



iCONNECT

---

# DECIDING WHETHER YOU NEED AN eDISCOVERY CLOUD OR ISLAND?

---

SECURITY ANALYSIS ON THE RIGHT  
SOLUTION FOR YOU

WRITTEN BY JOSHUA GILLILAND, ESQ.



# PRIVACY LAWS PROTECTING

---

Cloud computing has leveled the playing field between large organizations and small law firms. It is now possible for a firm of four attorneys to litigate with a multinational corporation represented by a mega-firm with an army of lawyers.

There is no question there are many advantages to cloud computing eDiscovery applications.

However, there are situations where the data is highly sensitive, either by the nature of the information or security requirements, where an eDiscovery solution is required behind an organization's firewall. This is when the data requires an eDiscovery Island and not a cloud.

## DEFINED eDISCOVERY

### CLOUD

---

Refers to an ambiguous location of data or documents and the review software that allows access to those documents. Although some cloud providers can apply geographic restrictions to the hosting, backup and access, most cloud providers use a network of computers around the world to optimize and scale. Typically, unless additional fees are charged, data and documents are co-mingled on the same computers and networks as other data and documents. This generic approach does not compromise security of the information. Instead, it optimizes the infrastructure usage such that each client of the system gets the benefit of shared resources. Although clients can typically perform tasks such as setup, security, and data import/export, administrative tasks such as operating system updates, CPU or worker configuration and the running of scripts is typically not allowed and the limited geographic restrictions may be problematic for some projects.

## DEFINED eDISCOVERY

### ISLAND

---

Refers to the geographic and infrastructure location of the e-discovery servers that host the data and documents, and the review software used to access those documents. Many firms already have hardware running their accounting, docketing or file management internally within the office or at a leased data center location dedicated to that firm. The addition of eDiscovery review data and servers simply becomes an extension of that hardware giving full administrative control over the system. Companies can then work directly with their own Information Technology (IT) staff to optimize all aspects of the system. Further, clients get the benefit of potentially integrating their e-discovery review system with other software programs via direct connection, scripts or API (Application Programming Interface).



## ISLAND EXAMPLES

---

Below are two examples of high-profile and complex projects that required an island deployment. In both cases the concept of using a generic cloud environment was not enough to satisfy the needs of the project.



An Intellectual Property (IP) dispute between the manufacturers of electric vehicle batteries required proprietary data to be secured and reviewed on an eDiscovery island. The sensitivity of the Intellectual Property (IP) and international government involvement in the documents required restricted access and control. Furthermore, 95% of the documents were in Korean and required searching in sync with English language searches.

The eDiscovery service provider created stringent security parameters to fully control access to the confidential 5.8 Terabytes of data that incorporated multi-factor authentication, intrusion detection logging, print/download restrictions and locked down physical computer access.

The project managers employed a step-by-step process to review the data set within a limited time frame. The primary language of each document was identified and segmented for native-speaking reviewers.

### **The workflow included:**

- Indexed Search
- Sharing of Results
- Identification of Hot Documents
- Ai (Conceptual Search)
- Email Threading Analysis
- High Volume Productions
- Multiple Security Layers

The review further leveraged predictive coding to identify documents to support the plaintiff's case, resulting in a settlement of \$1.8 billion.

*The iCONNECT platform was used to achieve project goals.*



The decades-long legal drama between Ecuador and Chevron is one example of an eDiscovery island being necessary for the litigation. The litigation went from Ecuador to the United States and then Canada. The brief history is that Texaco was accused of spilling crude oil in the 1970s and 1980s in Ecuador resulting in significant environmental impact. Texaco was eventually acquired by Chevron.

Over protests that the judgment was acquired through fraud, bribery, and allegations that the state-owned oil company was at fault, a \$19 billion judgment was entered against Chevron in Ecuador. The judgment was reduced to \$9.5 billion. The Ecuadorians attempted to secure the judgment against Chevron in the United States with the Alien Tort Statute.

After failing to enforce the judgment in the United States, the plaintiffs attempted to secure the judgment against Chevron Canada. The lawsuit's data was physically moved from the United States to Canada for the duration of the Canadian lawsuit. A cloud solution was not an option for the multi-national litigation.

The plaintiffs would ultimately lose, because Canadian courts held that the assets of Chevron Canada belonged to a separate legal entity that could not be used to satisfy a judgment against its parent corporation.

*The iCONNECT platform was used to achieve project goals.*

# THE VALUE OF AN eDISCOVERY ISLAND

---

Just as top secret documents don't belong in the basement of a beach house, there are some records too sensitive to be held in a cloud. In these cases, a locally installed solution or island can solve the security needs of highly sensitive data.

## RFP AND RFI CONSIDERATIONS

---

Consider these elements that may be included in a request for proposal (RFP), request for information (RFI) or project outline that all point to the benefits of an eDiscovery Island:

- **SECURITY:** Must integrate with a client's Microsoft Active Directory and Active Directory Groups
- **POLICIES:** If all security and access policies must apply to the review system including corporate Password requirements and maintenance policies
- **INTEGRATION:** Needs to integrate via API with in-house systems for interplay with 3rd party content
- **HARDWARE REQUIREMENTS:** Requires direct access to hardware such that specifications and maintenance continue/are adhered to as per current policy
- **OPERATING SYSTEM REQUIREMENTS:** Management of OS (operating system), virus scanning, and backups must adhere to current policy
- **MULTI-FACTOR AUTHENTICATION:** Requires use of MFA (multi-factor authentication), VPN or other additional security requirements
- **COUNTRY JURISDICTION:** Jurisdiction of hosted data must be known and controlled, including backups
- **CONFIDENTIALITY:** Restricted by data content, privacy, confidentiality, intellectual property or client preference
- **CONSISTENCY:** Client may already be using a cloud system and may want to minimize training by deploying the same system in-house
- **DATA/DOCUMENT MANAGEMENT:** Data loading must be done locally (not via shipping or upload)
- **VOLUME/LONGEVITY:** An individual project or multiple projects may make it cost effective to run a system in-house
- **IMPORT/EXPORT:** Full control of data chain of custody for both import and export of data

Make sure to ask all the right questions of your provider as many e-discovery companies do NOT offer the option for clients to operate their software on an island. These 'cloud only' providers have a solid offering, however, make sure to ask questions and look for alternative platform if a project requires specialized handling, infrastructure or geographic location.

Further, if an island deployment is selected, it's important to check with your provider to ensure that the 'island' version of the software contains the same feature set as the 'cloud' version and that future support of the island system is part of the long term company support strategy.

## ABOUT iCONNECT

iCONNECT Development, LLC develops the innovative iCONNECT eDiscovery review software platform. iCONNECT raises the bar by delivering intelligent, easy-to-use tools that help hosting providers, law firms, and legal departments optimize workflows and manage some of the world's most complex legal cases more efficiently. Leading AI and auto-redaction capabilities combined with a user's ability to search, sort, analyze, categorize and produce documents and multi-media files recently led industry publication 'Silicon Review' to name iCONNECT as one of the '30 Fastest Growing Tech Companies' of the year.



---

## ABOUT THE AUTHOR

### **Joshua Gilliland**

Twitter: @bowtielaw  
Josh@bowtielaw.com

Joshua Gilliland is a California attorney and creator of the eDiscovery blog Bow Tie Law and has presented at over 400 eDiscovery seminars and webinars. Josh is co-creator of The Legal Geeks blog and podcast, which has made the ABA Journal as one of the top 100 blogs for lawyers from 2013 to 2018. Josh grew up in Silicon Valley and is a graduate of UC Davis with a degree in Political Science and earned his law degree from McGeorge School of Law, University of the Pacific. Josh enjoys organizing panels and mock trials at comic conventions, photography, and volunteering in Scouting.

**FIND  
OUT  
MORE**

Contact iCONNECT for more information.  
[www.iconect.com](http://www.iconect.com) | [info@iconect.com](mailto:info@iconect.com) | 1-855-915-8888

Copyright© 2022 iCONNECT Development, LLC. All rights reserved. iCONNECT is a registered trademarks of iCONNECT Development, LLC.