Antitrust Division

Privacy Impact Assessment
for the
Antitrust Division/New York Attorney General's Office SharePoint Information Exchange (NY SharePoint)

Issued by:
Sarah Oldfield, Senior Component Official for Privacy, Antitrust Division

Approved by: Michelle Ramsden
Senior Counsel
U.S. Department of Justice

Date approved: [Component to insert date of PIA approval]

(May 2022 DOJ PIA Template)

This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or 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 (ATR) / New York Attorney General's Office (NY AG) SharePoint Information Exchange (NY SharePoint) provides a collaborative workspace hosted on the NY AG's SharePoint for co-plaintiffs in *United States, et al. v. Apple Inc.* and *United States, et al. v. Live Nation Entertainment, Inc. et al*. ATR may also use the NY AG SharePoint in connection with other cases to which both ATR and NY AG are plaintiffs within the scope of this Privacy Impact Assessment.

All information ATR shared through the NY AG SharePoint constitutes attorney work product and is shared pursuant to a common interest agreement and memorandum of understanding in the respective cases. This information may contain names and business contact information of counsel or witnesses in the cases. The work product may also contain confidential business information and PII from documents or deposition testimony provided to plaintiffs by the defendants or third parties in the cases pursuant to subpoenas, discovery requests, and court orders. The NY SharePoint will not, however, contain the underlying documents produced in discovery by the defendants or third parties, or deposition transcripts or recordings.

NY AG limits access to the NY SharePoint to personnel working on the *Apple* and *Live Nation* cases from ATR, NY AG, and the other plaintiffs. Documents maintained in NY SharePoint may be shared within the agencies as necessary, for example, with managers who would approve a court filing. Final versions of documents in the NY SharePoint may be shared with the defendants, witnesses, or their counsel, or may be submitted to the court or filed on the public docket. At the conclusion of a case, when collaboration is no longer necessary, NY AG will destroy the information in NY SharePoint. Plaintiffs may retain their work product on their respective systems.

This Privacy Impact Assessment was prepared in accordance with Section 208 of the E-Government Act of 2002 because ATR NY SharePoint collects, maintains, uses, and disseminates information in identifiable form about members of the public.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

NY SharePoint facilitates the secure exchange of information and provides a collaborative workspace for ATR and numerous co-plaintiffs in civil antitrust enforcement actions.[1] NY SharePoint serves as a central repository and allows team members to simultaneously provide feedback on documents. Documents and information exchanged and maintained in NY SharePoint are created by attorneys or at the direction of attorneys in anticipation of litigation or for trial. Draft documents and communications among plaintiffs constitute attorney work product and are not discoverable in litigation. Once a court filing or correspondence to defense counsel, for example, is finalized, the final document may be disclosed. NY SharePoint provides significant benefits over the alternative method of circulating documents back-and-forth by email.

NY SharePoint is a Software as a Service (SaaS) in the Azure Government Cloud. NY AG limits access to NY SharePoint information for each case to the ATR, NY AG, and other plaintiffs' personnel working on the case, as approved by ATR. Attorneys who have access to NY SharePoint are cleared through DOJ security. Those with access may move draft work product documents from their government systems to the NY SharePoint for collaboration and may comment on or edit documents in NY SharePoint. ATR's connected systems are ATR Cloud Computing Environment (CCE) and ATR General Support System (ATR GSS). Interconnection between ATR and NY SharePoint uses the Justice Cloud Optimized Trusted Internet Connection Service (JCOTS) cybersecurity protection stacks and SSL encryption to protect data in transit. ATR, for example, may move a document from an ATR GSS network drive to NY SharePoint, where ATR's co-plaintiffs in a case would access the document and multiple users could provide real-time feedback. Work product provided to or accessed through NY SharePoint may be retained on ATR or state information systems in accordance the protective order in the case and laws, policies, and regulations governing the handling of the information.

NY AG administrators are responsible for managing user access control, identification, and authentication; providing auditing and accountability protections; incident response; and destruction of information within NY SharePoint once a case concludes and NY SharePoint is no longer necessary for collaboration among plaintiffs.

---

[1] In *United States et al. v. Apple Inc.* the following states, the District of Columbia, and the Commonwealth of Massachusetts are plaintiffs in the First Amended Complaint: New Jersey, Arizona, California, Connecticut, Indiana, Maine, Michigan, Minnesota, Nevada, New Hampshire, New York, North Dakota, Oklahoma, Oregon, Tennessee, Vermont, Wisconsin, and Washington. In *United States et al. v. Live Nation Entertainment, Inc. et al.,* the following states, the District of Columbia, and the Commonwealths of Massachusetts, Pennsylvania, and Virginia are plaintiffs: Arizona, Arkansas, California, Colorado, Connecticut, Florida, Illinois, Maryland, Michigan, Minnesota, Nevada, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Washington, West Virginia, Wisconsin, and Wyoming.

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
Statute	
Executive Order	
Federal regulation	28 C.F.R. §§ 0.40 and 0.41
Agreement, memorandum of understanding, or other documented arrangement	Memorandums of Understanding Between United States Department of Justice Antitrust Division And State of New York; Common Interest Agreement
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 The system information processed will consist of draft briefs and other court filings, letters to the defendant, and other work product of plaintiffs. These documents may contain names and business contact information of counsel or witnesses in the Apple and Live Nation cases. Work product may contain information related to documents produced to plaintiffs by Apple, Live Nation or third parties, or deposition testimony in the case. The NY SharePoint will not, however, contain documents produced in discovery by Apple, Live Nation or third parties, or deposition transcripts or recordings.

(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 & D	
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			

(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
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	x	A, B, C & D	Employment information, such as employer, title or responsibilities
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	x	C & D	
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business 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
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	x	A, B, C & D	User IDs and access data of ATR and state AG co-plaintiff users in the *Apple and Live Nation* cases. Admin/audit data is managed by NY AG as detailed in the MOU.
- **User passwords/codes**			
- **IP address**	x	A, B, C & D	
- **Date/time of access**	x	A, B, C & D	
- **Queries run**	x	A, B, C & D	
- **Contents of files**	x	A, B, C & D	
Other (please list the type of info and describe as completely as possible):	x	A, B, C & D	Business contact information, e.g., email address, phone number, address of business

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	x	Hard copy: mail/fax	X	Online	x
Phone	x	Email	X		

Other (specify):

Government sources:					
Within the Component	x	Other DOJ Components		Other federal entities	
State, local, tribal	x	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	x	Public media, Internet	X	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			x	ATR users on the litigation team have direct access to NY SharePoint and may share documents
DOJ Components				
Federal entities				
State, local, tribal gov't entities			x	NY SharePoint hosted by NY AG and accessible by plaintiff state AG offices
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	x			Final documents in the NY SharePoint may be provided to counsel, parties, or witnesses or filed with the court in connection with the litigation

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.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for " " 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.

The information will not be released to the public for "Open Data" purposes.

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.

Individuals are provided generalized notice through this Privacy Impact Assessment and System of Records Notice 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).

Information about individuals contained in NY SharePoint documents is collected by ATR through subpoenas and discovery requests to corporations and other entities and individuals involved in the litigation. ATR is not required to provide individual notice to all whose PII is implicated.

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.

Regarding information in the system about members of the public obtained pursuant to compulsory process, individuals do not have the opportunity to decline to participate in the collection, use or dissemination of information in the system. ATR and other Federal Government personnel associated with the case may decline to participate in the collection, use, or dissemination of their information in the system.

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.

Members of the public may submit requests for access, amendment or correction to ATR's FOIA and Privacy Act Unit for processing and response. Notice of the procedures is available on ATR's public website at https://www.justice.gov/atr/antitrust-foia. ATR and other Federal Government personnel associated with the case have access to the information in the system.

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):** ATR consulted JMD OCIO regarding ATO or ATU requirements. ATR and NY AG entered into Memorandums of Understanding governing the secure exchange of information through the NY SharePoint, in accordance with NIST SP 800-47 Rev. 1, Managing the Security of Information Exchanges. Additionally, NY AG provided NIST SP 800-171 controls compliance, and based upon assessment, ATR issued an Authorization to Use**.** **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:**
	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	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Moderate
x	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The system has been assessed by ATR to verify compliance with the appliable NIST 800-171 rev2 security controls. The results of this assessment are available in JCAM.

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:**
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**. DOJ contractors support ATR GSS and ATR CCE, which will collect, contain, and disseminate information in the NY SharePoint. These contractors are subject to contractual provisions governing information security and privacy. All contractors with access to ATR GSS and ATR CCE are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role.
	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: There is no additional training specific to this system.

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 in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?*** New York state documented their compliance with the NIST SP 800-171 controls, which are tailored to provide appropriate protection for Controlled Unclassified Information and PII.

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 will be retained in the system while the litigation is pending. Once the litigation concludes, information in the system will be destroyed in accordance with the memorandum of understanding. ATR may retain certain information in other ATR information systems. Requirements governing retention and disposition of ATR documents and information are documented in ATR Directive 2710.1: "Procedures for Handling Division Documents and Information," consistent with National Archives and Records Administration regulations and records schedules.

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).

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 New York AG provided detailed compliance information to ATR documenting cybersecurity compliance. The security controls baseline used was the NIST SP 800-171 r2 security requirements, which represent a subset of the SP 800-53 controls. NIST SP 800-171 r2 security requirements only include those necessary to protect the confidentiality of Controlled Unclassified Information (CUI), and eliminates those 800-53 r5 controls that are:

-Primarily the responsibility of the Federal Government
-Not directly related to protecting the confidentiality of CUI
-Adequately addressed by other related controls, or
-Not applicable

ATR conducted a review of the submitted compliance information and documented NY SharePoint's non-compliance with the assigned security controls, which will contain any of the privacy and security risks associated with the use of this system. These will be tracked in JCAM and provided to the Authorizing Official as Plans of Action and Milestones (POAMs) as is the case with any other ATR system.

Information in the system consists of work product of Federal and State plaintiffs. These documents may incorporate information collected by the government in connection with the investigation and litigation primarily pursuant to compulsory process and to a smaller extent from voluntarily provided information. Sources of information include the defendants Apple and Live Nation, witnesses and other nonparties, and publicly available information. Information collected is relevant to the claims, defenses, and issues in the case. Information about individuals incorporated in work product is limited

to the information necessary to accomplish the purpose of the document. Privacy notices to individuals are not required or provided in these circumstances.