Planning for E-Discovery in the Cloud

Francoise Gilbert, JD, CIPP/US
About the Author

Francoise Gilbert, JD, CIPP/US, focuses her legal practice on information privacy and security, cloud computing, and data governance. She was voted one of the country’s top legal advisors on privacy matters in a recent industry survey and, for several years, has been recognized by Chambers, Best Lawyers, and Ethisphere as a leading lawyer in the field of information privacy and security. Gilbert is the author and editor of the two-volume treatise Global Privacy & Security Law (2,900 pages; Aspen Publishers, Wolters Kluwer Law and Business) (www.globalprivacybook.com), which analyzes the data protection laws of 65 countries on all continents.

She is the managing attorney of the IT Law Group (www.itlawgroup.com) and serves as the general counsel of the Cloud Security Alliance. She also keeps a blog on domestic and international data privacy and security issues (www.francoisegilbert.com).
Does your cloud strategy take into account the fact that your company may be sued or may need to initiate litigation against a third party, and may have to comply with rules regarding the protection and provision of evidence?

Unique rules apply to documents and records when a dispute arises and there is a threat of litigation, or a complaint has been filed and served. This complex process involves many aspects, including, for example, preservation of evidence (so evidence necessary for trial is not destroyed), identification of evidence that is relevant to the case, and delivery of this material to the other party in a form and format that is useable. When this evidence is in electronic form, the plaintiff (or potential plaintiff) and the defendant (or potential defendant) must follow stringent rules imposed by the e-discovery provisions of the Federal Rules of Civil Procedure and state laws.

When these electronic documents have been stored with a cloud service provider, additional complexity arises because the data owner no longer has full control over its documents. It must find a way to make the cloud service provider cooperate on e-discovery cloud issues. This article examines some key considerations in preparing for a discovery request in the cloud.

Preservation of evidence

The law imposes on the parties to a dispute a duty to preserve information that may become evidence in a lawsuit. Failure to implement a “litigation hold” carries significant legal consequences. A litigation hold is the process by which information is identified, preserved and maintained. It is intended to ensure evidence, when needed, will be available. Thus, anything that may result in hampering the discovery process or the production of evidence will expose your company to significant risks of adverse action by a judge.

Courts have imposed hefty sanctions on litigants that have failed to adequately preserve their data or organize the proper litigation hold. A case may be dismissed in whole or in part, or the jury may be instructed to assume that the missing or unavailable evidence was in favor of the other party.

There have also been sanctions when parties did preserve the evidence, but transferred it to a less accessible format that made it more costly and time consuming to retrieve. The litigant may be required to bear the cost of recovering the data, assessed substantial monetary penalties, and/or required to pay attorney fees.

Thus, it is important to prepare adequately for the eventual need to initiate a litigation hold and preserve the needed evidence. In a cloud setting, where the cloud provider may have its own constraints, ways of operating and other obligations, the preservation of evidence reaches a higher level of complexity.

Identification of data custodians and data segregation

It will be necessary to identify the data that may be required in a dispute and the likely custodians of the data. For example, while some of the data may be located with your primary cloud service provider, back up or archives may be stored with a different cloud service provider. Make sure you have up-to-date data maps in place that identify the specific custodians of the different types of files.
Once you have identified the specific data within the scope of the litigation hold, it may be complex or cumbersome for you and your cloud service provider to segregate the material to be preserved from data that is not subject to the litigation hold. How would you and your cloud service provider proceed to segregate the required data? Would it be easier or more efficient to preserve more than the information pertaining to the dispute in order to limit the time spent parsing the relevant data? Consider also preparing in advance for the need to launch a litigation hold, and ensure files are organized and segregated in a manner that allows the parsing to be done more efficiently.

Storage duration and cost

It may be that the duration of the preservation requirement is longer than the terms of the cloud service agreement. What would happen to the data if your contract with the cloud provider expires before the end of the required retention period?

Would it be better to make a copy of the data or application at a certain time, and retain this copy outside the cloud? In this case, if you take the data out of the cloud, will it be in a format such that the data can be searched as needed? Would you also need a copy of the software applications necessary to process the data? It may be necessary or useful to work -- in advance -- with the cloud service provider to identify the storage method and format that is most appropriate under the circumstances.

When you negotiate a cloud services agreement, you should both ensure that your cloud provider will cooperate with you if you need to implement a litigation hold, and understand the cost associated with it. Ask what may be involved, and what will be charged in addition to the mere cost of storage. Will there be administrative fees? Will there be professional service fees for retrieving the data? Be aware that preservation might require the storage of large volumes of data for extended periods, and that the related cost might be significant.

Planning ahead

Putting in place a plan of action for cloud e-discovery by carefully planning for the tools, capabilities, or functionalities that you will need and identifying the players with whom you will interact to obtain documents or evidence will simplify and ease the painful and time-consuming tasks of document or evidence gathering.

Cloud e-discovery: data access

The conditions for access to the data should be set forth in the Service Level Agreement (SLA) with the cloud service provider. There may be restrictions or limits on the volume of data that is accessible. The SLA may limit the ability to collect large amount of data quickly and in a forensically sound manner, so that the related metadata are preserved. You should investigate these issues early, and agree ahead of time with the cloud service provider on the feasibility of this access and the procedure to follow. You should also understand the administrative and other costs, as well as the time frame for performing these tasks.

The investigation or collection of evidence is likely to require that large amount of data be downloaded from the cloud site. Check your cloud service provider’s capabilities in this area ahead of time. Due to the volume of data,
this download may require a significant amount of time, so large that attempting to download information would be impossible or take days and a lot of patience. This would be the case for a site that, for security, technical or other reasons, only allows users to download small volumes of data. This limitation could be a significant issue and cause major delays or hurdles in the collection of the information. You should ensure that you understand whether it will be possible to bypass this restriction to download the relevant data or whether it will be necessary to seek special services from the cloud provider. If special services are needed, expect additional fees.

Data searches, quality and integrity

It will be critical to have the ability to perform complex, granular searches to limit the collected documents to those that are relevant to the subject matter of the search or investigation. Find out what search tools the host provides and how efficient they are. You may want to experiment ahead of time with the search capabilities that are directly available to you, and investigate whether other tools should or can be used, where they are located, how to get access to them.

In addition, it will be necessary to ensure the integrity of the data, especially in the case of litigation. That is, you must be able to prove that the data are accurate, and have not been modified. What assistance and methodology will the cloud provider be able to furnish to ensure that the data have not been modified? How will you be able to assure the judge and litigants of the integrity and accuracy of this information?

Cloud e-discovery: Whom to Call

An investigation or the collection of evidence will be less painful and more efficient if you have established in advance a procedure for conducting the investigation, know whom to call and what to ask. When a problem, a dispute or a complaint hits the desk of the CISO, CPO or General Counsel of a company, it is too late to try to figure out what to do. Having established lines and methods of communications will be extremely useful. Having a process in place will be even more useful if the cloud service agreement was not negotiated, and the services were obtained through the mere clicking of an “I-agree” button online.

Conclusion

Companies must account for the need to preserve evidence in their cloud strategy and weigh e-discovery issues and cost in their due diligence, contract negotiation, back-up and archival routine, and performance monitoring for their data held in one or several clouds.

The ease of access and ease of use of most cloud computing offerings hide or mask the complexity of the engines, applications and structures that make the machine run and operate. When a company must review, analyze and download large amounts of relevant data in a short time, the cloud can be a hindrance if there has been little preparation.

Whether or not you operate in the cloud under a negotiated agreement, it is important to prepare for the day when there is an investigation of the causes for a dispute, and you have a short time to access the relevant data.
If you put in place ahead of time the related safeguards, policies, agreements or tools, responding to a request for documents will be much easier.

* * * * * * *

This article was first published by SearchCloudSecurity.com