Discovia™
Discover Smarter

415.392.2900 | info@discovia.com

10 Best Practices for eDiscovery in Government Investigations

By: Amy W. Ray and John Del Piero

The arrival of a government subpoena on the doorstep of your corporate headquarters rarely rates as a welcome development. Yet, the fallout is far worse without a plan in place to manage document discovery throughout the ensuing government investigation.

"The Department of Justice is very serious about prosecuting cases where there is destruction of evidence," said John Haried, Criminal eDiscovery Coordinator and eDiscovery working group co-chair for the Executive Office of United States Attorneys in the DOJ. Failure to adhere to eDiscovery legal requirements and responsibilities while a government investigation is underway can trigger a wide range of sanctions, including spoliation of evidence and adverse inferences drawn therefrom.

Based on experience providing eDiscovery management for responses to government investigations – involving data collections by Discovia on five continents and in 22 countries – we have assembled a list of 10 best practices for effective eDiscovery management during federal investigations.

1. Map the data landscape

Government requests often can be extremely broad, necessitating informed negotiating strategies to limit the scope and ease the burden of eDiscovery. Before proposing subpoena modifications, consult your eDiscovery service provider. They may have thoughts as to whether a strategically narrowed scope of eDiscovery is both fair and feasible.

Focusing on your proposed eDiscovery parameters, next ensure that you understand the underlying data landscape. Are your company's emails automatically archived? Do you use cloud servers or on-premises servers? What types of electronic communications platforms do your employees use? In order to effectively support eDiscovery efforts required to respond to a government subpoena, it is essential that all members of the team – in-house counsel, outside counsel and eDiscovery service providers – are on the same page with respect to where the data resides in the corporate IT landscape.

2. Establish collection goals

Once everyone is clear on where the data can be found, it is time to identify specific goals and milestone deadlines for the anticipated data collection. Address all custodian and non-custodian sources to be collected and strategize as to how targeted your collection efforts will be. Taking these steps up front will enable your eDiscovery experts to suggest the most cost-effective and defensible collections workflows for each data source.

Also, be prepared for the reality that data collection strategies in government investigations tend to differ from those used in commercial litigation matters. For example, government agencies are more likely to leave the duration of an investigation open-ended, placing you in the position of preserving information for a long period of time and potentially returning to collect new data down the road.

3. Respect data privacy laws

Direct outside counsel to work closely with your eDiscovery service provider in evaluating how relevant privacy laws (international, national, state, local, etc.) might impact the eDiscovery process. For example, many providers previously were certified under the U.S. Department of Commerce's Safe Harbor program in order to fulfill privacy requirements specific to the EU. Today, you need to ensure that your team is in compliance with the new EU-US Privacy Shield standard.

A best practice is to facilitate conversations with your outside counsel and eDiscovery service provider that focus on the jurisdiction(s) in question. Collectively, you can assess privacy requirements that can impact the data collection workflow. Foremost, it is essential that your team strictly complies with relevant data privacy laws, such as the process used to transport privacy-restricted data between locations from which it is collected and processed.

4. Strategic on-site and remote collections

On-site collection for physical media is optimal because it offers maximum certainty and legal defensibility, as well as minimizes participation by your corporate IT team. The top eDiscovery service providers have dedicated teams that are in place for this exact purpose. For example, Discovia maintains a 16-person, full-time collections team that respects clients' business needs by collecting on-site during or after normal business hours or on weekends.

There will be some situations, however, where it is either impossible or impractical to deploy an on-site team within your budget and/or deadline. In those instances, a cost-effective alternative is to work with your eDiscovery service provider to conduct a remote data collection. This process typically involves the shipment of forensically prepared hard drives to data custodians anywhere in the world, then using those drives to perform the collection and documentation with the aid of pre-configured, encrypted software tools.

The government may also request sources that are not considered within the "possession or control" of the corporation, such as: Amazon S3, Box, Dropbox, Gmail, Google Apps for Business, HP Helion, Microsoft Azure, Office 365 Email, Office 365 OneDrive, Office 365 SharePoint, Rackspace Cloud Files, SharePoint, etc. These sources do not need to be collected on-site as they do not physically reside with the company. The collections professionals will be able to access and forensically preserve these datatypes remotely.

5. Maintain quality control

While under the shadow of a potential federal enforcement action, it is crucial to have sound quality control procedures to shore up the defensibility of your collections. Wherever it is technically feasible, your team should collect data sources into evidence containers that are validated with the use of MD5 hash values. Another best practice is to assess disk images for encryption so that stored data can both be protected and accessed.

For email collections, conduct quality control checks on specific metrics such as item counts, first message readability, last message readability, etc. Also, your team should store all collected data in a redundant environment to protect against data loss due to failure of the primary media device. In addition, document your data collection activities in a chain of custody form that details the data source, the physical description of media onto which data is transferred, as well as steps taken in the collections workflow.

6. Early data assessment

With initial collection complete, modern software tools can help reduce the database volume a more manageable size for processing and review. By applying sophisticated filtering tools in the earliest stages of the data assessment, your eDiscovery team can "cull" irrelevant or redundant documents.

Examples of these early data assessment tools include: email threading, duplicate detection, content clustering and conceptual search. These tools enable your team to optimize the document evaluation and review process in less time and at a materially lower cost.

7. Application of Technology Assisted Review

The largest cost element in eDiscovery is attorney review and selection of records for production and/or privilege. These costs can be especially staggering during a government investigation if the lawyers conduct a one-to-one review of every record that potentially will be produced. Technology Assisted Review (TAR) is a process that applies review decisions from examined sample records to records that have yet to be individually examined. TAR has the potential to be a powerful addition to the eDiscovery workflow during government investigations.

To best apply TAR, determine the most qualified in-house and/or law firm attorney team members to train the system. Those practitioners must have knowledge of the facts and arguments at issue in order to review document samples attentively and calibrate the TAR system in a way that will be efficient and defensible.

While TAR is not a good fit for every review, many government attorneys are enthusiastic about the efficiencies it can bring to the eDiscovery process. If your team agrees TAR can increase the efficiency and effectiveness of the review process in your case, aim to obtain government buy-in early on and keep investigating attorneys apprised as your TAR process progresses.

8. Secure data transfer

Now that your team has undertaken data collection and processing in a forensically sound and legally defensible manner, ensure that you transfer the electronic information for review just as carefully as it was obtained. Ask your eDiscovery service provider to establish an FTP service that will allow in-house and outside counsel to post, download and process the data in a highly secure online environment.

You should ensure that you have strict login credential requirements coupled with randomly generated passwords to protect against cyber intruders. Because the standard FTP protocol does not provide a premium level of information security, consider engaging a service provider that offers secure FTP with a higher level of encryption.

9. Robust hosting platform

Do not assume that all hosting platforms are equal, especially given the heightened scrutiny and high stakes often present in government investigations. You should seek a hosting platform that has best of breed security. For example, Discovia uses kCura's Relativity as the primary hosting platform and houses clients' data in redundant SOC 2, Type II-audited secure data centers.

At the same time, you want to utilize a hosting platform that facilitates attorney review, both in terms of ease of access and speed. Consult your eDiscovery service provider to develop innovative review workflows that will maximize efficiencies, such as repurposing coding across investigations that involve similar documents or creating protocols that allow for access by multiple authorized users at once.

10. Smart production protocols

Lastly, adhere to strict protocols for production that ensure you meet relevant deadlines and produce in the appropriate, government-specified format (e.g., TIFF, Native, Hybrid). If questions arise regarding redaction and privilege log requirements, consult with all members of the team to arrive at a defensible protocol. At all times, keep focus on your accuracy rate so you can make adjustments to the review protocol if needed.

To avoid waiving privilege and other protections – especially in an era when the government is scrutinizing "clawback" requests – implement specific quality-control protocols prior to production. For instance, consider running searches for: the names of all attorneys involved, phrases such as "privileged" or "confidential" or even keywords such as "ACP" or "ask legal." This back-end privilege check will reduce your risk of accidental disclosures to the government. Moreover, in the event of unintended disclosure, such protocols will support your clawback arguments by demonstrating that you were diligent in performing pre-production checks on potentially privileged documents.

It is never a good day when a government subpoena is served on your company, but an effective eDiscovery management plan can ease your burdens and allow you to focus on the advocacy necessary to defend a government investigation.

About the Authors

Amy W. Ray is a Partner at Cadwalader, Wickersham & Taft LLP. Cadwalader's Antitrust team advises clients and serves as counsel in connection with complex antitrust issues, including transactions, investigations and litigation. Cadwalader's attorneys focus on formulating practical and creative solutions that are designed to assist clients in achieving their business objectives, while at the same time minimizing litigation risk. Cadwalader's Antitrust team regularly assists clients in developing and administering antitrust compliance programs as well as advises clients on distribution, purchasing and R&D arrangements, pricing and standard-setting, and trade association and IP licensing matters.

John Del Piero is a Vice President at Discovia. Discovia is uniquely qualified to meet the eDiscovery needs of corporations that are facing government investigations. Discovia offers: a strategic understanding of data collections, forensics and processing; experience with data security and privacy compliance requirements; commitment to excellence in the context of government investigations; a deep bench of accomplished professionals that deliver services to in-house legal teams and law firms; and competitive pricing that produces cost savings for corporate legal departments.