

Seven steps to working successfully with e-discovery and forensic service companies

Peg Duncan, Director, Business Opportunities and Emerging Technologies, Department of Justice Canada¹

The Seven Steps follows the process from identification of requirements through finding a vendor partner through working with that partner to preserve, collect, process and produce the data and documents relevant to the case. The focus of the steps is on two key principles:

- Preservation of documents and data that may be relevant to the issues
- Defensibility of the process

Although conceived for dealing with e-discovery and forensic companies, the same steps could be used for establishing a contract with a legal outsourcing firm for document review.

Seven Steps

[*Step One – establishing what needs to be preserved and collected*](#)

[*Step Two – assessing the complexity and volume in consultation with IT and Records Management units*](#)

[*Step Three – what outside support services do you need?*](#)

[*Step Four – writing a Statement of Work*](#)

[*Step Five – evaluating the vendors*](#)

[*Step Six – building the project team – roles and responsibilities*](#)

[*Step Seven – managing the process*](#)

Step One – establishing what needs to be preserved and collected

As with all discovery projects, it depends on what you are looking for.

- Names of individuals involved in the events
- Specific details of the events
- Locations where the events happened
- Specific dates, or a range of dates

In the case of a large corporation, focusing the scope avoids disturbing offices that have no knowledge of or role in the alleged events. The corporation can identify custodians who may have information, and the search can be narrowed to the set of devices used by the custodians throughout the period at the specified locations.

Dates are important for a number of reasons. Documents, emails, data files and other communications relevant to events that took place over 5 years ago may no longer be

¹ The opinions expressed in this article are those of the author and do not necessarily reflect the views of the Department of Justice Canada or any other agency of the Government of Canada.

stored in active files on the networks, workstations, laptops and servers used by the custodians. Some of the custodians may also have moved to new positions in the company, or have left entirely. If the evidence exists, it will be in digital archives or, if the company retains them, in backup tapes from that period. In addition to being more difficult to find, older information may be more difficult to retrieve owing to changes in technology.

Step Two – assessing the complexity and volume in consultation with IT and Records Management units

Ninety-three per cent of all information is electronic, and of that, less than 30% is ever printed. With the almost universal use of electronic mail for business communications and the growth in use of Blackberries, Personal Digital Assistants and Instant Messaging, at least some if not most of the critical information will be electronic.

IT and Records can help you determine how complex the collection and processing of the information will be.

- What email system is in use, or was in use at the time? Were there email inbox restrictions in effect and was older mail archived or deleted? Are (were?) emails considered part of the corporate records and managed through their life cycle? Does the corporation communicate and strictly enforce email management policies?
- Are personal email archives permitted? Are they on servers or local workstations? Is there a practice of copying older email to CDs or DVDs and who manages the disks?
- What happens to the email and data stores of employees who have left the company?
- Where do users store operational files such as word processing, spreadsheets and the like? Are these files backed up? Are there server drives used for shared access to documents? Is there an electronic document management system (EDMS) or an enterprise content management (ECM) system?
- Is the relevant information housed in database applications? Workflow management systems?
- Is there (and was there at the time) an enterprise storage management system that moved older documents to near off-line or off-line storage for archive purposes?
- How are electronic stores backed up? How long are the backup tapes kept?

There are more questions than these to be asked, but at this point you are in the second stage of “scoping” out the project for collection, processing and producing the information.

The questions about email reveal how complex the collection, or “harvesting”, operation will be. In the best situation, all the relevant information resides in active files in active storage, but in less disciplined offices with few or inadequate policies and guidelines on information management, email and other information may be scattered in many

locations, requiring careful planning, documentation of contextual information, and execution to find and document the sources.

Office files. In the absence of a mature implementation of an EDMS or ECM, spreadsheets and reports, letters and presentations get stored in a “file system” such as a Windows directory. The hard drive of a workstation or the “personal share” on the server will be linked to an individual owner, but operational files on shared drives may be difficult to track down to any one author or custodian, particularly as time goes on and employees move to different positions in the company, or leave.

Database applications, computer-aided manufacturing or design, collaboration workspaces and workflow systems are all complex to discover.

Backup tapes. Whether you need to resort to backup tapes depends on when the events took place, whether there are active and archive sources that complete the record, and whether indeed there even ARE backup tapes. Some IT departments rotate a small number of tapes, so that in the event the most recent tape fails during recovery, there are several generations available for restoration if necessary. For these companies, backup tapes could never be used to recover older information unless the event in question happened in the last week.

In other cases, IT shops keep the last backup tape of the month while returning the others for re-use. Over time these tapes accumulate and may get shipped to an off-site storage depot where out-of-sight/out-of-mind takes over and they never get properly destroyed. As storage costs plummet and capacity expands, IT departments have adopted newer backup/recovery technologies. If and when the older backup tapes are identified as possibly containing relevant information, the software and hardware needed to restore the information from the tape may no longer be available.

Step Three – what outside support services do you need?

Factors to consider:

- The scope of the collection as determined in Steps One and Two
- The likely volume of information to be collected
- Whether the corporation has been involved in similar litigation and has already developed a relationship with an outside ediscovery/forensics vendor (in which case, lucky you!)
- Your own comfort with discovery and production of information from electronic sources,
- Your outside counsel’s comfort with electronic discovery and
- Allegations of fraud or conspiracy

If your comfort level and that of your outside counsel are low, an ediscovery consultant can provide education and practical advice on how to conduct the preservation, collection, processing and production of information from electronic sources. The

consultant can also act as a Project Manager and a General Contractor in assembling a team of vendor specialists, or can simply provide direction and guidance to your IT department as they collect the information if the data sources and volumes are straightforward and manageable.

Some cases like product liability by their very nature involve up to a hundred custodians in several physical locations over a time period spanning several years. Even if the information is strictly from active sources, the volume of sources that needs to be preserved, tracked, harvested and processed can require an experienced outside team to get the job done in anything like reasonable timeframes.

Backup tapes are in a category of their own. The recovery process involves rolling all the information on the backup out onto a server before any kind of extraction can be done, and most IT departments are not equipped to carry out this work. In fact, the only time a backup tape gets restored under normal circumstances is in the event of a catastrophic failure where a disk becomes unreadable and must be replaced. Moreover, if the tape is older technology, only a vendor with the right set of tools will be able to restore and extract the information.

In allegations of fraud or conspiracy, it may be necessary to bring in a neutral party to manage the preservation and extraction steps, and report to both plaintiffs and defendants on the methodology, the tools used in the analysis and the results of the search.

Appendix A lists services available from vendors.

Appendix B compares “computer forensics” with “data gathering”

Appendix C is a grid of Case Requirements for Vendor Services

Step Four – writing a Statement of Work

Whether or not you intend to request bids from a number of different vendors or have already decided on which vendor you will be using, you need to describe what you want to have done in such a way that a vendor can determine whether or not it can do the work, how long it will take and how much it will cost.

Generally speaking, a Statement of Work includes sections:

- A preamble or background statement describing the litigation and defining the parties
- An introduction outlining the purpose of the document and its general structure
- General requirements laying out the scope of the work to be done – time period, some estimate of volumes, variety of sources, treatment required, form of the completed product (i.e. format, medium, organization, etc.), services required (such as a hosted repository)
- Specific requirements – services needed, technologies in use, time constraints, security needs, quality assurance, among others

In July 2005, the Sedona Conference® published Navigating the Vendor Proposal Process: Best Practices for the Selection of Electronic Discovery Vendors, which includes sample Requests for Information and Requests for Proposals as well as a guide to what to look for when selecting vendors to receive the Request for Proposal.

Step Five – evaluating the vendors

If you have decided to seek bids from a number of firms, you will need some method of sorting out the “best solution” from those offered – probably the most cost effective, if not necessarily the least expensive. Mandatory criteria lay out those qualities, capabilities and capacities without which you will not consider the vendor further. Discretionary criteria, on the other hand, allow for a comparison among vendors.

Mandatory criteria might include:

- Minimum number of years a company has been in business
- Minimum years of experience for key employees
- Minimum volume of cases/projects of similar size and characteristics handled in, say, the past 2 years
- Certifications and other qualifications (e.g. project management professional, software vendor certifications appropriate to the environment, ISO 9000 compliance)

Discretionary criteria could include:

- Approaches to providing services or meeting requirements, such as security, performance, monitoring, data management, professional services
- Volumetrics
- Availability
- Support and professional services

Minimum marks may be established for discretionary criteria. For vendors exceeding the threshold, the comparison may then consider the overall value of the proposal.

Step Six – building the project team – roles and responsibilities

The Statement of Work becomes part of the negotiated contract with the vendor. However, it is also a partnership, with expectations on both sides. Cooperation and collaboration can reduce the intrusion and expense of ediscovery.

Vendors need a point of contact – someone to report progress to and to advise in the event of problems. Decisions will need to be made. That point of contact might be a member of the litigation team, perhaps someone who has agreed to become the firm’s ediscovery guru. This works where the client is small and has had no experience with ediscovery and little with litigation support. For experienced corporations, the point of contact might be someone in the General Counsel’s office, or a dedicated ediscovery unit. Whoever it is, the point of contact must have the power to make decisions and be well supported and connected within the corporation, especially if decisions involve funding.

The point of contact looks outward to the vendor, and inward to the IT and Information Management or Records units. As the source of information about systems used in the corporation – in fact, as the main source of the evidence, IT needs to be involved in the planning and scheduling of the extraction and collection phases. As important is their role in identifying and preserving the sources of information. They need to be well informed about the implications of preservation and consulted when decisions are made to take forensic images of workstations and servers, or suspend rotation of backup tapes.

Step Seven – managing the process

Status reports and periodic team meetings

- To track progress against timelines and budgets
- To identify problems and determine their impact in terms of cost and delay
- To get input on proposed alternatives and select the best from all perspectives
- Action plans as needed to get back on track
- To ensure procedures are being followed

Documentation

- Of processes involved in identifying, extracting, harvesting, culling and producing evidence
- Tracking individual items through the process as batch lots
- Chain of custody assertion – continuity and handoff
- Problems encountered, analysis of the options, selection and action taken

© Peg Duncan 2006