extraction of data, and may potentially compromise a subsequent criminal investigation.

Section 6: Information Security

6.1 Indicate all that apply.

	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: January 2015		
	A security risk assessment has been conducted. Note: A security risk assessment is planned to be completed by January 2015.		
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Physical access is controlled via PACS. Authentication to workstations requires the use of unique user IDs and passwords. Data is encrypted in storage.		
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Documentation is audited upon peer review and program review. Access to certain sensitive information requires specific authorization and is limited to select personnel.		
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: User access is audited on an annual basis.		
	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.		
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.		
X	The following training is required for authorized users to access or receive information in the system:		
	X		General information security training
	X		Training specific to the system for authorized users within the Department.

		Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

User access to the Lab's IT network is assigned and privileges to view data are based on such approval. User access for an employee must be requested by an applicable supervisor indicating that access is required for the performance of the employee's duties.

Users are trained as to the sensitive nature of the data within the system and continuously reminded as to the need to strictly control the viewing and/or output of data from the systems. BOP users are trained annually regarding the handling of sensitive information and information security requirements. All employees who are involved in the management, operation, programming, maintenance, or use of a DOJ information system are made aware of the threats to and vulnerabilities of those systems and their responsibilities with regard to privacy and information security.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: • BOP-001, "Prison Security and Intelligence Record System," 67 FR 41449 (06/18/02); 72 FR 3410 (01/25/07).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

No information on individuals is directly retrieved by a personal identifier from this system. Information, which may or may not contain information on individuals, is retrieved from the Lab system by either a Lab Tracking Number (TRK) or Evidence Control Number (ECN).