ESQUIRE
LITIGATION SOLUTIONS

Rule 30(b)(6) Depositions in Electronic Discovery:

Discovering What There Is to Discover

One of the challenges in electronic discovery is identifying the various sources of electronically stored information (ESI) that could potentially be relevant to a particular matter.

The electronic information that a company possesses is usually distributed on its various servers, employee's computers, backup tapes, and many other media and devices. How long a piece of information remains is generally determined by document management and retention policies (assuming such policies are in place and enforced), backup policies, and of course by the behavior of the employees. Moreover, ESI is, due to its very nature, bound to be available in numerous formats, some of which are more readily accessible or usable than others.

Understanding how a corporation or agency stores and manages its ESI is critical in developing an effective electronic discovery request. A rule 30(b)(6) deposition is an extremely useful tool to gain this understanding—helping to build the foundations of a case—as well as to explore all the ways persons within that entity actually conducted business day to day. (For the full text of the rule, turn to the end of this article.)

The Rule

Under Federal Rules of Civil Procedure 30(b)(6), a corporation, partnership, association, or governmental agency, subject to deposition on one or more issues, must designate one or more of its "officers, directors, or managing agents, or other persons" to testify on behalf of the corporation on each of those issues. The underlying effect of the rule is to shift the burden of determining who is able to provide the information from the requesting party to the corporation.

It is the obligation of the responding corporation to present a witness able to testify as to matters "known or reasonably available to the organization." If the 30(b)(6) witness cannot answer the questions for which that witness has been designated, the corporation is deemed to have failed to comply with the rule and may be required to produce another witness or, in some cases, be subject to sanctions.

The rule requires that the requesting party describe "with reasonable particularity" the subject matter on which testimony is being sought. The requesting party must describe what information is being sought in a way that fairly allows the corporation

to identify the person(s) able to provide the information and adequately prepare them to do so.

Please note that the requirement is only that the persons designated by the corporation "shall testify as to matters known or reasonably available to the organization". There is no requirement that the corporation produce the person who is the "most knowledgeable" witness.

Ultimately, the responding party has to be careful to select the right person to appear and to prepare him or her well to testify, considering what kind of information will be probed and to forestall against any potential traps for the witness, or for subsequent witnesses, that opposing counsel might attempt to set. Furthermore, 30(b)(6) testimony is not strictly limited to “facts” alone; the witness may need to speak to, for example, his or her company’s “positions,” “interpretations,” or “beliefs” on a given topic—thus demanding that an articulate, adroit individual be designated to appear. Presenting an unprepared, ill-informed witness could bring sanctions, although the inadequacies generally must be dramatic to get that far.

The Deposition Purpose and Strategy

The main purpose of the deposition is to determine the “who, what, where, when and how” of ESI: who generates and uses it; what is it; where and how is it transmitted and received, stored, and backed-up (with particular emphasis on retention policies and actual procedures); when and how data is destroyed; and how the data can be accessed and retrieved.

Equally important is the need to gather information to support a forensic expert’s declaration justifying the need for intrusive inspection/data-gathering on the network, to support further discovery requests, or to support a motion to compel/for protective order, and so forth.

Along these same lines, it is necessary to gather enough information to assist the forensic expert in ESI gathering, to let him know what he should expect to find and where he should expect to find it. A secondary goal is to support whatever motion you will need to get the data you want. So put yourself in the judge’s shoes and ask those questions that the judge will want answered before he grants your motion.

The Deposition Notice

As noted before, the deposition notice must describe "with reasonable particularity" the subject matter on which testimony is being sought. The notice must be tailored to fit the specific needs of each matter. Knowing who the subject of deposition is and that person's role in the corporation will subsequently influence how the deposition itself is crafted.

A sample Rule 30(b)(6) notice would request that a corporate designee(s) should be prepared to testify regarding the following subjects with respect to the corporation's information technology systems.

1. Written policies and enforcement procedures regarding electronic records management
2. Written policies and enforcement procedures regarding employee use of company computers and data, including but not limited to:
    a. Desktop computers
    b. Laptop computers
    c. Home-based computers used for company business or communication purposes
3. Locations of electronically stored information relevant to the specified matter
4. Computers currently in use and computers no longer in use:
    a. Number, types and locations
    b. Operating systems with versions, dates of use and upgrade history
    c. Application software with versions, dates of use and upgrade history
5. Network architecture
    a. Network topology
    b. File-naming conventions
    c. Location-saving conventions
    d. Disk or tape labeling conventions
6. Company Email Systems and Instant Messaging Systems
7. Company Intranets
8. Onsite and Off-site Servers
9. Off-site Escrow Services
10. Archival Systems and Procedures, including disk, tape, or other media
11. Backups Procedures, Inventories and Schedules, including Tape Reuse Cycles
12. Disaster Recovery Systems, including power source, capacity and location
13. Instances of computer or systems failures and subsequent data recovery efforts
14. Online (third party hosted) repositories
15. Portable devices, including but not limited to:

a. Portable Digital Assistants (PDAs)
b. Cellular Telephones
c. Mini Computers
d. External Hard Drives
e. CDs and DVDs
f. USB Flash Drives

16. Document Management Systems
17. Company Database and Systems Administration
18. Identities of all (a) current and (b) former personnel who have or had access to network administration, backup, archiving, or other system operations during any relevant time period.

Companies who are designating a Rule 30(b)(6) witness should pay close attention to a notice that has been drafted in a broad or vague manner. This may be an attempt to surprise an unprepared witness to obtain damaging admissions or to preclude future use of later testimony. Under such circumstances, a responding party should always attempt to negotiate a more specifically drafted notice. In some situations, it may be necessary to seek a protective order. As a precautionary measure, a responding party should anticipate questions beyond the scope and adequately prepare the witness for such an event.

Sample Deposition Question Areas

When it comes time to actually conduct the deposition, a comprehensive approach will take into account the following subject areas to explore.

The qualifications and responsibilities of the deponent –

- Explore the education, training and experience of the deponent. Pay particular attention to his background or experience in the handling or investigating of computer evidence. Oftentimes IT personnel are trained to provision systems but lack training in forensics.
- What is the deponent's rank in the organization? To whom does he report? Who reports to him? How long has he been with the company? Have his duties changed during his tenure—and if so, how so?
- The role/responsibility the deponent has (or will have) in responding to discovery requests seeking production of electronic documents, such as information created, stored, and/or utilized using computer technology.
- Ask what the deponent did to prepare for deposition, including any document review.
- Find out if the deponent has been involved with other, prior litigations involving ESI. If so, ask about specifics: case(s), what was at issue, what

role he played, what kind of information was produced, how it was used, and the outcomes of litigation.

The organizational structure and its data management systems –

- Who is responsible for systems administration? What are that person's specific duties? Does he have a subordinate staff? What are their roles?
- Pursue details regarding hardware (including model numbers and/or hard drive capacity) used by deponent's employer; security measures, such as the use of passwords by users, sharing of passwords, and access to passwords by system administrator(s).
- Explore operating systems for network servers, including model versions, maintenance, upgrades, and capacities.
- Ask about the networking of desktop computers, as well as information sharing methods among users via intranets, company email, and other means.
- What does the company do for backup, considering all aspects including tapes, hard drives, servers, and e-mail systems?
- Don't forget about ubiquitous items, such as facsimile machines used by deponent's employer and the procedures to use fax machines (e.g., fax logs, memory of fax machines, and the like).
- Pursue details about the disposal, recycling, or sale of hardware—including what happens to hard drives.
- Determine if the company uses consultants or outside vendors for maintenance and service of computer systems; you may want to depose these individuals as well.

Software and Email –

- Pin down what application software is used on desktops, laptops, and other devices. Identify standard software such as MS products, for example, Word, Excel, Power Point) as well as less-common types and their purposes. Find out the how long different versions of software the company used within the relevant time of your investigation.
- Seek details about company standards for personal digital assistants (e.g., hand-held devices such as Palm Pilot).
- Explore details about the company's email systems used, as well as the company's policies and enforcement procedures for retention periods, use of files, and deletion.

Document Preservation and Record Management –

- Establish specifics about the company's record management policy. First and foremost, is it a written policy? If so, be sure to obtain, at a minimum,

the most current version of it; you may also want to seek previous versions to determine instances of policy changes. Moreover, find out when the policy was originally instituted, when electronic documents became subject to it, and who is chiefly responsible for enforcement of it.

- Find out who prepared the notification and instructions about preservation of documents; also how and when it was communicated to the company and to the deponent.
- Determine if the deponent has examined any computers since learning of any litigation, and if so, get at those details.
- Seek details of any deletion of documents since the deponent received notification of the lawsuit, reasonably anticipated a lawsuit, or upon the commencement itself.

Backup and Disaster Recovery Procedures –

- What are the company's backup procedures? What are the intervals, the medium for backup, the reuse of backup medium, and the location of backup? Who is chiefly responsible for executing and overseeing backup procedures? Who else is responsible?
- Inquire after legacy systems; obtain information about software used for backup media or archived documentation, and determine whether the deponent has legacy software and manuals.
- Probe whether backup tapes have been reused or otherwise erased since the filing of lawsuit.

Miscellaneous sources of electronic information –

- Find out about any locations where electronic documents are regularly sent outside of the deponent's employer.
- Seek to obtain names, locations, and roles or responsibilities of other persons who would have knowledge about third party's computer systems.
- Ask about the company's Internet site, including who develops and loads content, who reviews/maintains/updates the site (and at what intervals, whether regular or irregular), and tracks the access of the site by third parties, if any user data is harvested and for what purposes.

A 30(b)(6) can be a powerful tool to gather, verify, or directly challenge information, impeach or exculpate witnesses, lead to new areas of inquiry, and shape the course of litigation. In light of the newly amended FRCP, wielding this tool may become more commonplace as IT professionals, computer forensics experts, corporate document retention policy managers, and other persons central to the labyrinth of ESI are deemed to be indispensable figures in the judicial process.

FRCP Rule 30(b)(6): *A party may in the party's notice and in a subpoena name as the deponent a public or private corporation or a partnership or association or governmental agency and describe with reasonable particularity the matters on which examination is requested. In that event, the organization so named shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. A subpoena shall advise a non-party organization of its duty to make such a designation. The persons so designated shall testify as to matters known or reasonably available to the organization. This subdivision (b)(6) does not preclude taking a deposition by any other procedure authorized in these rules.*

Theresa L. Widmann, Esq. is an Electronic Discovery Consultant and Business Development Manager for Esquire Litigation Solutions. Ms. Widmann received her Juris Doctor from Seton Hall University School of Law. Prior to joining Esquire Ms. Widmann was a Special Deputy Attorney General with the Essex County Prosecutor's Office in Newark, New Jersey. She is responsible for developing Continuing Legal Education courses for Esquire Litigation Solutions and counsels clients on various matters related to litigation including discovery of ESI, review tools, trial technology and litigation support technologies. Her email address is twidmann@esquirecom.com.