Antitrust Division

Privacy Impact Assessment
for the
ATR Relativity Database Management System
(ATR RDMS)

Issued by:
Dorothy Fountain
Office of the Chief Legal Advisor
Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: September 30, 2021

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Antitrust Division's Relativity Database Management System (ATR RDMS) is an e-discovery system used by ATR personnel and supported by the Litigation Support Section (LSS) to process, manage, tag, redact and control case documentation. RDMS is a web-based application that offers document assessment, fact management, review, searching, analytics, and legal hold functionalities. RDMS provides ATR a robust data management environment for e-discovery, investigations, and litigation.

RDMS is a client-server environment that is deployed on premise to support the needs of ATR internal litigation and trial support sections. The system operates within the ATR Azure IaaS and General Support System (GSS) enterprise environments and is deployed onto MS Windows server platforms. At a high level, the general information types supported relate to litigation and judicial activities, law enforcement, international affairs, and antitrust regulatory development. ATR conducted this Privacy Impact Assessment to document its use of RDMS, in accordance with Section 208 of the E-Government Act of 2002.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

RDMS supports ATR's criminal and civil investigation and litigation functions. ATR collects documents, data, and testimony from opposing parties and third parties through issuance of civil investigative demands, search warrants, subpoenas, and discovery requests. Collected information is imported to RDMS in a digital format for a particular investigation or litigation, where it is catalogued, indexed, processed, and archived. ATR authorized personnel working on civil or criminal matters use RDMS to review, search, sort, tag and analyze documents and data. Copies of material in RDMS may be produced to the court or opposing counsel in litigation.

RDMS users are internal ATR personnel, other DOJ users, other Federal and State agencies, or other consultants and experts. All information is collected and disseminated in support of ATR litigation cases and investigations. Access to RDMS data is strictly controlled, with users having access only to that data for which they are authorized. All such access must comply with Department and ATR requirements and must support ATR investigation and litigation needs. The RDMS system manages user authorizations and access to information, including for views, searches, and sorting activities to analyze documents and determine which are relevant to a case.

2.2 ***Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)***

Authority		Citation/Reference
X	Statute	This project is authorized under the Antitrust Division's statutory jurisdictional authorities, which are discussed in Chapter II of the Antitrust Division Manual, Fifth Edition, available at https://www.justice.gov/atr/file/761166/download.
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 ***Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.***

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	
Date of birth or age	X	C and D	
Place of birth	X	C and D	
Gender	X	C and D	
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	SSNs are not actively collected but documents containing full or partial SSNs may be produced in discovery. LSS searches RDMS to identify SSNs for redaction, using automated scripts where possible.
Tax Identification Number (TIN)	X	C and D	TINs are collected from companies involved in litigations or investigations, where applicable.
Driver's license	X	C and D	
Alien registration number	X	C and D	
Passport number	X	C and D	
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C and D	
Personal e-mail address	X	C and D	
Personal phone number	X	C and D	
Medical records number	X	C and D	
Medical notes or other medical or health information	X	C and D	
Financial account information	X	C and D	
Applicant information	X	C and D	Documents received from a company during investigation that may pertain to job applications (HR data).

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Education records			
Military status or other information	X	C and D	
Employment status, history, or similar information	X	C and D	Includes business address
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C and D	
Certificates	X	C and D	
Legal documents	X	C and D	
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	C and D	
Foreign activities	X	C and D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	
Whistleblower, e.g., tip, complaint or referral	X	C and D	
Grand jury information	X	C and D	Grand Jury information is collected and requires specific access by only authorized individuals
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C and D	Information regarding criminal matters is collected. Access is limited to only authorized individuals who have specific roles with the case
Procurement/contracting records	X	C and D	
Proprietary or business information	X	C and D	
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	
- **Video containing biometric data**	X	C and D	
- **Fingerprints**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	C and D	
- **Scars, marks, tattoos**	X	C and D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	RDMS is operated and administered by DOJ government and contractor personnel
- **User ID**	X	A	All administrators are provided unique user IDs
- **User passwords/codes**	X	A	All administrators use unique passwords and PIV cards
- **IP address**	X	A	IP address information is contained within the system
- **Date/time of access**	X	A	Access logs with date and time of access are maintained within the system and are generally limited to the user and administrators
- **Queries run**	X	A	Query runs are maintained within the system and are generally limited to the user
- **Content of files accessed/reviewed**	X	A	Audit logs of files accessed are stored and reviewed by admins
- **Contents of files**	X	A	Contents of all files are available to admins
Other (please list the type of info and describe as completely as possible):	X	C and D	Additional personal information could be collected or received through investigations and litigation.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	✓	Hard copy: mail/fax	✓	Online	✓
Phone	✓	Email	✓		
Other (specify):					

Government sources:					
Within the Component	✓	Other DOJ Components	✓	Online	✓
State, local, tribal	✓	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	✓		
Other (specify):					

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

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	✓		✓	ATR will share RDMS information among ATR offices on a case-by-case basis. ATR generally will provide access to data via a RDMS account upon Section Chief/Assistant Chief approval. The requester's access is limited to only the requested data.
DOJ Components	✓		✓	ATR will share RDMS information with other DOJ components on a case-by-case basis. ATR generally will provide access to data via an RDMS account upon Section Chief or OCLA approval. The requester's access is limited to only the requested data.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities	✓		✓	ATR will share RDMS information on a case-by-case basis with federal entities with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a RDMS account, utilizing a GFE and/or RSA token through VPN, for direct log-in or using the Justice Enterprise File Sharing System (JEFS). The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.
State, local, tribal gov't entities	✓		✓	ATR will share RDMS information on a case-by-case basis with state, local, tribal government entities with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a RDMS account, utilizing a GFE and/or RSA token through VPN, for direct log-in or using the Justice Enterprise File Sharing System (JEFS). The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes		✓		ATR will share case documents with the parties and court as required by discovery rules or court orders. Such documents are often provided to opposing parties and courts in bulk, for example, thousands of documents could be provided and received by the parties in a discovery document production.
Private sector	✓		✓	ATR will share RDMS information on a case-by-case basis with the private sector with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a RDMS account, utilizing a GFE and/or RSA token through VPN, for direct log-in or using the Justice Enterprise File Sharing System (JEFS). The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Foreign governments	✓		✓	ATR will share RDMS information on a case-by-case basis with foreign governments with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a RDMS account, utilizing a GFE and/or RSA token through VPN, for direct log-in. The requester's access is limited to only the requested data. Foreign governments with read access to ATR RDMS are litigating partners in criminal or civil matters. The requester's access is maintained until termination is directed by the legal staff.
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

ATR does not release to the public data or documents submitted by parties in investigations and litigation and stored in RDMS. ATR provides only statistics and case filings to the "Open Data" site (www.data.gov).

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

An ATR SORN provides generalized notice to the public.

ATR-006, "Antitrust Management Information System (AMIS) - Monthly Report," 63 Fed. Reg. 8659 (2-20-1998), 66 Fed. Reg. 8425 (1-31-2001), 66 Fed. Reg. 17200 (3-29-2001), 82 FR 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.88.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals involved in investigations and litigation are properly notified in accordance with Federal criminal and civil procedures and court rules. ATR obtains the majority of the information stored in RDMS through subpoenas, discovery requests, search warrants, civil investigative demands, or second requests under the Hart-Scott-Rodino Antitrust Improvements Act ("HSR" Act).[1] For these information-gathering mechanisms, individuals do not have the opportunity to decline to provide the requested information and documents. Certain information in RDMS may be provided voluntarily.[2] For information collected from public sources, notice is not provided to individuals.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

ATR's Privacy Program Plan captures policy and procedures to ensure compliance with Federal and Department FOIA guidelines regarding requests for information or amendment, to the extent the information is in a system of records and no exemption exists. All such requests are submitted to the ATR's FOIA/Privacy Act Unit (https://www.justice.gov/atr/antitrust-foia) for processing and response.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** 1/15/2020 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** There are no open POAMs within the profile.

[1] The HSR Act, 15 U.S.C. § 18a, requires parties to certain transactions to notify ATR and the Federal Trade Commission of the transaction and to provide certain documents, and it permits the agencies to make a request for additional information and documents (a "second request").
[2] For example, during the initial waiting period of an ATR investigation under the HSR Act, ATR typically requests and parties typically provide the voluntarily submission of certain information and documents.

n/a	**This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:**
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** ATR RDMS has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, the system has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook. The system has been fully incorporated within the ATR General Support System boundary, where it is subject to full system monitoring and audit in accordance with ATR and Department guidelines. All system documentation supporting these activities is maintained within the Department's system of record, Cybersecurity Assessment and Management (CSAM).
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** ATR RDMS compiles audits at multiple layers, including the network and application processing levels. All logs are reviewed weekly by onsite administrators and then gathered and centrally managed using the Department's audit analysis solution, SPLUNK.[3] All logs are forwarded to the DOJ Security Operations Center (JSOC) for automated analysis and review.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Pursuant to Department policy, contractors are generally required in their contracts to comply with the Privacy Act and other applicable laws. All contractors granted access to ATR RDMS are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All RDMS users are subject to onboarding training that includes computer security awareness and privacy training, which is an annual requirement thereafter. They are also required to undergo initial training for specific use of RDMS during Entry on Duty. Additional RDMS training is offered periodically, as needed for particular matters or users.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII

[3] The Department's Splunk Instance captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.

in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

All RDMS users are required to use multi-factor authentication or unique username and passwords to access their RDMS accounts. Data access is highly restrictive; users require formal approval and authorization to access information on a case-by-case basis. Users can access only data for which they are authorized. All users are required to undergo training and sign formal Rules of Behavior prior to being granted access to RDMS data.

6.3 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.)

Information is disposed of or retained in accordance with Directive ATR 2710.1, "Procedures for Handling Division Documents and Information," consistent with National Archives and Records Administration regulations and records schedules. Material submitted in investigations and litigation that are maintained in RDMS and are not Federal records or that have completed their retention period are often destroyed or returned to the submitting party.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. ___X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

ATR-006, "Antitrust Management Information System (AMIS) - Monthly Report," 63 Fed. Reg. 8659 (2-20-1998), 66 Fed. Reg. 8425 (1-31-2001), 66 Fed. Reg. 17200 (3-29-2001), 82 FR 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.88.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be***

retained (in accordance with applicable record retention schedules),

- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The privacy risks associated with information collected within RDMS primarily relate to the loss of confidentiality, integrity, and availability of data. Access by unauthorized entities to sensitive data, including personal information collected for investigation or litigation potentially could lead to destruction of that data, compromised identities, exposure of sensitive court records and personal data, and/or disruption to an ongoing investigation or litigation. ATR uses a number of proven protection methods, including secure communications (e.g., JUTNET), malicious code protection and intrusion detection software, active monitoring controls, encryption, and enhanced access control techniques designed to safeguard data in accordance with DOJ IT security standards.[4]

Additionally, all data collected within RDMS is protected by encryption and file permissions and is viewable only by authorized individuals, who must authenticate and be given direct permission for each dataset. Some data that is deemed sensitive by the appropriate authorities may be redacted to prevent unauthorized viewing and render the information unsearchable. All user activity is monitored and audited based on user actions and accesses. RDMS internal user management module manages user access and only allows users the ability retrieve data based on each user authorized role and rights at the case/matter or data level. Once authorized, users can retrieve data by searching Relativity[5] database files using a variety of parameters to include name, address, case/matter number, phone, and email.

To avoid over collection, data collected is limited to a specific case or investigation but can be collected from a variety of sources. This information is shared with only approved authorized users either through direct log on to RDMS or through other secure means, such as the Justice Enterprise File Sharing System (JEFS). ATR provides privacy notices through system of records notices (SORNS), published on DOJ's system of records website (https://www.justice.gov/opcl/doj-systems-records), and PIAs. Additionally, personnel are required to take Computer Security and Awareness Training (CSAT), which incorporates privacy.

ATR shares RDMS information on a case-by-case basis with foreign governments with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access via applicable personnel security requirements, after which ATR will provide training and grant access to approved/requested

[4] ATR adheres to DOJ continuous monitoring requirements. ATR assesses core control annually and all controls at least every three years. Furthermore, ATR adheres to the OIG schedule for routine FISMA assessment.
[5] Relativity is an ATR system used to effectively store, process, transmit and maintain critical information for the Division related to its litigation and investigation functions.

read data via a RDMS account, utilizing a GFE and/or RSA token through VPN, for direct log. The requester's access is limited to only the requested data. Foreign governments with read-only access to ATR RDMS data are partners in criminal or civil matters. The requester's access is maintained until termination is directed by the legal staff.

ATR complies with Department policies and processes designed to ensure the integrity of PII in active cases. Data is strictly controlled within the system so only data objects associated with a given case are loaded into that case repository with case-specific identification and object version control.

ATR establishes control over information contained in RDMS by strictly managing access controls, limiting permissions to only those cases that a user requires, and ensuring compliance with DOJ two-factor identification and authentication requirements. Further, privacy specific analysis and reporting is maintained within an authorized Cybersecurity Assessment and Management (CSAM) profile. The capability to generate reports from RDMS is controlled by permission and limited to authorized personnel in support of the ATR litigating mission.