Department of Justice – Civil Division

Privacy Impact Assessment
for

Palantir Relational Information Management Application
(PRIMA)

Issued by:
Allison Stanton

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: September 27, 2018

EXECUTIVE SUMMARY

The Civil Division's Palantir Relational Information Management Application (PRIMA) provides a highly configurable commercial software product to support the management of cases for the attorneys and staff members of the Civil Division of the Department of Justice (DOJ). PRIMA is designed to help attorneys or other professional staff members acquire, organize, analyze and present evidence or other data as part of investigations and litigation. Through the use of computer data processing, image management, trial presentation systems, and other technologies, litigation materials are effectively organized so that the litigating attorneys and other professional staff can rapidly locate information and make the best use of it in conducting an investigation, litigation, or settlement negotiation.

The Civil Division conducted a PIA to comply with the E-Government Act of 2002, the Federal Information Security Modernization Act, Department of Justice IT Security Standards and Security Authorization Process, and National Institute of Standards and Technology's NIST 800-53 Rev. 4. Based on these requirements, the Civil Division (Division) determined that PRIMA maintains sensitive material, including information about individuals that is protected by various privacy statutes, regulations, and guidance. The personally identifiable information PRIMA maintains is collected by the Division or its client agencies in the course of investigations and litigation in order to effectuate the Division's litigation mission.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

a. The purpose that the records and/or system are designed to serve:
PRIMA is an electronic system that facilitates data analysis to support the Division's investigations and litigation. The system allows authorized Division trial attorneys, client agencies, contract attorneys, paralegals, and analysts to support the following investigation and litigation functions: document review and triage; and link analysis, case theory investigations,

deposition preparation, and creation of trial exhibits. PRIMA allows the investigation or trial team to share case data in a secure and collaborative environment and to limit access to data sets on a need-to-know basis.

b. The way the system operates to achieve the purpose(s):
To provide this support, PRIMA is a data integration and analysis platform that integrates data of any size or format, indexes and models the data into a unified format, and makes the data available for analysis using a variety of embedded applications and helpers. The system allows users to integrate data in different formats, analyze this data within a single compatible workspace, and produce analytic work products in a variety of formats. The system provides statistical analysis to identify trends, highlight outliers, and identify correlations in large-scale data sets. The collaborative features integrated into PRIMA's security model allow the maximum amount of information to be shared as authorized without leaking protected information. This secured sharing is accomplished by the "security-aware" functionality. When users collaborate in PRIMA they are actually sharing a link and each are accessing the underlying data element directly (within the secured space of the application), not passing a copy of the information between users. When the recipient uses the shared link to view the data element, the recipient only sees the components of that item which the recipient has permission to view, if any. PRIMA can ingest documents directly and/or pull them from software tools (Concordance, Relativity, etc.) to support litigation efforts within the Division.

c. The type of information collected, maintained, used, or disseminated by the system:
PRIMA houses data collected in the course of Civil Division's investigations or litigation. The information may be collected as part of a client-agency's investigation and provided to the Division or may be produced to the Division by an opposing party in the course of the discovery process overseen by the federal courts. The information ingested into the system depends on the data provided to the DOJ for a specific case. It can include, but is not limited to, all types of sensitive, confidential business information, personally identifiable information (PII), or personal health information (PHI) collected in an investigation or produced in the discovery process. Publicly available information may also be incorporated if deemed relevant to the litigation. Publicly available information may include, but is not limited to, newspaper articles and other published journalism, public records, court records, social media information, and other data traditionally considered "open source."

d. Who has access to information in the system:
The information maintained in PRIMA may be accessed by authorized Civil Division employees, other federal employees and contractors. For example, Civil Division employees and contractors are only granted access to databases on the system that support a matter they are working on. If an employee or contractor leaves or is reassigned, the account access is disabled or access to a particular database may be rescinded. PRIMA has security controls that are applied to individual pieces of information and role-based access permissions are assigned to individuals or groups of individuals. The security protocols ensure that users only see information they are authorized to see within cases they are assigned. Before access is authorized, the individual's access rights and purpose for accessing the documents is reviewed

by the Civil Division's IT security staff and the investigation and/or litigation team.

e. How information in the system is retrieved by the user:
There are multiple methods of retrieval in the system: text-based searches, structured searches, related searches and geospatial searches. Text-based searches allow investigators to search for keywords within the metadata and contents of items in PRIMA (e.g. author, title, & body of a document item). Structured searches allow investigators to narrow results based on metadata, such as a specific date range, or monetary threshold. Related searches allow users to find data elements that are linked to items they have selected. For example, a user could take a set of communications and search for all people involved in that communication, then search a second time to find other communications between those individuals. Geospatial searches allow investigators to find any data elements, such as office addressees, that appear within the specified area of a map. All of the searches that are retrievable by users are also "security-aware," meaning that users only see the results they have permission to see.

f. How information is transmitted to and from the system:
Information is transmitted to and from the system through PRIMA's version of the traditional Extract, Transform, Load process, the Crawl Extract Transform pipeline. This is powered by a collection of PRIMA integration functions that systematically identify the information in a given data source, extract the content into PRIMA, and transform the data into the PRIMA object model. The Civil Division transmits data into the system through a connection to another database, such as Relativity. Data can also be ingested into the system from removable storage devices (CDs, USBs, and hard drives), sent to the DOJ during discovery, attached to local system servers. Additional data may be uploaded into the system directly by users with the appropriate authorization on an *ad hoc* basis when deemed necessary to support specific litigation or investigation requirements. PRIMA maintains a detailed history of integration and transformations, including time of ingestion, source, and revision history for every piece of data. Built-in processes structure data upon ingest and automated checks are designed to ensure that data was technically ingested correctly and remains up-to-date. The data integrations include importing data from Relativity, supporting user imports of small data scales directly through the front-end interface, and future data integrations as agreed upon with DOJ's Civil Division. Data is then transformed or combined based on the needs of the case team and made available in a user-friendly format. For example, a user may wish to have one database of information merged with a database of different information, so that they are able to see associations and overlaps between the datasets. The integration process would involve bringing the respective database into PRIMA, merging each dataset based on the specifications of the user. The merged dataset is then made available in PRIMA for the case team.

g. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):
PRIMA interconnects to CIV-JCON (Justice Consolidated Office Network) and CORA (Civil Online Relativity Application) - both are Civil Division systems.

JCON is the Civil Division network, file storage, email, computer, desktop and application

infrastructure. PRIMA resides within the JCON space and shares physical access controls, network capabilities, security protections, etc. as do other Civil Division information systems. The interconnections between systems is documented within the CIV-JCON PIA and within each application or infrastructure system PIA.

CORA is the primary litigation support/e-discovery application for cases that the Civil Division hosts for DOJ and other Federal entities. CORA is a minor application, which relies on OLS Servers Systems (OLSSS) and CIV-JCON for physical, electronic, and security controls.

PRIMA does not communicate with any external systems. PRIMA is granted direct database access to specific CORA case folders. This connection allows for bulk extract from the CORA case folder and integration of the data into PRIMA. No information from PRIMA is sent to CORA, and the extract setup is read-only, meaning PRIMA does not modify, add, or delete data within CORA.

h. Whether it is a general support system, major application, or other type of system:
PRIMA is a minor application.

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	X	Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	X
Employee ID	X	Passport	X	Patient ID	X
File/case ID	X	Credit card	X		
Other identifying numbers (specify):					

General personal data					
Name	X	Date of birth	X	Religion	X
Maiden name	X	Place of birth	X	Financial info	X
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	X
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education	X	Mother's maiden name	X
Other general personal data (specify):					

Work-related data					
Occupation	X	Telephone number	X	Salary	X
Job title	X	Email address	X	Work history	X
Work address	X	Business associates	X		
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures	X	Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

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

Other information (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	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (specify): Information collected in the course of discovery may be collected from individuals who are opposing parties in the litigation. The request for such information would be through the discovery process overseen by the court. However, individuals do not directly input information into the system.					

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

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers	X				
Other (specify):					

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.)

As described above, the information contained in PRIMA is provided to the Civil Division in the course of an investigation or litigation. The documents are typically provided by another federal or state entity involved in the investigation or by the opposing party in the litigation in response to a subpoena or other discovery request. The privacy risks associated with collecting records from other entities is that they will share information outside the scope of the investigation or not properly identify the data being ingested into the system as containing personally identifying information. Preventing the exposure of the data once is it received by the Civil Division minimizes the risk that personal information will be shared outside the team of individuals working on a particular matter. To this end, the Civil Division places strict access controls on PRIMA via physical and electronic means in order to secure the information.

An additional risk is the collection of inaccurate data. Data produced for the system may contain errors. By allowing data from different sources to be analyzed in a single workspace while allowing multiple authorized users to review the data, the system facilitates the identification of inconsistencies that might indicate an error. Corrections to data are disseminated to all users within seconds of correction, and audit trails ensure that users are aware of the error and the correction.

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	X	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.	[ ]	For administering human resources programs
[X]	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 Civil Division's litigation mission includes civil and criminal enforcement. The information collected is used to accomplish activities inherent in the Division's investigations and litigation, including: reviewing documents for relevance to claims and defenses involved in the litigation; conducting privilege reviews of documents collected in the investigation; tracking the use of documentary evidence in litigation; preparing witness kits/binders for depositions and hearings; geospatial and link analysis relevant to litigation or investigation; and selecting and preparing exhibits for trial. PRIMA analysis and output aids the user's ability to review and understand the information; the analysis and output are not used as evidence. For example, temporal, geospatial, and link analysis of call detail record (CDR) data obtained from telecommunications providers are used to analyze contacts and connections between individuals relevant to the litigation. Temporal, geospatial, and link analysis of financial transactions may be used to demonstrate connections between individuals and/or movement of funds relevant to the investigation or litigation. Top-down or bottom-up analysis of relevant healthcare records, generally relating to healthcare fraud, may be utilized to identify outliers and patterns of behavior.

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	[28 U.S.C. §§ 514-19]
[ ]	Executive Order	[ ]
[X]	Federal Regulation	[28 C.F.R. §§ 0.45-0.49, Subpart I]
[ ]	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 will be retained in the system until the DOJ Civil Division case attorney and the Office of Litigation Support determine that the litigation materials no longer need to be stored in the system, typically after a case has closed or settled, and the information is not needed for other cases or investigations. In consultation with the attorney assigned to the matter, the Office of Litigation Support will dispose of records that do not need to be maintained in any form pursuant to the Division's obligations under the Federal Records Act, as explained below. Records that must be maintained will be retained in accordance with the applicable retention schedule. Archiving a case leaves the data with the attorney and the space previously used by the case is re-used (deleted, then made available elsewhere).

Files managed on PRIMA may include both federal records and non-records that are associated with a variety of different types of Civil Division's litigation case files. The retention policies for the files depend on the federal record status as well as the classification of the type of case file to which the files pertain. The Department of Justice record retention schedules are published at https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060. Record retentions for case files range from approximately 5 years to 65 years after the case closure date. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of the National Archives and Records Administration. Non-records are destroyed when no longer needed for convenience of reference.

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.)

There is a potential risk to privacy that could result from the improper access to information in the system or storage of information longer than is required by the Division's record-keeping requirements. Security protections that authorize and limit a user's access to information within the system mitigate the risk of improper access. Physical controls such as secured entrances and security officers protect access to the building where the servers and workstations are located. To access the system, the Civil Division enforces Department standards for accessing a network system, such as Personal Identity Verification (PIV) card entry. In addition, before a user is granted access to a system hosted by the Civil Division, the user completes required security training, including cybersecurity training and privacy training targeted to the user's role. Individuals outside the Civil Division are required to sign a confidentiality agreement and rules of behavior documents before they are provided with access to accounts. In addition, all contractors granted access to the system must adhere to the Department's IT security standards for reporting security incidents.

Information access to the system is granted on a need-to-know basis. For example, Civil Division attorneys, other staff members, other federal employees, and contractors are only granted limited access to the matters they work on, not the entire system. Strict electronic access controls ensure that users are only able to access data collected in support of their specific investigation or litigation. Granular access controls allow data to be secured at the data source level, as well as more granularly, including data point by data point (cell-level) security when necessary. Users may be further restricted to "view only" permissions to protect the integrity of particularly sensitive data.

There are monitoring and auditing tools for each system to review user activity, so the Civil Division can monitor user access within the system. Access controls are backed up by detailed audit logs that provide a detailed overview of how data has been accessed and used within the system to ensure compliance with applicable handling policies. In addition, the system generates detailed metadata and audit logging information that can help administrators manage data retention schedules as established for the system. Data can be identified based on its age, the specific case that it is supporting, whether the data remains in active use, and other parameters that might be relevant to a data retention decision. The Civil Division follows DOJ internal policies and procedures for unauthorized access or release of information from the system.

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	X	X	
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities	X			
Public	X			
Private sector	X			
Foreign governments	X			
Foreign entities	X			
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.)

Security protections that authorize and limit a users' access to information within the system mitigate the risks to privacy. Unauthorized physical access to PRIMA is limited by physical controls such as secured entrances and security officers who protect access to the building where the servers and workstations are located. The data maintained by PRIMA is protected through compliance with the Department's access control policy. To access the system, the Civil Division enforces Department standards for accessing a network system, such as Personal Identity Verification (PIV) card entry and role-based access controls. In addition, before a user is granted access to a system hosted on a DOJ system, the user completes required security training, including cybersecurity training and privacy training targeted to the user's role. Individuals outside the Civil Division are required to sign a confidentiality agreement and rules of behavior documents before they are provided with access to accounts. In addition, all contractors granted access to the system must adhere to the Department's IT security standards for reporting security incidents.

Information access to the system is granted on a need-to-know basis. Users both inside and outside the Civil Division are only granted limited access to the matters they work on, not the entire system. Users outside the Civil Division may include personnel from another component or agency, such as the client agency, partners at the United States Attorney's Office, or expert witnesses. Electronic access controls can be used to limit sensitive data access to only those users trained in data handling policies and authorized to make specific data sharing decisions. Applications used to export data can also be electronically limited to only those users with appropriate training and authority to make data sharing decisions. There are monitoring and auditing tools for each system to review user activity, so the Civil Division can monitor user access within the system. For data sets that contain particularly sensitive information, folder access is audited with greater scrutiny. The Civil Division follows DOJ internal policies and procedures for unauthorized access or release of information from the system.

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: [ ]
[ ]	No, notice is not provided.	Specify why not: [ ]

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: Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. An opposing party may challenge the relevance of the information and not produce the information in litigation. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.

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: Documents are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. An opposing party may challenge the relevance of the information and not produce the information in litigation. For social media captures and web site collections, notice is not provided to individuals as the information is considered to be in the public domain.

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.

Unless individuals are opposing parties in litigation, individuals do not provide information directly to the Civil Division for use in PRIMA. Individuals who are opposing parties in litigation can object to the Division obtaining the information through the discovery

process. Individuals whose information is collected in the course of litigation involving another entity, such as another government agency or business entity, may have the opportunity to consent at the collection from the other entity. If another government agency is involved in the investigation or litigation, the agency's System of Records Notice would provide notice that the information may be shared with the Department of Justice for the context of a civil or criminal investigation or litigation. For information collected from the internet, notice is not provided to individuals as the information collected is in the public domain.

Section 6: Information Security

6.1 Indicate all that apply.

[X]	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: [7/25/2017] If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: [ ]	
[X]	A security risk assessment has been conducted.	
[X]	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: [The Civil Division has applied the policies and procedures outlined in the DOJ Security and Privacy Authorization and Assessment Handbook and NIST 800-53 Rev. 4.]	
[X]	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: [Testing of the system is performed during operation by various IT security tools available within DOJ. Monitoring is performed in real-time by not only Civil IT staff but also in conjunction with Justice Management Division. Evaluation is performed in real-time via several packages of software, in place on the local machines and scanning network transmissions.]	
[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: [PRIMA complies with DOJ IT Security Standards via PIV card access, attribution to named individuals, disallowing test or training accounts and strict compartmentalization of information and accounts.]	
[X]	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
[X]	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.
	[X]	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.

The information maintained on PRIMA is protected in accordance with applicable DOJ guidance, policies, and directives. PRIMA exists on a physically secure, environmentally protected, DOJ network. The network is protected by firewalls, and is administered by both DOJ and non-DOJ contractor personnel. Access to PRIMA is granted only to DOJ-approved individuals who have signed a confidentiality agreement and system rules of behavior. Security training and a public-trust background check are performed on a regular basis on all staff who request access. Access to specific databases/folders/material is granted on a need-to-know basis by authorized Federal staff. Finally, all PRIMA accounts are "named user" accounts assigned to a single individual and require PIV authentication. Test, training, or temporary accounts are not permitted in order to accurately log the individual accessing the information.

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: [JUSTICE/CIV-001 *Civil Division Case File System*, last published in full at 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), https://www.gpo.gov/fdsys/pkg/FR-1998-02-20/pdf/98-4206.pdf.]
[ ]	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.

[Information about U.S. citizens or lawfully admitted permanent resident aliens is typically retrieved by full-text search. This search would look for the keyword combination “FirstName LastName” in the body or metadata of available records to that user based on their permissions. PRIMA privacy protections do not differ depending on whether the information about an individual is a U.S. citizen or a lawfully admitted permanent resident alien.]