2011

Admissibility of Electronic Documents

Curtis E.A. Karnow

Admissibility of Electronic Documents

Hon. Curtis E.A. Karnow
Superior Court, County of San Francisco

(San Francisco Bar Association Presentations, including 2009, 2011)

⌨

Three preliminary points:

- What everyone should own: M. Simons, CALIFORNIA EVIDENCE MANUAL

- What's different: 3 concepts: ephemeral, mutating, 'logical' documents

- What you need to know: Computer literacy: Understanding computers and the digital realm. E.g., types of data and formats, architecture [stack of software (BIOS, OS to apps)]; how databases work; terminology

⌨

Preliminary issues: What is unique re: e-documents

- WHAT **is** the thing in question?
  - ◦ Issues erupt because unlike paper, where we are all familiar with what it is and how the thing is usually prepared, most people don't know how the electronic document is created, leading to incoherent discussions on evidence.
- WHO created it?
  - ◦ w/ e-doc, usually many pieces went into its making:
    - ▪ both computer and human (originally) data entry, data calculated, data dependencies ('1' changes into '2' because someone else (or some program)) did something in another place in the database
    - ▪ An e-doc–which *looks* static and like "one thing"-- may contain data created at different times by different people
  - ◦ Default formats, underlying programming, acceptable range of input constraints on data entry- whose input is that then?
    - ▪ It is reliable and correct?
    - ▪ Programming defects eviscerate the print out?
- Data corrupted? Has it been changed or modified?
  - ◦ We think computers are infallible. They are not.[1] 352 issue.
    - ▪ Most software uses methods of disambiguation / Round out error / Data accepted only within parameters / Rejected if not within data values or types / Resolved automatically to fit (how spellchecker works!) > error
  - ◦ Where the program is also measuring, or computers are networked > issue of clocks, accuracy. Networked computers have serious issues of network protocols, clock

---

[1] http://www.cs.dartmouth.edu/~sergey/trusting-e-evidence.pdf

inconsistency, etc., and we do not have good intuitions about these sorts of problems.[2]

- ◦ Harder to tell if there are errors because we don't understand the context as well as with paper, where we look to torn, erased, broken item. Evidence of tampering may be easier to see on paper
    - ▪ BUT: Existence of copies, and which is latest version, and who has it or who saw it-- all more difficult with paper
    - ▪ Assurances via hashing, e-sign & encryption, metadata, etc > perhaps e-doc is more reliable?
- ◦ Paper doesn't change every time it's read!
- ◦ Management (storage & retrieval) and creation of paper easier to explain
- ◦ Distinguishing a record as it was on date X and *later* on date Y may be far more difficult than with paper (or is it perhaps *easier* with audit trials and metadata?)

More Background

A. New types of documents and data
- a. Meta data & embedded data. Distinguish (for e.g., hearsay purposes) data created by humans (see below) and that created by computers). E.g.,
    - i. Document (author, date revised, drafts & changes)
    - ii. Email (to, from, BCCs, route, date)
    - iii. Web page (source includes spider-searchable words in e.g. ® case)
    - iv. Formulae in spreadsheets
    - v. *Note* that humans can change metadata. Who is the 'author'?
- b. Computer logs, indices
- c. Drafts
- d. Electronic calendars
- e. IM & text messages, SMS
- f. Web pages
- g. Cookies
    - i. Permanent
    - ii. Session
- h. Cache/RAM
- i. History logs
- j. Blogs, & as revised & commented on (& Facebook entries)
- k. Comments on commercial sites (YouTube, Amazon, FaceBook)
- l. Emails- at a many locations
- m. Tweets
- n. Voicemail
- o. Chat groups/ chat room: logs and transcripts
- p. IRC
- q. Ephemeral data: document = momentary, transitory integration of databases
    - i. XML
    - ii. RAM
    - iii. RSS feed
    - iv. Framed and framing sites

---

[2] C. Karnow, "Information Loss and Implicit Error in Complex Modeling Machines," FUTURE CODES: ESSAYS IN ADVANCED COMPUTER TECHNOLOGY & THE LAW 87 (Artech House 1997).

      v.   Ads on web sites

      vi. Remember- *just opening a file changes it*

      vii. Database reports generated by query language (e.g. SQL)

  r. The notion of the *logical document*

      i. Why we care: what's the *complete* document (admissibility and review issues)? What's the *context*? Is it prejudicial, relevant?

      ii. E.g.,

        1. Web sites

        2. email string & attachments

        3. collaborative documents

        4. inclusion of metadata

        5. blogs, commercial sites, & their [public] comments

        6. database reports

      iii. Issues:

        1. Attachments

        2. Multiple authors

        3. Creation & metamorphosis over time

        4. "Destruction" and loss

Evidentiary Issues

B. What is *purpose* of using the item?

  a. Truth of statements? Then full panoply of issues.

      i. *Bypass the issues—hearsay and perhaps authenticity as well:*

        1. Stipulations

        2. Req. for admission

        3. Use opposing party's pleadings

        4. Deposition of custodian

        5. Advanced exchange or documents

        6. Use of experts to rely on what might be inadmissible evidence to in effect at least get the <u>results</u> into evidence

        7. Judicial notice? (*Ampex Corp v. Cargle* (2005) 128 Cal.App.4th 1569 at n.2)

          a. Recall: *advanced* notice in writing to the other side!

        8. Handle in advance of trial: may need single assignment access to trial judge (ask for it in SF)

  b. State of mind

  c. Past recollection recorded

  d. Refresh recollection: The *FISH* Rule- anything goes: For Instance, Saffron Hogs[3]

  e. Animation v. simulation

      i. <u>Animation</u> = illustrates W.'s testimony- not as many issues

        1. Demonstrative/Illustrative : Does not go to jury room

        2. If not useful to explain, excluded

        3. Illustrative? How to tell:

          a. Did not exist at time of litigated facts

          b. is not a summary of other documents

          c. was created specially for or at trial

          d. e.g., drawing on white board by W while testifying

---

[3] I.e. anything, whether admissible or not, from a Madeleine cookie to a computer screen of data, can be used to refresh memory.

e.   <u>W</u> is vouching for the accuracy, and cross examining
                     this W is *all* one needs to test the exhibit
        ii. <u>Simulation</u> = is evidence as such
                1. Is re-creation of evidence
                2. For which you need to know *source* of data, *method* by which it
                    was used (software rules)
                3. *Creates new evidence* from pre-existing data
                4. Multiple layered experts issue
        iii. Problems
                1. Remarkable POWER of animation/simulation- can take over,
                    blotting everything else out >>> 352 issues
                2. Shows perspective / field of view no witness had or could have
                    had
                3. Speeds up, slows down actual event
                4. More or less lighting
                5. More or less field of view
                6. More or fewer background items in scene
                7. Affects attention viewer places on a central event
                8. Include aspects (sound) that maker just invented to create mood
                    or feeling (music can be very evocative)
                9. Other objections
                        a.   in effect *coaching* the witness?
                        b.   In effect *leading*?
                        c.   *Argumentative*?

C. Evidence issues
    a. Authentication
        i.   What it purports to be
                1. is the author who you think he is?—the use of handles & screen
                    names in chat rooms, comments on sites, IMs, etc.
                        a.   Impacts who needs to testify re authenticity
                2. Circumstantial evidence
                        a.   Internal markers
                        b.   How item stored and retrieved—chain of custody
                             approach
                3. First hand testimony of creator
                4. Wayback machines- conflicting rulings on authentication issues
        ii. Challenges to computer records often take one of three forms:
                1. whether the records were altered, manipulated, or damaged
                        a.   just raising the issue is pointless
                2. challenging reliability of the computer program that generated
                    the records
                        a.   Generally don't need programmer expert to discuss the
                             mechanism (or maintenance) of the program or hardware
                             where the compute *stores* the data
                                i.   But because data can be modified there may be
                                     issue whether data is as originally stored/created.
                                     In which case there will be issues re:
                                        1.   access & security: logs re changes and
                                             access
                                        2.   audit programs

  b. But where the computer program *manipulates* data, the reliability of program to do calculations accurately must be established. E.g.,
   i. spreadsheet formulae
   ii. computer generated logs such as proxy sever logs. Do we need programmer for this?
    1. if so, what do we do with open source software?
  3. questioning the identity of their author
 iii. Opposing party ACTED on it *as if* it were authentic. EV 1414
 iv. Chain of custody for e.g.,
  1. mirrored drive
  2. decrypted data
  3. recovered 'deleted'
 v. This is just a *prima facie* matter: Not meant to be a high hurdle
  1. Doesn't matter if there's contrary evidence (unless judge really thinks evidence unreliable): the Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so
  2. Accuracy issues- programmable databases- even "computer generated" (per algorithm) data has at some earlier point been human-programmed!

b. Secondary Evidence
 i. We do not have a 'best evidence' rule anymore
 ii. Rule: copies of a "writing" are OK unless it fails as secondary evidence. Copy presumptively ok
  1. There may be large number of varying originals of the "same" thing
 iii. Computer output is a "writing" [EV 250] and an original [EV 255] and printout presumptively accurate (EV 1552(a)) of the data inside the computer—the print out function works—not a presumption that the data inside computer itself is accurate or reliable. *Hawkins*, 98 CA4th 1428
  1. Same if data is video or image. EV 1553
  2. But for official records see EV 1552(b)
c. Hearsay
 i. Most computer output is hearsay- reflects statements made by humans out of court. Thus go to:
  1. Public records
  2. Business records
   a. Regular course of biz
    i. Not made in preparation for suit. But alert:
     1. Printouts prepared specifically for litigation from databases that were compiled in the ordinary course of business are admissible as business records to the same extent as if the printouts were, themselves, prepared in the ordinary course of business. The important issue is whether **the database**, not the printout from the

database, was compiled in the ordinary course of business

  b. Writing done @ or near the time
    i. Irrelevant: date of print-out or retrieval. Issue is: when data *entered*- was that '@ the time'?
      1. Courts get this wrong & get reversed. *Miyamoto*, 176 CA4th 1210
    ii. how <u>close</u> in time? Depends. If data entry is done three days later and he had 42 million results to record, it's too late. If he has two results, might be fine. ISSUE is whether it's reasonable to think the results were accurately recalled at time of entry. Case specific
      1. *Glatman*, 146 Cal.App.4th 700, 704 (2006): Here, the record is silent as to the department's recordation policies and procedures, any automatic recording capability of the testing equipment used, and the average number of tests performed by an analyst each day.
      2. `Whether an entry made subsequent to the transaction has been made within a sufficient time to render it within the [hearsay] exception depends upon whether the time span between the transaction and the entry was so great as to suggest *a danger of inaccuracy by lapse of memory*.'
    iii. entered by- whom? Someone with knowledge of the event-- right?! (Note the trap: sometime it's just a data clerk who knows nothing)
  c. Qualified W testifies as to preparation
    i. Computers: W generally understands system operation, generally can use systems, & can explain data, even if W can't do every task from input to print out
  d. Appears trustworthy
  3. Recall that hearsay may be contained *within* the business/public record (e.g., police report)
 ii. Hearsay exceptions, e.g.
  1. Against party opponent (their records, computers, etc.)
 iii. Internal calculations and logs (such as when data accessed), *not* human statements and so not hearsay. See also log-in records from Internet service providers, telephone records, ATM receipts, computer generated metadata.
  1. But do need foundation computer was operating properly at the time. *Hawkins*, 121 Cal.Rptr.2d 627 (2002)
    a. To be precise, we'd want to know about each of these:
      i. Source
        1. Modules are commonly reused from one environment to another—and,

commonly, the code is not suited to the
new environment
- ii. Compiler
- iii. Interpreter
- iv. Operating system
- v. *Interaction* of all these
- vi. In general: Turing/halting problem etc.-
practically impossible to prove no defects.
- b. But courts don't usually require this level of detail. And
we can't afford the time or resources
- 2. Note: 'machine statements' often trace back to *human*
programming-- human statements, perhaps? But not that which
is coming in for the truth of the matter. How to cross examine
the algorithm.
- iv. Operative Fact doctrine, e.g.,
- 1. An e-mail sent by X to Y "I accept" contract. Not to prove the
truth of any facts asserted but just that the words were
transmitted
- 2. Invoices sent from X to Y to establish the nature of their
relationship, not as proof for the truth of the matters stated in the
invoice
- d. EV 352
- i. Massive visual impact alone can be problem as well as benefit
- ii. The 'authority' of the computer generated document
- iii. Recreations and animations
- 1. prejudice? too confusing?
- a. Even color choice might matter
- b. Graphs and charts- number manipulation
- 2. Too much time to handle? Too many experts needed?
- iv. Lies, damn lies, and statistics
- v. Low amount of $ at stake- let's not make it too costly to authenticate
- vi. Re: core issue? > get it right, spend $ to ensure authenticity
- vii. So: small case where computer data is core?? (e.g. credit card collection)
- viii. How much time (how many witnesses) will it take to get over
admissibility hurdles? Is it worth it?

- e. One 'part' comes in -- so does the rest…. EV 356
- f. Compilation? EV 1340- if relied on as accurate in a business. "Fast lane" biz
record

D. Key Role of Advanced Preparation
- a. See above re 'bypass the issues'
- b. RFAs to get ok on authenticity (fees if OK improperly refused)
- c. Depositions of those who can authenticate
- d. Stipulations
- e. Advance exchange of
- i. simulation and animations and underlying data
- ii. all e-docs

E. Use of Experts
- a. Will they really qualify -- for the purpose they are presented?

b. Experts testifying
　　　　　　i. Experts can rely on *inadmissible* materials
　　　　　　ii. Experts can rely on materials *not* entirely reliable (Wikipedia case)(SDNY 2007)
　　　　c. Experts assisting other testimony
　　　　　　i. Presentations, re-creations, animations: multiple 'experts'
　　　　　　　　1. Underlying data collection & storage
　　　　　　　　2. Scientific principles which translated data to visual
　　　　　　　　3. Prior disclosure to opposing side- enough time to analyze?
　　　　　　　　4. Explain digital signature technology
　　　　　　ii. Forensics
　　　　　　　　1. Encryption
　　　　　　　　2. Recovery
　　　　　　　　3. Chain of custody
　　　　　　　　4. Explain digital signatures

　　F. Contact with the court
　　　　a. In single assignment, confer with court long before trial
　　　　b. Use targeted motions in limine
　　　　c. Consider: limited admissibility

Cases
- *Lorraine v. Markel American Ins. Co.,* 241 F.R.D. 534, 538 (D.Md. 2007)
- *Perfect 10, Inc. v. Cybernet Ventures, Inc.,* 213 F.Supp.2d 1146 (C.D.Cal. 2002)
- *United States v. Tank,* 200 F.3d 627, 630 (9th Cir. 2000)
- *People v. Lugashi*, 205 Cal. App. 3d 632, 252 Cal. Rptr. 434 (1988)
- *In re Homestore.com, Inc. Sec.Litig.,* 347 F.Supp.2d 769, 782 (C.D.Cal.2004)(To authenticate printouts from a website, the party proffering the evidence must produce "some statement or affidavit from someone with knowledge [of the website] ... for example [a] web master or someone else with personal knowledge would be sufficient"); *as cited by* ST. LUKE'S CATARACT AND LASER INSTITUTE v. SANDERSON, (No. 8:06-CV-223-T-MSS. May 12, 2006)(M.D. Fla.)
- *Nightlight Systems, Inc. v. Nitelites Franchise Systems, Inc*. 2007 WL 4563875, 6 (N.D.Ga.,2007)("In addition to a witness with personal knowledge of the web page at issue, to authenticate a printout from a web page, the proponent must present evidence from a percipient witness stating that the printout accurately reflects the content of the page and the image of the page on the computer at which the printout was made.")

The 352 nightmare: multiple experts needed
Hypo: frequency of pings from certain remote locations indicate attack, intent to disrupt.
- Forensic recovery of deleted data from drive
- Explain server log: how entries are made
- Explain relationship between logs and specified sites
- Data selection: criteria
- Frequency analysis. Kelley//Frye?, generally accepted in scientific community?
- Someone to explain the graphic

Resources on Technology in the Courtroom
- Effective Use of Courtroom Technology: A Judge's Guide to Pretrial and Trial
- http://www.fjc.gov/public/pdf.nsf/lookup/CTtech00.pdf/$file/CTtech00.pdf
- http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/schofield
- http://criminaldefense.homestead.com/Technology.html
- Harold Weiss & J.B. McGrath, Jr., Technically Speaking: Oral Communication for Engineers, Scientists and Technical Personnel (1963)(72 hours typical jurors will retain only 10% of verbally presented information)
- Dr. Damian Schofield, "Animating Evidence: Computer Game Technology in the Courtroom," http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/schofield (includes references to many studies)
- K. Fulcher, "The Jury as Witness: Forensic Computer Animation Transports Jurors to the Scene of a Crime or Automobile Accident," 22 U. Dayton L. Rev. 55 (1996), http://heinonline.org/HOL/Page?handle=hein.journals/udlr22&div=9&g_sent=1&collection=journals
- E. Tufte:
  - http://www.edwardtufte.com/tufte/
  - Books: Beautiful Evidence; Envisioning Information

The Everything Will Fail Rule:
- Set aside time to set up
- Some s/w may not show all elements (various versions of PowerPoint)
- Counsel must have rehearsed. Practice practice practice
- Extra plugs, cables, etc. thumbtacks, projector, screen, pens, marker pens, extension cables…..
- Counsel must have back up plan (paper, foam-core boards, copies for handouts, etc.)
- Assume light projectors will fail
- Assume CD ROM drive will fail
- Video screen quality- lights in the courtroom might not turn off, or judge may not allow dark courtroom (serious security issue in criminal case)
- Audio quality- can everyone hear? Did lawyers bring speakers?
    – Use transcripts to follow along

The Power of Low Tech
PowerPoints and the *distractions* of technology.
- Remember the shuttle O ring (KISS).
- Smooth transitions down the technology ladder (paper!)
- Required Reading: Edward Tufte, The Visual Display of Quantitative Information and his other works.
- What is the *lowest* technology that works?
    - Less likely to break
    - Judge more likely to be familiar, comfortable with it
    - Won't alienate juries as big spender
    - More like to work in the courtroom (which one you can't predict)