US Department of Justice - Civil Division

Privacy Impact Assessment
for the
Omega Web Repository System (OMEGA)

Issued by:
Angie E. Cecil

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

Date approved: September 27, 2018

EXECUTIVE SUMMARY

The Omega Web Repository System (OMEGA) is a high-availability web-based system for document retention for small projects in the Civil Division (Division). A high-availability system is a system that maintains operations through the use of redundant fault-tolerant system components and data centers. OMEGA allows projects that do not have the budget for a dedicated document management system to utilize the benefits of one without the expense of setting a system up from scratch. The OMEGA system helps attorneys or other professional staff members acquire, organize, and analyze information collected as part of civil and criminal investigations and litigation. Through the use of computer data processing, image management, and other technologies, investigation and litigation materials are effectively organized. The litigating attorneys and other professional staff can rapidly locate and make the best use of information when handling an investigation or litigation. The purpose of this Privacy Impact Assessment is to comply with the Department's requirements to document systems that contain personally identifiable information.

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:
OMEGA is a collection of e-discovery platforms (with one child system reportable under the Federal Information Security Modernization Act (FISMA) – see 1(h) below) maintained by the Civil Division which is used to effectively store, process, transmit, and maintain information for investigations and litigation conducted by the Division. The information maintained in the system is collected from client agencies, opposing parties, or other entities involved in a particular matter in response to document requests or subpoenas. The information is used as part of the Civil Division's investigative and litigation functions. The system is maintained by CACI, a government contractor.

b) The way the system operates to achieve the purpose(s):
The system is used as an online web-based repository and application-hosting environment. The applications and tools within the OMEGA system help attorneys or other professional staff

acquire, organize, and analyze evidence. It consists of web-based e-Discovery applications and support systems tied to backend databases and data stores. The databases include Microsoft SQL, Oracle, MySQL or other database management systems for tracking/holding document records and to facilitate searching for documents. The data is stored on a centralized storage area network (SAN) solution. Applications hosted typically contain records which contain metadata stored in the database which also have links to files stored on the SAN.

c) The type of information collected, maintained, used, or disseminated by the system:
All information collected, maintained, used, or disseminated by the system is used in an effort to support the Division's litigation and investigation functions through discovery. The information collected and stored on OMEGA consists of factual case documents obtained through discovery. Depending upon the nature of the case or matter, the information may include names, addresses, telephone numbers and other personal information for individuals and entities from numerous sources. The Division obtains the information through the discovery process or subpoenas. The individuals may be a party to, or the subject of, DOJ litigating activities or investigations. The information will vary based upon the nature of the investigation and the documents provided via the discovery or subpoena activities.

d) Who has access to information in the system:
All access to the system is tightly controlled by contract stipulations, DOJ security standards, and FISMA requirements. Once these requirements are met, access may be granted to any individual working on the matter, including Division attorneys, paralegals, agency counsel, expert witnesses, or other authorized individuals involved in reviewing information collected in the course of the investigation or litigation. Civil Division employees, contractors, and other authorized users are only granted access to databases on the system that support a matter they are working on. If an authorized user leaves the organization or is reassigned to other matters, the account access is disabled or access to a particular database may be rescinded.

e) How information in the system is retrieved by the user:
If the user is granted access to the system, information is retrieved via user-generated queries to the system. Users can construct full-text queries, in which the system(s) searches through the full-text indices to locate data to search for personal identifiers utilizing the applications' user interfaces. The system(s) search through the dtSearch component within OMEGA and full-text indices to locate data. Users may search for patterns of data via the advanced full-text search.

f) How information is transmitted to and from the system:
Information is transmitted to and from the system via industry standard HTTPS encryption protocols and requires multi-factor authentication. The Department of Justice has developed a managed process to ensure its automated systems' security programs are current with revisions and releases of applicable Federal standards. This is complimented by activities designed to ensure system patches and fixes are fully current, and security configuration polices are not compromised. Information is transferred to OMEGA after it is provided to the Civil Division on USB drives, CDs, DVDs, and other electronic deliveries via approved SFTP/File Transfer solutions.

g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):
This system is the parent system that interconnects with the Omega Relativity Content Analytics (ORCA) system and is reportable under FISMA.

h) Whether it is a general support system, major application, or other type of system:
OMEGA is a General Support System and its FISMA child, Omega Relativity Content Analytics System (ORCA), is a Major 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 Registmration	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	

Distinguishing features/Biometrics					
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	
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		Online	
Telephone	X	Email	X		
Other (specify): Documents are obtained through litigation discovery and production, the processes by which parties to a lawsuit, hearing or other legal proceeding are required to exchange documents pertinent to the case at hand.					

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

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers					
Other (specify): Documents are obtained through litigation discovery and production, the processes by which parties to a lawsuit, hearing or other legal proceeding are required to exchange documents pertinent to the case at hand.					

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.)

[Data is 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.

The system is also configured with multi-factor authentication. This requires all authorized end users to provide two levels of authentication prior to accessing any data hosted on the system. Users may also request access to multiple databases, and are required to go through the request process for each database they wish to be authorized to access. The system is configured to ensure that access to a specific database and its content is restricted to only those users that have authorized access. The system is also monitored and audited to identify any unauthorized access attempts and to verify that the appropriate access levels have been granted to its users. The system is hosted behind security firewalls and intrusion detection systems. All sites are also encrypted using secure protocols (e.g., Secure Sockets Layer (SSL) and Hypertext Transfer Protocol Secure (HTTPS)). These procedures are designed to protect all data transmissions from compromise.]

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
[ ]	For intelligence activities	[ ]	For administrative matters
[X]	To conduct analysis concerning subjects of investigative or other interest	[ ]	To promote information sharing initiatives
[ ]	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; link analysis relevant to litigation or investigation; and selecting and preparing exhibits for trial. Collection, maintenance, and use of the information supports the Civil Division's litigation and administrative functions.]

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 – Civil Division Federal Rules of Civil Procedure]
[X]	Memorandum of Understanding/agreement	[Federal Trade Commission (FTC)]
[X]	Other (summarize and provide copy of relevant portion)	[MEGA 4 Contract – DOJ Contract # DJJ13-C-2439]

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 Civil Division case attorney and the Office of Litigation Support determine that the litigation materials no longer need to be stored on 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 pursuant to the Division's obligations under the Federal Records Act. Records that must be maintained will be retained in accordance with the applicable retention schedule. When closing or settling a case, or archiving case information, and removing it from the system, the data is saved to an external hard drive or other media and provided to the attorney closing the case. The data is then deleted from OMEGA, and the space previously used by the case is re-used (deleted, then made

available elsewhere). Data will be finally disposed of after consultation with the case attorney. After the data is disposed of, no additional copies of the data are retained in this system or elsewhere.

Files managed on OMEGA may include both federal records and non-records that are associated with a variety of different types of Civil Division 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 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. 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.

In addition to these protections, all disk volumes and backup tapes containing PII or Sensitive But Unclassified information (SBU) are encrypted via a hardware-based FIPS 140-2 encryption mechanisms. In addition, OMEGA employs intrusion detection and prevention systems to detect and prevent potential malicious activity, changes to the network, and traffic anomalies. Further, OMEGA backs up data regularly and controls access to data stored on the application. Frequent network and system vulnerability scanning are designed to ensure all vulnerabilities and associated risks are addressed and mitigated in a timely manner. A combination of access, logical, and technical controls provides a robust suite of policies, procedures, and technology designed to ensure that PII and other SBU are protected at all points in the OMEGA 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]	[ ]
DOJ components	[X]	[ ]	[X]	[ ]
Federal entities	[X]	[ ]	[X]	[ ]
State, local, tribal gov't entities	[X]	[ ]	[X]	[ ]
Public	[ ]	[ ]	[ ]	[Some information collected and used for Civil Division investigations and litigation becomes public through court proceedings, pursuant to court rules, orders, and procedures.
Private sector	[ ]	[ ]	[X]	[Contractors to the Department; other parties and individuals involved in investigations and litigation, pursuant to court rules, orders, and procedures.]

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
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.)

Security protections that authorize and limit a user's access to information within the system mitigate the risks to privacy when information is shared within the Division and outside the Division. Unauthorized physical access to OMEGA is limited by physical controls such as secured entrances and security officers protect access to the building where the servers and workstations are located. The data maintained by OMEGA 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 PIV card entry and role-based access controls. In addition, before a user is granted access to an application hosted on OMEGA, 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 accounts. For data in transit, the Civil Division utilizes Department-approved encryption technology and PII filtration for email services. 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 investigators from another component or agency, partners at the United States Attorney's Office, or expert witnesses. There are monitoring and auditing tools for each system to review user activity, so the Civil Division can monitor user access within the system. The Civil Division follows DOJ internal policies and procedures for unauthorized access or release of information from the system. The process for establishing and reviewing accounts includes application and monitoring of initial distribution of accounts. Credentials are controlled according to DOJ and NIST standards. The controls include password management, including password composition, history, complexity, and changes. The processes also include monitoring account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review, all of

which support implementation of need-to-know requirements. Additionally, the processes include monitoring of access privileges monthly, to further enforce need-to-know. When a user account is created, the account is provided the least possible privileges for the user to perform tasks related to the investigation and litigation activities. OMEGA logs and tracks unsuccessful logins and automatically locks the account when the maximum number of consecutive unsuccessful attempts are exceeded. A system administrator must be called to unlock the account. The system also forces re-authentication after the specified period of inactivity. For users who access OMEGA outside of a DOJ facility, remote access via Virtual Private Network is controlled and monitored. Encryption is used to protect the confidentiality of remote access sessions and secure remote access tokens are implemented to authorize and control access. Remote users are presented with Department policies regarding authorized use before login each time they are required to authenticate or re-authenticate.

Audit trails are generated by OMEGA. The audit trails detect intrusion and are used to identify data misuse. OMEGA also is configured to protect audit information and tools from unauthorized access, modification and deletion. The intrusion detection audit trails are reviewed on a weekly basis, or when an incident is suspected. The application audit trails are reviewed on an as-needed basis. In addition, OMEGA employs an intrusion detection system to detect vulnerabilities, changes to the network and traffic anomalies. Further, OMEGA backs up data regularly and controls access to data stored on the Application.]

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, but that challenge would be determined before the

		information is collected and maintained by OMEGA. 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: Individuals do not have the ability to consent to the collection of documents and uses that are obtained through court order, warrant, subpoena, discovery requests, and other such legal means. An opposing party may, however, challenge the use of this information pursuant to the rules of evidence.

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 OMEGA. 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: [6/2/2016] 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: [Completed FISMA Moderate risk evaluation via 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: [Completed DOJ Security Authorization, and continuously monitor applications and web sites for misuse.]	
[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: [This system satisfies the Audit and Accountability (AU) controls outlined by NIST 800-53A-Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, including formalized Audit and Accountability Policies and Procedures, technical controls, and role-based privilege separation. All approved policies, procedures, standards, and program plans fully meet the requirements of FISMA.]	
[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.

[All policies, procedures, standards and program plans for the OMEGA system fully meet the security policies and requirements of the Department of Justice and the Federal Information Security Modernization Act. Relevant procedural documents are created when needed. DOJ defines the frequency of reviews and updates for security documents via the DOJ Security and Privacy Assessment and Authorization Handbook. DOJ Core Controls are assessed annually. Key information security controls employed to assure information is handled in accordance with its prescribed use including strong authentication requirements (multi-factor authentication), centralized security event management, and FIPS 140-2 validated strong encryption.]

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-00,1 *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 specifically pertaining to US citizens and/or lawfully admitted permanent resident aliens can be retrieved from the system, but is handled in strict accordance with all Federal regulations regarding PII and SBU material. OMEGA offers a variety of retrieval solutions, which generally allow a full-text or fielded search on document data and metadata collected (e.g., date sent, from, to, cc, as collected or produced via the discovery protocols). A full-text search uses the database's index to quickly sift through every word (of every record) that can be entered in the database. The user can search and retrieve a list of documents and then view the documents found by the search.]