2013

E-Discovery Issues

Curtis E.A. Karnow

E-Discovery Issues

U.C. Hastings, *Negotiating Solutions to Your e-Discovery problems*

Curtis E.A. Karnow
Superior Court of California (San Francisco)[1]
May 16, 2013

I. Backdrop

A. *Very* high expense
   a. E-discovery may be the single most costly aspect of litigation
      i. 93 backup tapes- $6.2 million
   b. Non-parties will ask to be compensated
   c. Software to gather and review old data--proprietary formats
   d. High volume
      i. 1 CD-ROM = 650 megabytes = 325,000 typed pages (DVD is 7 to 14 times this)
      ii. Corporate databases likely exceed terabyte (1,000,000 megabytes) = (500 million pages of text)
      iii. Average employee sends or receives about 50 messages per working day = more than 1,200,000 messages/yr for organization of 100 employees

B. Computer Literacy: Understanding computers and the digital realm
   a. E.g., types of data and formats, architecture [stack of software (BIOS, OS to apps)]; how databases work; terminology. [Take the "test" below]

C. Types of documents and data
   a. Meta data & embedded data, e.g.
      i. Document (author, date revised, drafts & changes)
      ii. Email (to, from, BCCs, route, date)
      iii. Web page (source includes spider-searchable words)
      iv. Formulae in spreadsheets
   b. System level information such as computer logs, indices, audit trails, browser history files, etc. created when applications are opened, when employees log on to the network, or when files are purged
   c. Drafts
   d. Electronic calendars
   e. IM & text messages, SMS

[1] None of these materials suggests how I or any other judge would rule in a specific case.

f. Web pages
g. Cache/RAM
h. Blogs, & as revised + comments
i. Monitoring data (e.g. keystroke monitoring)
j. Comments on commercial sites (YouTube, Amazon, FaceBook, etc. etc.)
k. Emails- at a many locations
l. Voicemail
m. Chat groups
n. IRC
o. Ephemeral data: document = momentary integration of databases
    i. RAM
    ii. RSS feed
    iii. Framed and framing sites
    iv. Ads on web sites
    v. Remember- *just opening a file changes it*
    vi. Cookies: "permanent" and transient (session only)
    vii. Deleted data
        1. Recovery
            a. Do it yourself
            b. Professional
p. The notion of the *logical document*
    i. Why we care:
        1. what's the *complete* document (admissibility and review issues)?
        2. What's the *context*? Is it prejudicial, relevant?
        3. Spoliation?
    ii. E.g.,
        1. Web sites
        2. email string & attachments
        3. collaborative documents
        4. inclusion of metadata
        5. blogs & comments
    iii. Issues:
        1. Attachments
        2. Multiple authors
        3. Creation & metamorphosis over time
        4. "Destruction" and loss

D. New locations of items –includes 3d parties
    a. "Cloud" computing:
        i. Hosted applications: Yahoo, Google, collaborative environments
        ii. Application Service Providers (ASP)
    b. Mirror sites

c. Locations used by outsourcing vendor
d. Server farms
e. Enterprise databases
f. Archival locations (Iron Mountain)
g. Backup tapes (off site, on site)
    i. Reused & not reused
h. Home PC, iPad, laptop
i. GPS
j. MP3 players
k. Vehicle tracking devices
l. Cell "phones" {actually small computers}
m. Flash & USB drives & other removable media

II Handling Discovery

E. Before litigation is ever a twinkle in the eye
    a. Document / records retention policies
        i. Plain, easy to understand
        ii. Universally adhered to (corporate leadership issues)
        iii. Supported by the technology- manageable
        iv. Standards for when items are encrypted and storage of keys (in event employee leaves etc.)
    b. Preparing for litigation holds- communications with and within the client
        i. Ability to instantly implement hold
    c. Computer usage policies (e.g. what email is NOT for!)
    d. For clients often in litigation & own more than a handful of computers: must form *internal e-discovery team* in advance of litigation
        i. IT & lawyers
        ii. Handles most of the pre-review tasks
        iii. 2006 survey- only 19% of corporations "well prepared" for e-discovery

F. Communications with other parties
    a. Work out issues *without* the court. Only the parties really know what's needed and what the burden really is.
        i. "Agree, for the law is costly….."
    b. Stipulated protective orders
    c. Claw backs
    d. Meet and confer- *pick up the phone*
    e. Use your IT experts

G. Communicating with the court
    a. The usual contexts
        i. TRO, ex parte, request for preservation order
        ii. Informal discovery conference
        iii. Discovery motion
        iv. Case management conference
        v. Trial (in limine motions, requests for sanctions and exclusion)
    b. Essential for parties to *meet & confer* as early as possible to avoid disputes, take control, preserve data, limit costs
        i. Alert: following state mandated timelines is generally *too late*
            1. I.e. in preparation for first CMC
        ii. You *have* previously familiarized yourself with the client's systems (can be a very large task)
    c. Informal off-the-record conference with judge
        i. In complex and direct assignment
        ii. Highly recommended
    d. Discovery motions
        i. Mandatory fee shifting sanctions on losing party
        ii. Fast way to lose motion:
            1. plainly overbroad demands (see *Calcor Space*, 53 Cal.App.4th 216)
            2. plainly boilerplate knee-jerk objections
            3. claims of burden without admissible evidence
    e. Raise issue early
        i. Preservation orders
        ii. TRO?
    f. CMC
    g. If issues likely- consider complex or single assignment/complex designation
    h. Stipulated protective orders
        i. Why order and not just stipulation? (Sanctions)
        ii. Note <u>*strict*</u> rules about sealing records. Not applicable in discovery context, but is in subsequent contexts.
            1. Parties' agreement to seal irrelevant
            2. The 'delta' document (lodge redlined version of original)(helpful for judge)

H. Procedures
    a. Needs evaluation
    b. Preliminary discovery?
        i. custodians
        ii. locations
        iii. systems
        iv. data type & need for proprietary s/w to view

v. available search tools
vi. encryption use
vii. Per meet & confer if at all possible, else: depositions (PMK), interrogatories etc.

c. Collect:
   i. I.d. custodians
   ii. I.d persons who know the system- how documents are stored & created
   iii. I.d. data sources
   iv. Interview key players
   v. Litigation holds
      1. How early? Reasonably should have anticipated litigation…
      2. What scope? Can be enormous burden
   vi. Preservation demands & orders
   vii. Format?
      1. native
      2. 'translation'
      3. Alert: destruction / loss of data (e.g. TIFF from spreadsheet)
   viii. de duping
      1. paper v. electronic?
      2. multiple drafts- some are identical & some are not— depending on what you're looking at (i.e. metadata)
         a. 'same' email on e.g., 2 different drives may be significant
   ix. Sampling
   x. Key word search
   xi. Recovery of "deleted"
      1. Must the physical drive be seized?
   xii. Keeping the string (e.g. emails + other 'logical' documents) together

d. Review:
   i. Relevancy
   ii. Privileges
   iii. Privacy
   iv. Third party rights, contractual (e.g., confidentiality, trade secrets) and other, such as statutory (consumer)
   v. Protections under foreign law (EU)
   vi. Trade secrets & proprietary systems and data
   vii. "Translations"
      1. public key encryption & digital signatures
      2. recovered/reconstructed data

e. Produce
   i. Cost sharing with other side: common vendor, repository
   ii. Bates stamping and tracking documents

iii. Cost shifting for data which is difficult/expensive to access because e.g.,
    1. proprietary software
    2. archival "tape" – 1 big soup of data
    3. cost of search through production of vast amounts of data 'as it is kept in the ordinary course of business'

I. Working with outside vendors
    a. Will not excuse results. Their failures are the failures of the lawyers/parties.
    b. Supervision
    c. Cost
    d. What s/w are they using? Predictive coding, concept based searches, probabilistic or fuzzy search models - etc. everything depends on *specifically* what is done. No one size fits all.

J. Cost allocation
    a. *Toshiba*. Court power to allocate.
    b. Proportionality (see next topic for detail)
    c. Toe in the water: Much lower costs to see if it's worth it
        i. Sampling
        ii. Obvious custodians first
        iii. Narrow time period
        iv. Other testing
        v. Quick peek[2]
        vi. Take deposition first, or meet with IT people, to investigate reduction in scope of targeted data
        vii. Key word search
            1. fewer, or more specific words; mechanisms to narrow search
            2. Issue: Discover other side's keywords?

K. Proportionality: possible factors (must be shown by admissible evidence)

---

[2] ""Quick peek" agreements are agreements to speed up productions and reduce costs by agreeing (1) to let the requesting party take a "quick peek" at ESI without the producing party undertaking the time and expense in advance to review the entire population of ESI to eliminate non-responsive and protected information; (2) during the course of its "quick peek," the requesting party then flags the particular ESI records it wants the producing party to formally produce; and (3) the producing party then limits its responsiveness and privilege review to the set of flagged documents, actually producing only those that are responsive and not privileged, with the requesting party agreeing that it will return, not use and not claim waiver with respect to any non-responsive or privileged information that it saw during the "quick peek." Most companies, however, likely will be unwilling to accept the central premise of a "quick peek" agreement which involves turning over ESI without any advance review."

a. Burden (costs, interruption of business to producing party, other opportunity costs, etc.)
b. Worth of case/range of damages
c. Alternative locales for information (even if not same form of information)
d. Extent to which demanding or producing party is responsible for any lack of alternatives means to secure the information
e. Importance of issue to which information relates
f. Precedence of issue (need is immediate vs. need depends on other events in the case)
g. Fishing expedition vs. specifically described data/item
h. Probability that sought-for information will be located in targeted area
i. Availability of "toe in the water" alternatives (see above)
j. Role of custodian (peripheral, third party vs. central party)
k. Available alternatives (e.g., stipulations, creation of summaries, use of copies)
l. Offer of demanding party to pay
m. Risk of destruction if data if not now preserved/disclosed/retrieved
n. Parties' financial resources
o. Public policy considerations (benefits to public)

L. Burden
   a. See below, state law: *two* levels of inquiry and so likely two levels of burden analysis
   b. Must establish with admissible evidence. *Calcor Space,* 53 Cal.App.4th 216
      i. Declarations of lawyers are *not* usually admissible
   c. Extra consideration for *non*-party targets

M. Direct access to systems
   a. Forensic exam of systems (for deleted etc.)
   b. Imaging (cloning) media
   c. Some issue:
      i. adversary access to trade secrets
      ii. adversary needs the drives up and running (issue if media needed to e.g., do data recovery)

N. Safe harbor
   a. Re data destroyed (e.g. overwritten) in the *good faith* and *routine* operation of a system
   b. Not immunity. Not good faith if you know it's needed? Perhaps no 'safe harbor' if no action taken to preserve

O. Privileges (work product, attorney-client)
   a. Inadvertent disclosure & claw back agreements

b. Waiver issues not settled

P. "Reasonably accessible"
   a. Under new rules this concept divides discovery into 2 portions
      i. Reasonably accessible
      ii. Not reasonably accessible
      iii. Really, still, a spectrum analysis
   b. Balancing act; proportionality; what alternatives do we have?
   c. Not reasonably accessible perhaps because: of location; format; locating the specifically useful data in the (otherwise easily accessible) soup

Q. Ethics / Professional responsibility
   a. Are you truly competent to handle e-discovery on your own? To articulate what you really want, to articulate what the burden of production really is? (Take the 'test' below)
   b. Preservation & working with clients
      i. Estimating costs
      ii. Communication: Knowing what the client has (data map)
   c. Not taking client's word for it
      i. *Qualcomm*: massive cache of documents not turned over to other side.[3]
         1. Attys. did not do reasonable inquiry
         2. "blindly accepting Qualcomm's unsupported assurances that its document search was adequate"
         3. Stand up for the right thing
         4. Resign from case if necessary
         5. Err on side of disclosure
   d. Negligent disclosure of protected / privileged materials
   e. Is it ethical to mine metadata? Divergence of opinion

R. Sanctions for discovery abuse/spoliation
   a. Terminating
   b. Issue
   c. Adverse inference + jury instructions
   d. Deemed facts
   e. Preclude evidence
   f. Costs and fees of other side
   g. Malpractice exposure
   h. Bad P.R.
   i. Disciplinary proceedings

[3] Sanctions later set aside. *See generally*, http://www.clearwellsystems.com/e-discovery-blog/2010/04/20/what-you-can-learn-from-qualcomm-v-broadcom/; http://www.abajournal.com/news/article/after_sanctions_are_lifted_qualcomm_lawyers_react_this_can_happy_to_anybody/

S. State rules: Amendments to both CRCs and Discovery Code – Among other things:
    a. Parties must confer on ESI *before* the first case management conference;
    b. parties may undertake discovery not only by "inspecting," but also by "copying, testing, and sampling" electronically stored information;
    c. Authorize a party to specify the *form* in which electronically stored information is to be produced;
    d. If no form is specified, the responding party must produce the information in the form or forms in which it is ordinarily maintained or in a form that is reasonably usable;
    e. party opposing or objecting to a demand bears the burden of showing that the electronically stored information sought in discovery is from a source that is not reasonably accessible because of undue burden or cost;
    f. That the court may nonetheless order discovery of such information if the demanding party shows good cause;
    g. "safe harbor" provisions that provide: "absent exceptional circumstances, the court shall not impose sanctions on a party or its attorneys for failure to provide electronically stored information lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system;"
    h. Not entirely the same as federal

Test your ability to handle related IT issues without assistance from a professional!

- True/false:
    - If you only *open* a Word document (to read it) you change it.
    - IP address always identifies a specific computer?
    - Printers' memory contain discoverable data .
    - A PDF has the same data as a Word document in its native (Word) format.
    - Data encrypted with a 256 bit key can be decrypted using a brute force attack within about a week.
- What is open source?
- What is PGP? RSA? Twofish?
- Penguin is the symbol of what OS?
- Have you programmed before?—what language?
- Explain
    - permanent vs. session cookie
    - cloud computing
    - XML
    - Source vs. object code
    - Fuzzy search

- RAID (about how many levels are there?)
- Whois – is used for what?
- The hash [MD5 hash] for a file and how it's useful to authenticate

Resources

-Navigating the Hazards of E-Discovery: A Manual for judges in state courts across the nation (Institute for the Advancement of the American legal system, Univ. Of Denver)
- N.D. Cal.'s new (January 2013) Guidelines for the Discovery of Electronically Stored Information
-http://california-discovery-law.com/site_info_bio.htm (items up through 2009)
-https://thesedonaconference.org/publications
- Pocket Guide, Managing Discovery of Electronic Information, http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt2d_eb.pdf/$file/eldscpkt2d_eb.pdf
-Karnow, contributing editor of:

- CEB, HANDLING EXPERT WITNESSES
- CEB, CALIFORNIA CIVIL DISCOVERY PRACTICE (2 vols., loose leaf)
- CALIFORNIA JUDGES BENCHBOOK, CIVIL PROCEEDINGS: DISCOVERY at 325 *et seq.* (e-discovery)