March 06, 2011

The Beginning of the End for Current Practice in Digital Forensic Recovery?

That's the title --without the question mark-- of a report appearing in the Journal of Digital Forensics, Security, and Law (JDFSL). If there was a question, I think the answer is an emphatic Yes, and it affects both technologists and attorneys alike.

SSDs changing the technical and legal landscape

The report posits --and I agree-- that the fact we computer forensics analysts have had access to a treasure trove of evidence found as deleted files and slack file space was just good fortune taken for granted, because the natural state of modern digital storage is not to 'preserve deleted data' as magnetic drives have done for the past few decades, but rather to purge deleted files to improve read and write speeds.

According to the article, we should be aware that a "paradigm shift" is taking place in technology storage from magnetic hard drives to solid-state drives (SSDs); that solid-state drives have the "capacity to destroy evidence catastrophically under their own volition;" that it is "imprudent and potentially reckless to rely on existing evidence collection processes and procedures;" and that conventional assumptions about the behaviour of storage media are no longer valid. *Id.*

Why computer forenscis analysts should care about SSDs:

In summation, report authors Bell & Boddington note that the latest generation of SSDs on the market (of which I own three) use firmware controllers to equally distribute data across the drive's blocks, so that they're being accessed and used with equally over time; and they use a "garbage collection" process to identify deleted or slack file data so as to make these blocks available for reuse subject to the aforesaid equal allocation. The authors further posit that, because the garbage collection runs within the SSD (just by turning it on), using a write-blocker on the SSD during an investigation will have no effect -- *i.e.,* evidence spoliation will resume as soon as the SSD is energized (which it must be to retrieve data from). The end-result is that deleted data and slack-file evidence, which historically has yielded an abundance for fruit in digital forensics investigations, is no longer persistent.

Why litigators should care about SSDs:

The following may be welcome news to defense attorneys, as authors Bell & Boddington warn:

- that data stored on all types of solid-state drives "should be immediately and henceforth considered to be a 'grey area' as far as forensic recovery and legal validation are concerned until extensive studies have been made of drive and data behavior;"
- that evidence spoliation may take place extremely suddenly, extremely quickly and automatically without human awareness or control;

- that present-day evidence indicating 'no data' does not authoritatively prove that data did not exist at the time of capture;
- that evidence of deleted data being permanently erased or partially corrupted is not evidence of intentional permanent erasure or corruption;
- that hashes not matching at the end of a forensic analysis should be evaluated to establish if the original or subsequent images could have been taken during or after a garbage collection;
- that past metadata and data blocks may be deleted without warning and without the opportunity to realise that they had existed at time of capture;
- that quick-formatting of disks is a reasonable activity that an innocent person might choose to do to improve performance, tidy up a disk, *etc.,* yet may completely eradicate evidence from a disk within minutes;
- that there are no longer any guarantees for previously deleted file data to be preserved on an SSD, regardless of whether the drive image was taken during a 'live' capture of evidence or following a 'dead' capture of evidence;
- that drives can clearly self-modify their data after physical evidence has been gathered, despite best practice efforts by forensic analysts to prevent such behavior using traditionally effective write-blockers;
- that it would be an unwise investment of time for analysts to try to develop workaround procedures that operate against the drive controller behavior specifically identified, because new firmware & models are regularly released;
- that it would be imprudent to develop procedures for physical asset capture whereby operators attempt to distinguish SSDs from HDDs, because of the similar physical appearance of the drives and the need to gain access to the computer's internals, and because hybrid disks incorporate both HDD and SSD technologies;
- that it is unwise to assume that irreversible file erasure suggests intent to destroy evidence in cases where a defendant has quick-formatted a SSD drive prior to police seizure; and
- that the issues identified in the Bell & Boddington report will later come to affect large USB flash drives as well.

Mobile Devices Changing the technical and legal Landscape

Perhaps needless to say, mobile devices are pervasive and, to a growing extent, replacing traditional PCs in the home. Some PC users, who have been besieged with and befuddled by malware, spyware, computer viruses, and maintaining a complex operation system (*viz.* Microsoft Windows), have replaced their computers with tablets and other devices, including Apple's iPad, Sony WebTV, Samsung Galaxy, *inter alia.* Some people I know have even substituted their trouble-prone PCs with ordinary smart-phones (iPhone, Android, *inter alia*).

Because mobile devices use a variety of operating systems, file systems, and data storage models; and because some are proprietary and, perhaps, not subject to standards (or, at best, subject to rapidly evolving standards); and because some use proprietary hardware connections and protocols, an ordinary computer forensics analyst with expertise in Windows, Macintosh, or Linux has not the skills, software, or hardware to conduct a competent analysis. Further, the technology is evolving and being released with blinding speed.

Cloud Computing Changing the technical and legal Landscape

Cloud computing is defined by the National Institute of Standards and Technology (NIST) as “a model for enabling convenient, on-demand network access to a shared pool of

configurable computing resources (*e.g.,* networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

For companies, this may mean entrusting either data or computing resources or both to other companies' data centers, like Microsoft (NASDAQ:MSFT), Salesforce (NYSE:CRM), or EMC (NYSE:EMC). For private individuals, it may mean entrusting personal data from their computer or mobile devices to, for example, Apple's MobileMe, or Motorolla's Motoblur.

Cloud computing raises digital evidence challenges regarding the location of potential responsive data, preservation, and analysis. Because data can be stored anywhere in the world, it may reside in a jurisdiction where subpoena power or privacy laws are non-existent or not enforced, and establishing a chain of custody might prove difficult or impossible, where data integrity and authenticity (where was it stored, who had access to it, was data leaked, was the data commingled, *etc.*) cannot be fully ascertained. Moreover, data entrusted to the cloud may be logically (and certainly physically) disassociated from the local metadata usually accompanying it (*e.g.,* registry entries, temp files, *etc.*) and which may not exist in the virtual/cloud environment. For example, modifying data in a cloud environment, rather than locally, might be less likely to result in metadata written to a client device's hard-drive (if it has one), and more likely to reside in the packets and client or host server logs, if applicable.

Conclusion

The foregoing is a summary, not an exhaustive discussion, of three challenges facing the discipline and profession of digital forensics examinations and electronic discovery. Computer forensics examiners will be hard-pressed to stay current, to diversify, and to rely on a network referral partners in order to understand and meet their clients' needs. Lawyers will need to understand how these developments may hurt or help their clients' causes, and to become even more vigilant in selecting a digital forensics consultant to identify what expertise is needed in a particular case. finally, it will be the lawyers' responsibility, and not the experts or the courts, to understand these developments and the judiciary on its import, lest the outcome of justice be the result of ignorance.

Posted by Sean Harrington on March 06, 2011 at 04:59 PM in Articles, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

February 18, 2011

Twin Cities Bank Avails Itself of Seldom-used Safe Harbor Provision

Perhaps it's safe to assume that many employees of any company might have have been inconvenienced, if not annoyed, if an automated, compulsory e-mail deletion policy went into effect.

Such a policy, implemented in many corporations across America in contemplation of the December, 2009 federal rules amendments affecting e-discovery practice, was effectuated throughout U.S. Bank's Lotus Notes e-mail system in 2009, permanently deleting electronic mail aged 90 days thereafter. The policy complimented a mature litigation hold procedure, about which all bank employees receive mandatory training.

So, when a 21-year old veteran of the bank filed an employment discrimination suit against the bank following termination of her employment, the issue arose as to the whereabouts of certain erstwhile e-mails. This in turn required a determination as to when the bank's duty to preserve evidence attached.

Plaintiff contended that a letter she wrote to the human resources dep't triggered the duty-to-preserve. Although the court in this case (Viramontes v. U.S. Bancorp *et al.,* 2011 U.S.

Dist. Lexis 7850 (N.D.Ill. January 27, 2011)) did not explicate in detail when the duty to preserve attaches, it ordinarily does whenever a reasonably credible threat of litigation is received or, based upon the totality of the circumstances, it would appear to a reasonable person that litigation concerning a dispute is more likely than not. *See, generally,* Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y., 2003) ("Zubulake IV").

Here, the court found that a complaint letter to human resources, which did not so much as hint as litigation, did not trigger the duty to preserve and, therefore, the filing of the EEOC complaint was the effective date.

In light of the effective date when the bank's duty to preserve was triggered, the court found that the safe harbor provision of Fed.R.Civ.P. 37(e) insulated the bank from spoliation sanctions. The so-called safe harbor provision provides insulation from sanctions where evidence has been spoliated as a result of routine, good-faith operation of an electronic information system, rather than spoliation from bad faith or recklessness.

Posted by Sean Harrington on February 18, 2011 at 02:42 PM in Caselaw | Permalink | Comments (0) | TrackBack (0)

January 27, 2011

Rule 11, barratry, champerty, and "inline links"

When's the last time --in an intellectual property case or *any* case-- you've heard of counterclaims of champerty (an improper arrangement where a party with no interest in a lawsuit agrees to finance and bear the expense of litigation in exchange for a portion of the proceeds) or barratry (creating legal business by stirring up disputes and quarrels, generally for the benefit of the lawyer who sees fees in the matter)?

Perhaps it's long overdue. These are the counterclaims now being levied against the specious litigation mill, Righthaven, LLC. Righthaven, which is co-owned by Vegas attorney Steven Gibson and Stephens Medial, LLC, has an interesting [alleged] lawsuit business model: First, it scours the Internet for copyrighted content owned by its newspaper clients, including Fair Use multi-line excerpts of articles (not entire works). Next, the newspaper-client licenses the work to Righthaven. Righthaven then sues --without any takedown request-- the party alleged to have infringed the work. Many, if not most, of the 215 suits filed so far in the U.S. Court for the District of Nevada are mom & pop bloggers. As part of its business model, Righthaven claims damages of up to $150,000 under the Copyright Act's statutory damages provisions and demands transfer of the Web site domain to Righthaven. These threats have been successfully used, thus far, to intimidate some defendants into a quick settlement.

Righthaven has already lost one or two suits under Fair Use. In *Righthaven v. Realty One Group, Inc.,* the court granted a Motion to Dismiss on Fair Use grounds. As aptly argued, by counsel for *Realty One*:

> Plaintiff brings these claims with unclean hands, which mandates dismissal of this action. The defense of unclean hands can be invoked as a defense in a copyright infringement action. See 4 Nimmer on Copyright § 13.09[B]. The actions of Plaintiff Righthaven in pursuing the instant action for copyright infringement smack of barratry. Righthaven was created by its counsel, Steven Gibson, apparently to pursue violations of the copyrights it purchased from the Review Journal. Righthaven is not the author of the work that was alleged to have been copied. In fact, Righthaven purchased the copyright in the Program Article sometime after the alleged infringement occurred, and likely purchased the copyright with the specific intention of pursuing this action against Mr. Nelson.

The barratry claim was not reached in *Realty One,* because the case settled one day before the Order granting the Motion to Dismiss issued. But, separately, a judge in *Righthaven LLC v. Center For Intercultural Organizing* sua sponte ordered Righthaven to show cause why the case should not be dismissed under the 17 U.S.C. § 107 Fair Use exception. The show cause hearing is set for February 10, 2011.

And most recently, counsel for Choudhry and Pak.org --in addition to filing a Motion to Dismiss-- filed separately an Answer and counterclaim for, *inter alia,* "barratry, champerty, and maintenance."

Technologically, *Righthaven v. Choudhry* may be interesting, because Righthaven is suing for an allegedly protected work that *appeared* to exist on Choudhry's site, but which Choudhry alleges actually was not hosted by his site. In the Motion to Dismiss, Choudhry's counsel explains that the image was substituted in by the client's browser by means of an "inline link . . . by virtue of an automated RSS feed published by a third party." Choudhry defined inline link as, "a line of computer code used in internet web pages to direct a user's browser program to a third-party site to retrieve an image directly from that thirdparty site." Relying on *Perfect 10, Inc. v. Amazon.com, Inc.,* 508 F.3d 1146, 1160-1161 (9th Cir. 2007), Choudhry argued that inline linking does not reproduce, distribute, or display copyrighted material. Rather than providing an image directly to an end user, inline linking directs the web browsers of its users to load content from a third party source. Thus, it is the third party that is reproducing, distributing, or displaying any allegedly infringing image, not the provider of the inline link.

More importantly, the *Choudhry* case, and others appear to demonstrate a lack of a good faith inquiry into the facts, as required by Fed.R.Civ.P. Rule 11. The *pro se* defendant in *Righthaven v. Eiser,* argued as much, when she alleged in her response that she did not post the newspaper column at issue, and that Righthaven's suit "was undertaken without any diligence in determining the facts or party allegedly responsible for placing the allegedly owned and copyrighted article on the Internet weblog."

Posted by Sean Harrington on January 27, 2011 at 11:42 PM | Permalink | Comments (0) | TrackBack (0)

Is the Attorney Client Privilege a Substitute for Reasonable Expectation of Privacy in the Workplace?

This is a brief mention about yet another case, *Holmes v. Petrovich, LLC,* announced last week, concerning whether an employee enjoys a reasonable expectation of privacy when sending and receiving personal e-mails while using corporate resources. I last wrote about this topic in March of last year, concerning *Stengart v. Loving Care Agency,* 990 A.2d 650 (N.J. 2010), and in June, 2008, I discussed *Quon v. Arch Wireless,* a Ninth Circuit decision that established, among other things, that employers could not obtain the contents of employee emails or text messages from a service provider without employee consent, pursuant to the Stored Communications Act. And, in December, 2007, I discussed *Long v. Marubeni America Corporation,* 2006 WL 2998671 (S.D.N.Y., October 19, 2006), where that court held that both the attorney client and work product privileges were waived by employees using a company computer system to transmit otherwise privileged communications to private counsel, which communications were sent from private password-protected accounts (not from the employer's email system).

In *Marubeni America Corp.,* a cache of the emails were retained by the company's system as "temporary internet files." Because the company could and did obtain these emails by reviewing its own system, the court held that the waiver was created through employees' failure to maintain the confidentiality of these communications with regard to the company's electronic communications policy, which policy advised employees not to use the company system for personal purposes and warned that they had no right of privacy in any materials sent over the system. The court reached this result notwithstanding its factual finding that employees were without knowledge that a cache of their email communications had been retained.

In *Stengart, supra,* plaintiff was provided with a laptop computer to conduct company business. From the laptop, she had access to the Internet through the employer's server,

and she used her laptop to access a personal, password-protected Yahoo! e-mail account, through which she communicated with her attorney about her situation at work. She never saved her Yahoo ID or password on the company laptop. Because plaintiff, "plainly took steps to protect the privacy of those e-mails and shield them from her employer . . . us[ing] a personal, password-protected e-mail account instead of her company e-mail address and . . . not sav[ing] the account's password on her computer," the court ruled she had a subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future lawsuit, and that defendant's lawyers violated RPC 4.4(b) in reading those e-mails.[1]

Although I am a privacy advocate, I don't mind mentioning that --in my opinion-- the New Jersey Supreme Court used reasoning of dubious providence to preserve the sanctity of the attorney-client privilege. That may be laudable (in our profession), but doubtful reasoning does not provide clarity or certainty about what doctrines and principles truly govern the outcome of these cases from one jurisdiction to the next, and --as the *Stengart* case demonstrated-- attorneys can be subject to discipline based on how a particular court chooses to view the issue.

An example of such reasoning is where the *Stengart* court explained:

> Unbeknownst to [plaintiff], certain browser software in place automatically made a copy of each web page she viewed, which was then saved on the computer's hard drive in a "cache" folder of temporary Internet files. Unless deleted and overwritten with new data, those temporary Internet files remained on the hard drive.

Whether plaintiff knew that the browser created a cache of the Web pages she visited is irrelevant. In child pornography cases, for example, the trend has been for courts to disregard defendants' knowledge of browser software caching, because liability should attach to defendant's act of "reach[ing] out to the Internet through use of a web browser" to obtain the content. Ty E. Howard, *Don't Cache out your Case,* 19 Berkely Tech. L.J. 1227 (2004). Likewise, an employee has relinquished dominion over information (and assumed risk) by using a company-owned computer, and volitionally placing the unencrypted information into the company's information stream.

Moreover, plaintiff had been advised, "The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice. . . . . E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee."

Yet the court ruled that "The scope of the written Policy . . . is not entirely clear." Why? Because, said the court, the policy did not specify whether the use of personal, password-protected, web-based e-mail accounts via company equipment is covered. *Id.* Because the Policy used "general language" to refer to its "media systems and services" but didn't define those terms. *Id.* Because the policy did not warn employees that the contents of such e-mails are stored on a hard drive and can be forensically retrieved and read by the employer. *Id.*

So, let's get this straight: To have an effective policy, and to purge an employees' "reasonable expectation of privacy," an employer must explicate in detail every fact scenario that is in-scope for the policy, what is meant by network media systems and services, and, further, the policy must disclose: the nature and character of the monitoring software that is in use by the company, the inherent caching functionality of the browser software that is installed on the workstations throughout the enterprise; and an explanation of how the operating system stores files and [fails to] delete files?

Yet, just one year earlier, a lower New Jersey appellate court, citing several federal cases, ruled "we conclude that defendant had no reasonable expectation of privacy in the personal information stored in his workplace computer." *State v. M.A.,* 402 N.J. Super. 353 (App. Div. 2008) (which has not been overruled). If you read that decision, much emphasis is placed upon the fact that the computer was owned by the company, and that employees were warned that the company reserved the right to monitor communications --facts no different than *Stengart.* Indeed, the only difference is that in *State v. M.A.,* the court found

that, even if defendant had a subjective reasonable expectation of privacy [as later was conferred to plaintiff in *Stengart*], he lost that expectation because he was using the computer for criminal activity ("A burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate'").

Last week, the California court in *Petrovich, supra,* which considered *Stengart,* and distinguished *Stengart* as a dissimilar fact situation, ruled that an employee who used the employer's computer and corporate e-mail account (in violation of corporate policy) to communicate with her lawyer, and having been advised that the employer randomly monitors e-mail usage, was analogous to the employee consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard.

---

[1]Curiously, even `though the court did not formally refer the matter to attorney regulation counsel, and even `though a violation of the Rules of Professional Conduct does not give rise to a private cause of action, the court remanded the case back to the trial court to fashion an "appropriate remedy," on the basis of the violation.

Posted by Sean Harrington on January 27, 2011 at 07:32 PM in Caselaw | Permalink | Comments (0) | TrackBack (0)

March 31, 2010

Attorney Who Read Password-Protected and Privileged E-Mails on Company-owned Laptop Violated RPC

Hat tip to *The Legal Profession Blog*:

From Stengart v. Loving Care Agency, Inc. (NJ, *en banc*) (March 30, 2010):

> This case presents novel questions about the extent to which an employee can expect privacy and confidentiality in e-mails with her attorney, which she sent and received through her personal, password-protected, web-based e-mail account using an employer-issued computer.

The Court held that an employee "could reasonably expect that e-mail communications with her lawyer through her personal, password-protected, web-based e-mail account would remain private, and that sending and receiving them using a company laptop did not eliminate the attorney-client privilege that protected them." Employer's counsel violated Rule 4.4(b) by reading those e-mails and failing to promptly notify the employee. The court noted that no reported New Jersey decision offered direct guidance on the issue.

Posted by Sean Harrington on March 31, 2010 at 03:49 PM in Caselaw | Permalink

March 24, 2010

Why Divorce Lawyers Should Get Up to Speed on CyberCrime Law

One of my clients, a Texas divorce law firm, recently presented the following fact situation to me, which prompted me to write this article:

> Lawyer accepted a case where client (hereinafter "wife") surreptitiously took husband's laptop three or four months ago while the parties were still residing together, and had it forensically imaged by a private investigator.[1] Wife intends to present evidence obtained from the laptop in support of her petition for marital dissolution.[2]
>
> Issue: Is the lawyer precluded from introducing evidence and does the lawyer incur any malpractice, tort, or attorney disciplinary liability in possessing, viewing, or proffering evidence obtained from the laptop?

My conclusions —based on somewhat cursory research— appear immediately below. I've provided some annotations as footnotes for application in Minnesota (for academic discussion purposes only, not as legal advice). I found very little in the way of Minnesota published cases regarding unauthorized computer access. *See, e.g.,* In re Trudeau, 705 N. W.2d 409 (Minn. 2005) (attorney discipline conditional admission based, in part, on respondent's unauthorized computer access by installing and using an email spyware program).

(1) If husband's laptop was not an employer's computer, and if husband's laptop was not password protected by him (requiring wife or wife's private investigator to circumvent any security measure that would create a reasonable expectation of privacy), then wife probably had equal dominion over laptop, as a matter of law (*see* Texas statute re: "effective consent," *infra*). However, to whatever extent the court's evidentiary ruling is discretionary, the court might well frown on procurement of evidence through such means, and husband might attempt to invoke the Unclean Hands doctrine. This is even more likely so if that area of the hard-drive was password-protected (from wife), or if the laptop belonged to an employer.

(2) Unless some Texas Rule of Evidence and/or rule of Civil Procure (unknown to me) bars admissibility of evidence based upon "unlawful interception of communications," in a civil case (compare Tex. Code Crim. Proc. Ann. art. 38.23(a)) or based upon any violation of criminal or administrative law, and if wife's conduct in surreptitiously taking laptop for forensic imaging would not constitute an act of "interception" in violation of Tex. Penal Code Ann. § 16.02(b)(1) or unauthorized access under § 33.02, the evidence recovered from the hard-drive probably is admissible, subject to the court's broad discretion.

My conclusions are based on cases from around the country. Although, this fact situation does not appear to have been yet addressed Texas' appellate courts, I did find the following authorities and analysis helpful:

> • Tex.Penal Code Ann. § 33.02 ("A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner").[3]
>
> • Tex.Penal Code Ann. § 33.01(12) ("'Effective consent' includes consent by a person legally authorized to act for the owner. Consent is not effective

if: (A) induced by deception, as defined by Section 31.01, or induced by coercion . . . (E) used for a purpose other than that for which the consent was given").[4]

• Tex.Penal Code Ann. § 16.02(c)(4)(B). (It is an affirmative defense to prosecution a person not acting under color of law intercepts a wire, oral, or electronic communication and is one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing an unlawful act).

• Vaughn v. Drennon, 202 S.W.3d 308, 320 (Tex.App., 2006) (tort case, noting that the intrusion-upon-seclusion type of invasion of privacy is "generally associated with either a physical invasion of a person's property or eavesdropping on another's conversation with the aid of wiretaps, microphones, or spying")

• Signorelli v. State, 2008-TX-V0117.004 (In a criminal context, "Generally, when a third party has equal control over the thing to be searched, the third party may properly consent to the search.")

• Lasater v. State, 2007-TX-V0829.002 (discussing reasonable expectation of privacy and scope of consent, where defendant granted victim limited consent to enter his home, and victim searched for and found evidence she provided to law enforcement)

• *But see* Tave v. Alanis, 109 S.W.3d 890 (Tex.App., Dallas, 2003) (School district employee's termination affirmed, where employee accessed and subsequently disseminated confidential information (inadvertently left on a computer assigned to him for classroom use) violated the District's policy and constituted conduct could cause the public, students, or employees to lose confidence in the administration and integrity of the District).

So, whereas I found no Texas appellate cases that directly address the fact situation, the cases below from around the country do. In reading through these cases, the advocate should pay particular attention to "effective consent," (in Minnesota "without authorization," which phrase is defined under Minn. Stat. § 609.87(b)) and the meaning of the phrase "interception of electronic communications." Although some courts, have held that recorded screen-shots constitute "interception of electronic communications," (*e.g.,* O'Brien v. O'brien, *infra*), under the narrow reading of the Wiretap Act adopted by the Fifth, Ninth and Eleventh Circuits, very few seizures of electronic communications from computers will constitute "interceptions." Larue, Wiechman, Terry, & Turner, *Trails from the Aether: Cyber-Evidence,* (State Bar of Texas CLE, 2007). The advocate should also consider whether a violation of criminal law by wife (or wife's PI) could translate to liability to the firm as an "accessory after the fact," and that some judges in similar cases from other states based their discretionary decisions on whether the conduct in obtaining the hard-drive was an unlawful act.

(1) Bailey v. Bailey, 2008 WL 324156 (E.D. Mich)). In this recent case from the US District Court for the Eastern District of Michigan, the parties were married for nearly 30 years and had three children. Husband became suspicious of his wife's activities and installed keystroke logging software on both home computers, with which he was obtained wife's e-mail and instant-messaging passwords. Husband used these passwords to access her e-mail and messages and learned of her extra-marital activities. Husband fled the marital home with the parties' three children. He provided the e-mails and messages to his divorce attorney and petitioned for divorce. A custody dispute ensued and husband's attorney used the wife's e-mails to impeach her. Wife lost custody and was granted only supervised visitation. After the divorce action concluded, wife sued ex-husband, his attorney and her attorney. Husband and his attorney were sued for violation of (1) 18 U.S. C. §2511 (the Wiretap Act); (2) 18 U.S.C. §2701 (the Stored Communications Act) against husband; (3) 18 U.S.C. §2512 (Wiretap Act) against the husband, his attorney and a John Doe who supplied the keystroke logging software; (4) MCL § 750.539a *et seq.* and MCL §750.540 (Michigan's Eavesdropping statutes) against the husband, his attorney and John Doe; (5) invasion of privacy against the husband and his attorney; (6) intentional infliction of emotional distress against all defendants; and (7) malpractice against the wife's own attorney.

The Wiretap Act. Wife claim against husband and his attorney was based on their obtaining her e-mails and messages using the password retrieved from the key logger software. Under § 2511 (1)(a), a person violates this Act if he or she "intentionally intercepts…any…electronic communication" (c) "intentionally discloses…any…electronic communication…knowing…the information was obtained through the interception of a … electronic communication in violation of [the Act]" and (d) intentionally uses…any… electronic communication" (c) "intentionally discloses…any…electronic communication… knowing…the information was obtained through the interception of a …electronic communication in violation of [the Act]" Defendants successfully argued that there was no "interception" as defined in the Wiretap Act. The court agreed and reasoned that the key logging software only allowed the husband to learn his wife's passwords, which he then used to access her e-mail. Since the husband did not obtain the e-mails and messages contemporaneously with the transmission, the court ruled the Wiretap Act was inapplicable. The court also ruled that that § 2512 of the Act does not provide for a private right of action and the court dismissed wife's claim based regarding husband, his attorney and a John Doe who supplied the key logger software.

Stored Communications Act. Wife contended her husband violated the Stored Communications Act by accessing her e-mails. The Act provided that a person was in violation if that person (a)(1) "intentionally accesses without authorization a facility through which an electronic communication service is provided…and thereby obtains…a… electronic communications while it is in electronic storage in such system…" Although husband accessed the wife's e-mail on her Internet service provider's (ISP) server and not from the messages stored on her home computer, he argued, because wife had already accessed her e-mails, the Act was inapplicable. But, the court found that the messages on the ISP's server were stored for purposes of backup protection (since the wife had already accessed those messages) but that does not take it out of the provisions of the Stored Communications Act and therefore the husband's motion for summary judgment on this count was denied.

Invasion of Privacy tort claim: The court granted husband's attorney's motion for summary judgment because there was no evidence the attorney participated in the "intrusion of another's seclusion," as alleged by wife. But, the court stated that the wife had a right to privacy in her private e-mail account. Husband's defense was that wife could not establish her claim because his actions were not objectionable to a reasonable man, because they were subsequent and based upon his inadvertently discovery of wife's extra-marital activities, and because they were necessary and prudent to protect his family and children. The court found that an issue of fact existed as to whether or not use of keystroke logging to gain access to the wife's e-mail was objectionable to a reasonable man. Intentional Infliction of Emotional Distress tort claim: The court dismissed wife's IIED cause-of-action because the use of the key logger did not constitute "extreme and outrageous conduct."

(2) In Moore v. Moore, (NYLJ, August 14, 2008, at 26, col 1 [Sup Ct, New York County]), a New York County trial court recently ruled that a wife seeking a divorce can use evidence of her husband's internet activities with another woman which she found on a computer she took from her husband's car.

The Moore's were married in 1963. Wife took a laptop computer from husband's car just before she petitioned for marital dissolution. According to wife's attorney, she was searching the computer for financial information when she came upon a large number of salacious instant messages which the husband exchanged with a woman in Texas.

Wife's counsel informed husband's counsel she had the computer, and the parties agreed to make forensic images from of the computer's hard drive. The materials found on the hard drive were repeatedly referred to by the wife in affidavits submitted to the Court without objection by husband.

Subsequently, husband moved to suppress the contents of the hard drive. The Court denied the motion, finding that the wife did not commit a crime or otherwise violate the husband's rights in taking the computer and copying its contents.

The Court noted that the attorneys for the parties specifically agreed to image the hard drive, and husband waived his objection by not timely moving to suppress the evidence. The Court determined that the computer was a family computer and not a work

computer as alleged by the husband. The Court also found that the taking of the computer was appropriate since it was done before the commencement of the dissolution case and was taken from the family car.

(3) In O'Brien v. O'Brien, 899 So.2d 1133 (Fla.App. 5 Dist. 2005), a Florida appeals court ruled that wife "illegally obtained" records of husband's Internet conversations with another woman as the two played Yahoo Dominoes online. "It is illegal and punishable as a crime under (state law) to intercept electronic communications," wrote the panel.

The court barred wife from revealing the contents of the intercepted conversations, and said the chat records could not be introduced as evidence in the divorce proceedings. At issue in a civil case arising out of the divorce proceedings was whether the use of the spyware, called Spector, violated Florida's wiretapping law, which provides that a person who "intentionally intercepts" any "electronic communication" commits a criminal act.

Wife's lawyers argued that the monitoring didn't fall under the law's prohibitions and was kin to reading a stored file on her husband's computer--which would not be treated as wiretapping. But the court concluded, "because the spyware installed by the wife intercepted the electronic communication contemporaneously with transmission, copied it and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act."

(4) In Gurevich v Gurevich (2009 NY Slip Op 29191) the Supreme Court considered CPLR 4506 [5] in the context of matrimonial proceedings in which the wife sought to lead email communications obtained from her husband's email account after the service of the divorce action.

The parties had been married for 16 years prior to separation, during which husband had provided wife with the password to his email account, and during which both parties had access to each others email accounts. After separation, wife changed her email password, but the husband neither changed his, nor told or gave notice to the wife that she was not permitted to access his account.

Husband argued that wife was aware he used one password for all his computer accounts, and that she was unreasonable in her belief that, despite his not changing his password until some two years after separation, she was allowed to access his accounts. Husband argued that the content of his emails were inadmissible under CPLR 4506 by reason that the wife had acted unlawfully under Penal Law 250.05 (hereinafter "eavesdropping statute"). Further, husband argued that the initiation of the divorce proceedings was an implied revocation of any authority previously given to her to access his account. The Supreme Court rejected husband's contention, holding "there is no statute that would recognize an 'implied revocation upon service of a divorce action' and bar the use of the email 'stored.'"

The court examined the eavesdropping statute and CPLR 4506, and rejected wife's contention that CPLR 4506 did not apply to electronic communications:

> She relies on dicta in the case of Pure Power Boot Camp v. Warrior Fitness Boot Camp (587 F.Supp.2d 548 [SD NY 2008]) for the proposition that "[t]he plain language of the statute [CPLR 4506] seems to limit its application to the contents of the overheard or recorded communication[s]'" not electronic communication. However, the U.S. District Court further stated that "[u]ltimately, a determination of the meaning of CPLR § 4506 is unnecessary, and better left to the New York state courts." Furthermore, the court in Power Boot Camp v. Warrior Fitness Boot Camp in a footnote stated "Penal Law section 250.05 explicitly includes "electronic communication . . . ."

Husband argued that CPLR 4506 and the eavesdropping statute were not limited to communication or transmission, but also applied to "the intentional acquiring, receiving, collecting, . . . of an electronic communication, without the consent of the sender or intended receiver thereof . . ."

The Supreme Court considered cases cited by wife and the legislative intent behind the eavesdropping statute (to prohibit the interception of communications, not the access of stored communications) and found that she was entitled to rely on the content of the email transmission:

> It is this court's understanding from the reading of the statute, legislative history and case law that the purpose of Penal Law section 250.00 is to prohibit individuals from intercepting communication going from one person to another, and in this case an email from one person to another. In the case at bar the email was not "in transit," but stored in the email account. Even assuming the husband's facts, as stated, to be true, the wife may have unlawfully retrieved information from a computer; in violation of Penal Law 153.10 but there was no interception and accordingly fails to fall within scope of CPLR 4506 as presently written.

(5) [6] In White v. White, 781 A.2d at 87-88, the family computer and entertainment center were located in the sun room, where the husband slept; the wife and the parties' children often used the sun room to utilize the computer, watch television, and adjust the stereo volume. It was in the sun room that the wife discovered, fatefully, a letter from the husband to his girlfriend.

Shortly after the wife discovered the letter, she hired a private investigative firm, and unbeknownst to the husband-and without using the husband's password-the PI firm copied the husband's files from the computer's hard drive. Such files contained e-mail sent between the husband and his girlfriend, as well as images [uh-oh] that he viewed on [and apparently downloaded from] Netscape. It was only while being deposed during the divorce proceedings that the husband learned that the wife had accessed his e-mail; he had thought-incorrectly as it turned out-that his e-mail and attachments could not be read without his AOL password. Understandably concerned about his e-mails, the husband sought to suppress the electronic evidence, based on violations of the New Jersey Wiretap Act. The New Jersey court opined that, in order to understand the error of the husband's thinking, it was necessary to understand the technical workings of America Online Service ["AOL"], the husband's Internet Service Provider ["ISP], explaining as follows:

> [i]ncoming e-mails are received on the AOL e-mail server and are accessible to an AOL user only after dialing in and authenticating with the user's screen name and password. Also, a user cannot send an e-mail via the AOL server until he has similarly dialed in....AOL's server receives and maintains the e-mail until the recipient dials into AOL and accesses (seeks to read) his mail. In addition, an AOL user can save his e-mails and attachments on his computer's hard drive. AOL offers the Personal Filing Cabinet ["PFC"] feature, which is created automatically on the hard drive during the installation of AOL on the user's computer. The PFC is named for user's screen name...[A]n AOL user must voluntarily choose to save the e-mail, attachment or address to his PFC or address book. The AOL user can save e-mail, attachments, or addresses either by using the automatic AOL feature or manually. To save automatically to the PFC on the hard drive, the user must select that option in "Mail Preferences."
>
> Specifically, in the main tool bar, the user chooses "Mail Center," "Preferences" and then checks "Retain All Mail I Send in My Personal Filing Cabinet" and/or "Retain All Mail I Read in My Personal Filing Cabinet".... Additionally, in the "Notes" section of [the Help screens], AOL informs the user that he can read mail stored in the PFC when he is not signed onto AOL, i.e. the PFC is on the hard drive. Similarly... AOL informs the user that e-mail saved in the PFC will remain on the hard drive until the user deletes it.

Id. at 87-88.

Thus, the only way for the husband to be sure that his e-mail would be saved permanently was to use the PFC file on the his hard drive, because his e-mail could not be saved permanently on AOL's server. *Id.* at 88. Not knowing his e-mails were being saved, he took no steps to delete them, nor any steps to protect them with a password,

which meant that any computer user could view his PFC and e-mails by simply opening the AOL software on the hard drive, and that was exactly what happened: the wife' s expert simply opened the AOL software and viewed and copied the husband's emails.

Turning to the legal issues in the case, the New Jersey court first held that the doctrine of interspousal immunity was inapplicable, and that the New Jersey Wiretap Act applied to unauthorized access of electronic communications of one's spouse. *Id*. at 88.

Next, the court noted that the New Jersey act [identical to the federal act] prohibited "access" to electronic information in "temporary, immediate storage," in backup protection, or in transmission. *Id.* at 89. The court observed that the e-mail in the hard-drive of the computer was in "post-transmission storage." *Id.* Pursuant to the statutory language, the court held that the New Jersey act was not meant to extend to e-mail retrieved by the recipient and then stored, but rather protected only those electronic communications which were in the course of transmission, or were backup to that course of transmission. *Id.* at 90.

The Court then rejected the husband's argument that the wife accessed his e-mail "without authorization." *Id.* Since other courts had held that "without authorization" meant using a computer from which one has been prohibited, or using another's password or code use the family computer, the court stated that nonetheless she had the authority to do so. *Id.* (citations omitted). Additionally, according to the court, the wife did not use the husband's password or code without authorization, but instead accessed the information in question by roaming in and out of different directories on the hard drive. *Id.*

Finally, the New Jersey court held that the wife did not "intercept" the husband's e-mails, since the concept of "interception" did not apply to "electronic storage." Id. at 91. The husband's electronic communications had already ceased being in "electronic storage," i.e., they were in post-transmission storage, and therefore the court held that the wife did not "intercept" them. *Id.*

Endnotes

---

1 Under Texas law, a person performing computer forensics analysis must be licensed as a private investigator in that state.

2 Texas is not a no-fault divorce state, and divorces may be tried to a jury.

3 *See* Minn. Stat. §§ 609.89 (Computer theft) & 609.891 (Unauthorized Computer Access, amended 2006).

4 Minn. Stat. § 609.891 uses the phrase, "without authorization"

5 Under CPLR 4506, (Eavesdropping evidence; admissibility; motion to suppress in certain cases), "The contents of any overheard or recorded communication, conversation or discussion, or evidence derived therefrom, which has been obtained by conduct constituting the crime of eavesdropping, as defined by section 250.05 of the penal law, may not be received in evidence any trial, hearing or proceeding before any court or grand jury, or before any legislative committee, department, officer, agency, regulatory body, or other authority of the state, or a political subdivision thereof; provided, however, that such communication, conversation, discussion or evidence, shall be admissible in any civil or criminal trial, hearing or proceeding against a person who has, or is alleged to have, committed such crime of eavesdropping."

6 The White v. White case digest is excerpted in its entirety from Larue, Wiechman, Terry, & Turner, *Trails from the Aether: Cyber-Evidence,* (State Bar of Texas CLE, 2007).

Posted by Sean Harrington on March 24, 2010 at 09:40 PM in Articles, Caselaw, Technology and the Law | Permalink

August 15, 2009

Catching up . . .

I've been negligent in posting here since the end of April because of competing priorities. Nevertheless, I've been scanning for news items with you in mind:

Sam Glover informs us at his *Lawyerist* blog (here) of a fantastic new Firefox plug-in called RECAP that, while a user is browsing documents in PACER, provides the option to download a free copy from public.resource.org (if the document exists there) by placing an icon next to the regular download link. Alternatively, if you download a document that isn't on public.resource.org, RECAP will upload the document thereto. More info. is at https://www.recapthelaw.org/

"*Judges and journalists have more in common than they probably realize: They search for the truth every day, they're never entirely sure who's lying to them and they routinely publish writings that live forever in the public record.*"\

So begins an article published by The First Amendment Center discussing the difficulty in determining who is a journalist, including "online contributors, bloggers and tweeters," and citing the recent Texas Court of Appeals decision in *Kaufman v. Islamic Society of Arlington,* where the court held that a contributor to a Web site was entitled to a statutory right of interlucutory appeal available to members of "the electronic or print media."

The court, finding support from other jurisdictions, extended the First Amendment and other protections to Internet publications as "a type of nontraditional electronic media." Although the court did hold that not everyone who publishes to the Internet qualifies under Texas' interlocutory appeal statute, the court rejected the argument that an Internet author never is a member of the media.

Here are some other news stories from the last few months that I thought you'd find interesting:

- Most recent developments regarding the former employee charged with stealing top secret code in Goldman Sachs' high-frequency trading program
- Report: Shortage of cyber experts may hinder govt
- Sec'y of Defense Creates Cyber Defense Command
- Bloggers, Beware: What You Write Can Get You Sued
- No Bail for Blogger Accused of Threatening Federal Circuit Panel
- Do Interactive Websites Have a Legal Duty to Remove Malicious Content?
- Law Students Teach Scalia About Privacy and the Web
- Supreme Court Will Hear Sarbanes-Oxley Challenge: Accounting Oversight Board Wields Too Much Power, Plaintiffs Say
- Government Secrets Found on Computer Sold on eBay
- Hackers into Virginia database demand $10M million ransom
- Prison Awaiting Hostile Bloggers? Proposed congressional legislation would demand up to two years in prison for those whose electronic speech is meant to 'coerce, intimidate, harass, or cause substantial emotional distress to a person
- Lawmaker Defends Imprisoning Hostile Bloggers
- Minnesota Court Orders Release of DUI 'Breathalyzer' Source Code
- Federal Reserve Tech Arrested
- Report labels U.S. Computer security "embarassing"

April 27, 2009

Another blogger seeks journalist status

A New Jersey Superior Court will decide in a defamation case whether a Shellee Hale, a woman who posted comments online about the pornography industry, should have the same protections as working journalists. Hale, who writes four blogs and has contributed to *The Wall Street Journal* and *Business Week,* is seeking protection from disclosing her sources.

Tom Cafferty, counsel to the New Jersey Press Association, suggested in an interview with *The Star-Ledger* that her claim to privilege may be dubious and contends that judges realize they must be careful who gets the protection, because If the newsperson's shield is extended to everyone who posts items on the internet, "then everyone is a journalist and the privilege becomes meaningless," he said.

This is a recurring theme that I have written about previously, and --doubtless-- will be revisited again. For one view on this topic, *see* Randall Eliason, Leakers, Bloggers, and Fourth Estate Inmates: The Misguided Pursuit of a Reporter's Privilege, 24 Cardozo Arts & Ent. L.J. 385 (2006).

Another view is that bloggers --many of them working anonymously-- have taken on an increasing role as vanguards of accountability and accuracy in public discourse. *See, e.g.,* Walaika Haskins, Bloggers Greatest Hits, Volume I & Volume II, TechNewsWorld (June 27 & July 11, 2007).

In a concurring opinion released earlier this month in *Andrew v. Clark* (4th Cir.), Judge J. Harvey Wilkinson, III, wrote:

> It is well known that the advent of the Internet and the economic downturn have caused traditional news organizations throughout the country to lose circulation and advertising revenue to an unforeseen extent. As a result, the staffs and bureaus of newsgathering organizations—newspapers and television stations alike — have been shuttered or shrunk. Municipal and statehouse coverage in particular has too often been reduced to low-hanging fruit. The in-depth investigative report, so essential to exposure of public malfeasance, may seem a luxury even in the best of economic times, because such reports take time to develop and involve many dry (and commercially unproductive) runs. And in these most difficult of times, not only investigative coverage, but substantive reports on matters of critical public policy are increasingly shortchanged.
>
> . . .
>
> The verdict is still out on whether the Internet and the online ventures of traditional journalistic enterprises can help fill the void left by less comprehensive print and network coverage of public business. While the Internet has produced information in vast quantities, speedy access to breaking news, more interactive discussion of public affairs and a healthy surfeit of unabashed opinion, much of its content remains derivative and dependent on mainstream media reportage. It likewise remains to be seen whether the web—or other forms of modern media—can replicate the deep sourcing and accumulated insights of the seasoned beat reporter and whether niche publications and proliferating sites and outlets can provide the community focus on governmental shortcomings that professional and independent metropolitan dailies have historically brought to bear.

MSBA Computer and Technology Law Section

The Official Blog of the Minnesota State Bar Association's Computer and Technology Law Section.

April 27, 2009

Employers Watching Workers Online Spurs Privacy Debate

A Wall Street Journal article of the same caption (above) was published April 23, 2009, regarding a case in New Jersey, where an employer obtained access to a private Internet forum where employees were disparaging the company's managements. The company then fired the employees involved.

It's generally well-settled that an employee has no reasonable expectation of privacy when the employer has disseminated a notice that use of company equipment is a waiver of that right. However, in this case, no such notice was given. Nevertheless, it's not clear (to me) whether a claim could be made out, if plaintiffs asserted that the injury-in-fact was employment termination.

The plaintiffs allege common-law invasion of privacy and "accessing without permission the electronic communications being stored on the plaintiff's private group," in violation of the Stored Communications Act, 18 U.S.C. 2701 *et seq.,* and a parallel state statute, N. J.S.A. 156A-27. Among other counts, they allege that management "used the improperly accessed and monitored electronic communications to wrongfully discharge the plaintiffs."

The case is *Pietrylo, et al v. Hillstone Restaurant Group,* No. 06-cv-05754 (D. N.J.).

Posted by Sean Harrington on April 27, 2009 at 02:58 AM in Technology and the Law | Permalink | Comments (1) | TrackBack (0)

March 31, 2009

Decrypt hard drive for gov't or face jail time

Over a year ago, I discussed a magistrate's opinion in a case captioned *in re Boucher,* which held that providing a PGP passphrase or otherwise decrypting an encrypted PGP volume to aid in a law enforcement investigation against one's self violated the Fifth Amendment. I'm amazed to discover that there is even a Wikipedia page for this case (here).

The magistrate's decision has been reversed by the U.S. Judge for the District of Vermont, directing defendant to produce the drive in an unencrypted form.

Because I need not attempt to duplicate Professor Orin Kerr's apt coverage of this latest development, allow me to point you to his commentary here.

Defendant's attorney, Jim Budreau, filed an interlocutory appeal to the Second Circuit.

Posted by Sean Harrington on March 31, 2009 at 11:16 PM | Permalink | Comments (0) | TrackBack (0)

March 30, 2009

No cryptographic hash analysis without warrant - How did I miss this one?

Between law school and the CISSP, CSOXP and CHFI exams, I guess I must not be doing a good job keeping up with current events. If I had, I would've known about this November decision from the the U.S. Court for the Middle District of Pennsylvania, where a judge is characterized in an article by Dan Goodin as saying, "*a hard drive is comprised of many platters, or magnetic data storage units, mounted together," and, therefore each platter constitutes its own separate container and the lawful acquisition of one didn't breach the others.*" What?!

Indeed, that genius bit of reasoning was the basis of a suppression order, finding that a landlord's eviction of a tenant and subsequent discovery of child pornography would have given way to a valid gov't seizure under the private search doctrine if prosecutors had limited their activities to the same file search employed by the landlord rather than a file-signature inventory.

I'm all for the Exclusionary Rule --which is on the brink of abolishment-- as a deterrent for police misconduct, but the problem with this reasoning is that the separate internal platters of a hard-drive are certainly not separate containers. Individual files are stored in sectors and often span across several platters. A Windows file search would access the same sectors that an EnCase hashing routine (discussed in the opinion) would access. The judge's reasoning would have been valid if there was more than one hard-drive in the computer and the landlord's search was confined to one, but the Government had accessed the others [without a warrant].

Whereas Goodin didn't pick up on this, I was relieved to discover that another blogger, Rich Cannata did. In his December 11, 2008 post, Rich wrote:

> *Wow. While the Judge deserves some recognition for an attempt at technical savvy, this analogy falls quite short. Under the guise of this analogy, the geometry of the hard drives platter's determined what is searchable and what is not. If the target is a 500GB Seagate drive with four platters and eight read/ write heads, is less data is to be considered within the scope of the search than if the exact same information were stored on a 500GB Samsung drive with one platter and two read write heads? If the data is stored on a RAID array, how do you determine which platters in which drives are within the scope of the search? The judge also skips over the fact that even in the Runyan case, there were two recording surfaces for each floppy disk. Since the introduction of MS-DOS 1.1, the Microsoft operating system has used both sides of a diskette, these are distinctly two separate recording surfaces of a floppy disk, yet it appears to the computer user as a single "container". Using the single platter logic, in the Runyan case, they would have only been within bounds to search the side of the floppy disk that contained the file that the third party found/viewed. In this context, it appears that a logical volume should be the boundary for a container, but, with the advances in drive density, considering this as a boundary is disconcerting.*

Posted by Sean Harrington on March 30, 2009 at 01:48 AM | Permalink | Comments (0) | TrackBack (0)

Plaintiffs must prove actual damages for statutory damages award under Stored Communications Act

According to a March 18th ruling by the Fourth Circuit, plaintiffs must prove actual damages in order to be eligible for an award of statutory damages under the federal Stored Communications Act, but that a showing of actual damages is not required for

awards of punitive damages or attorney fees. Plaintiff had sued under the Stored Communications Act, 18 U.S.C.A. § 2707(a), alleging that her former employer and its president illegally accessed her personal email account for over a year. *Van Alstyne v. Electronic Scriptorium Ltd., No. 07-1892.*

Further reading: Marcia Coyle, *E-Mail Theft Case Sparks First-of-a-Kind Ruling,* Law.com, March 27, 2009.

Posted by Sean Harrington on March 30, 2009 at 12:05 AM in Caselaw | Permalink | Comments (0) | TrackBack (0)

March 29, 2009

A dose of reality

Tomorrow afternoon, I am taking the CHFI exam. While studying through the official 2,721 page exam courseware, I encountered a "case study" that was laughable. Let me share it with you

> *TargetMac* and *OneMac* are two magazines that cater to the growing Ipod users. The CEO of *TargetMac* is Bryan Smith and the CEO of *OneMac* is John Beetlesman. Bryan calls John one day and convinces him to purchase *TargetMac.* The lawyers of both companies were called in to finalize the deal. The lawyers draft the sale contract, which restricts removal of sensitive and confidential information and non solicitation of *TargetMac* customers and working staff. A non compete clause was also added in the agreement.
>
> It has been two years and John Beetlesman is suspicious about Bryan's activities. John suspects Bryan has breached the contract. John knows that you are a CHFI professional and provide computer forensics services to his clients. John's company lawyer, Smith Franklyn, contacts you to investigate and provide evidence to support the breach of contract so that John can file a lawsuit against Bryan at local civil court in San Francisco, California.
>
> How do you investigate this incident?
>
> Answer:
>
> 1. You want to examine hard disk and laptop computers of Bryan's home and office for evidence.
> 2. You ask the lawyer Smith Franklyn to obtain a search and seizure warrant at Bryan's home located at 37 Albert Avenue, San Jose and his office located at 46, Mathew Street, Santa Monica.
> 3. Smith Franklyn works with the local District Attorney to obtain the required search warrant.
> 4. Smith Franklyn and you visit Bryan's home and seize his computer which is a HP Pavilion Model 1172.
> 5. You later visit Bryan's office and seize his laptop, floppy disks and CD-ROMS.
> 6. You place the devices carefully in anti-static bags and transport it to the forensics laboratory.
> 7. Create a bit-stream image of the hard disk using tools such as R-Drive and Linux dd commands.
> 8. Generate MD5 or SHA-I hashes of the bit stream images.
> 9. Prepare the chain of custody and store the original hard disk in a secure location. You would be investigating the bit stream image copy.
> 10. You are ready for investigation.
> 11. You are asked to retrieve: a. Any document in the computer which shows proof for breach of contract.
> 12. You load the bit stream image in AccessData Forensic Tool Kit (FI'K) and browse every single file in the file system.
> 13. You also read every single email displayed in FTK.
> 14. After many days/nights of investigation you retrieve the following crucial evidence:

a. Encrypted file titled "Business Plan AppleMac Magazine"
b. Excel spreadsheet "revenuestreams.xls"
c. Numerous email messages back and forth with his investors.

15. You run a password cracking utility to crack the encrypted file "Business Plan AppleMac Magazine.doc" and the password was "planapple".
16. These above documents clearly indicate that his new business would compete with *TargetOnes's* business.
17. You copy these files to a CD-ROM.
18. You use FTK report facility feature and produce a professional report.
19. You deliver the report to the company along with the fee for the forensics service you rendered.

Based on your submitted report the lawyer, Smith Franklyn initiates a $20 million lawsuit against Bryan. After two weeks the court of law holds Smith Franklyn Bryan guilty and asks to pay the amount.

In my judgment, this portion of the courseware was not written with the aid of an attorney. First, in a civil matter --contract breach-- one doesn't obtain a "search and seizure warrant" with the aid of the district attorney. A plaintiff first files suit, then issues a narrowly tailored request for production (or subpoena, if it is third-party property) and then awaits opposing counsel's Motion to Quash and for Protective Order.

Second, assuming the Court finds that the suit is not a fishing expedition (which this fact situation appears to be), an adverse would never be entitled to "visit Bryan's home and seize his computer . . . and later visit Bryan's office and seize his laptop, floppy disks and CD-ROMS." Instead, one would expect to retain a third-party vendor to search for potentially-responsive ESI or the court would appoint a special master for that same purpose.

This calls to mind a recent decision by the Colorado Supreme Court in November in the case of *Cantrell v. Cameron,* 195 P.3d 659 (Colo. 2008) (*en banc*). The case arose from a traffic accident in which the allegedly negligent party (Cameron) was accused of using his laptop computer while driving. Cantrell asked to inspect Cameron's laptop for evidence that it was in use at the time of the accident. Cameron agreed to a limited inspection, but wouldn't produce the laptop without a written agreement limiting the scope of the inspection. Whereas Cameron insisted the scope be limited "to the time of the accident," Cantrell understandably wanted a broader search to confirm that there had been no subsequent manipulation of the hard drive. Cantrell sought an order to compel, which the trial court granted. Cameron then filed for a writ of prohibition with the state's Supreme Court.

In its ruling, the Colorado Supreme Court noted:

> personal computers may contain a great deal of confidential data. Computers today touch on all aspects of daily life . . . they are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more. Very often, computers contain intimate, confidential information about a person. When the right to confidentiality is invoked, discovery of personal computer information thus requires serious consideration of a person's privacy interests.

195 P.3d at 661. (quotations and citations omitted).

As a result of these findings, the court concluded that the trial court abused its discretion in issuing an unqualified order directing Cameron to produce his laptop for inspection and without establishing parameters to balance the truth-seeking purpose of discovery with the privacy interests at stake.

In my opinion, Cantrell had a right to ascertain that the hard-drive had not been tampered with, which required inspection of the entire drive. In most cases, I would argue that the entire hard drive is certainly needed, although a very small fraction of ESI on the drive will be relevant.

By way of example, I was very recently involved in a case where I obtained the entire hard-drive for inspection. All the data sought resided in slack-file space, deleted files and printer spool files (documents drafted in MS-Word and sent to the printer, but never saved, probably in an effort to leave no record). Obviously, opposing counsel would not

have been able to direct his client to extract that information (let alone produce it in a readily usable form).

The answer to this dilemma, which would not have conflicted with the Colorado Supreme Court's ruling, is: (a) to craft a narrowly-tailored discover request that is limited in relevance to the case but specific enough to overcome efforts to conceal data; and (b) to retain an third-party vendor (or ask the court to appoint a special master); and (c) to provide the forensic analyst with as much specific guidance as possible to discover potentially responsive data. When questions arise as to whether data discovered is relevant or privileged, they may be resolved by an *in camera* review or the special master, if applicable, will make that call.

Posted by Sean Harrington on March 29, 2009 at 11:40 PM in Caselaw, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

March 01, 2009

Online anonymity not guaranteed in all Internet libel cases

The Maryland Court of Appeals issued a decision yesterday in *Independent Newspapers, Inc. v. Zebulon J. Brodie* protecting the identity of anonymous Internet posters and, for the first time, offering guidelines for that state's courts to follow in libel cases before compelling disclosure of online commenters' identities.

The five-step process the court adopted was borrowed from *Dendrite Int'l, Inc. v. John Doe No. 3,* 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001) and explicated in detail in yesterday's 43-page majority opinion. It seeks to help trial courts "balance First Amendment rights with the right to seek protection for defamation" by suggesting they:

- Require that plaintiffs notify anonymous parties that their identities are sought.
- Give the posters time to reply with reasons why they should remain nameless.
- Require plaintiffs to identify the defamatory statements and who made them.
- Determine whether the complaint has set forth a prima facie defamation, where the words are obviously libelous, or a per quod action, meaning it requires outside evidence.
- Weigh the poster's right to free speech against the strength of the case and the necessity of identity disclosure.

For further reading, *see*:

- Ki Mae Heussner, Lawsuit Cracks Open Online Anonymity, *ABC News* (Feb. 27, 2009)
- Tracy Frazier, *You Read What About Me on the Internet?!: Anonymous Online Libel, theLegality* (Feb. 26, 2009)
- *Bizub v. Paterson,* No. 07CV1960, district court, El Paso County, Colorado (unsuccessful attempt to compel *The Colorado Springs Gazette* to divulge identities of online posters)
- Federal District Court Mandates the Disclosure of the Identify of Online Posters in Yale Law Student Case, Internet Defamation Law Blog (Sep. 22, 2008)
- Kevin F. Berry, How to Unmask an Anonymous Blogger, *Law.com In-House Counsel* (Apr. 4, 2006)
- The First Amendment Center
- Electronic Frontier Foundation's "Bloggers' Rights" page
- Public Citizen's Internet Free Speech resources page
- Citizen Medial Law Project

Posted by Sean Harrington on March 01, 2009 at 12:25 AM in Caselaw | Permalink | Comments (0) | TrackBack (0)

February 28, 2009

[internet] Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009

Under the Electronic Communications Privacy Act of 1986, ISPs based in the United States are already required to retain data affixed to an IP address for at least 90 days -- upon the request of law enforcement.

However, the so-called SAFETY Act of 2009 would, inter alia, require any, "provider of an electronic communication service or remote computing service" to "retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user."

If enacted, Internet cafes, ISPs, hotels, universities, and employers would be required to keep logs of all data associated with IP addresses assigned individual users ð from e-mail logins to search queries to visited Web sites.

Further reading:

- Scott Nichols, Proposed Law Saves Internet User Data, *PC World* (Feb. 20, 2009)
- Senate Bill 436
- House Bill 1076

Posted by Sean Harrington on February 28, 2009 at 02:00 PM in Technology and the Law | Permalink

February 28, 2009

Sen. Lieberman fumed over PACER?

In a letter to the Chair, Hon. Lee Rosenthal, of the Committee on Rules of Practice & Procedure (Judicial Conference of the U.S.), Senator Joe Lieberman observes that "*The goal of [Section 205(e) of the E-Government Act] . . . was to increase free public access to these records,*" and demands to know why access to PACER isn't free and also why "*not enough has been done to protect personal information contained in publicly available court filings.*"

Further reading: John Schwartz, *An effort to upgrade a court archive system to free and easy,* New York Times (Feb. 13, 2009)"

Posted by Sean Harrington on February 28, 2009 at 01:32 PM in Technology and the Law | Permalink

MSBA Computer and Technology Law Section

The Official Blog of the Minnesota State Bar Association's Computer and Technology Law Section.

February 15, 2009

"Visual" Computer Forensic Analysis ?

In recent research presented at the Black Hat 2008 conference in Las Vegas, Greg Conti and Erik Dean from the United States Military Academy have adapted a new concept to computer forensics: visualization. The researchers demonstrated how visual computer forensic methods can dramatically reduce the time it takes to review files by substituting visual heuristics for traditional modes of file signature identification, file extension selection or hexadecimal searching.

By placing more data in front of the examiner in a smaller amount of screen space, the review speed of many file types is claimed to dramatically increase. In short, visual forensic tools have the potential to save an examiner a significant amount of analysis time.

"Visualization has the potential to dramatically change the field of computer forensics," urge Conti and Dean. "Each time we created a new visualization tool there were always surprising insights. Visualizations create windows on data that hasn't ever been readily visible, much to the dismay of people trying to hide information in the dark corners of a computer."

Full story at:
http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202428248638

The tools are available for free download. I will experiment with them on data from an actual case and may report my findings here in a future post.

Sean L. Harrington
MCSE, CSOXP, CISSP

Posted by Sean Harrington on February 15, 2009 at 11:48 PM in Technology and the Law | Permalink | Comments (0) | TrackBack (0)

Distance learning law grad granted exception to sit for Massachusetts Bar

The Massachusetts Supreme Judicial Court granted permission to a valedictorian graduate of Concord Law School, waiving the requirement of graduation from an ABA accredited school. A digest of the case, Mitchell v. Board of Bar Examiners, is reported at the Legal Profession Blog (here).

Previously, I had written about four grads from this same school, who've been admitted to SCotUS. In fact, I recall meeting a local judge --can't recall whether district or county-- at the 2006 Bar Convention in Brainard who was an adjunct professor for Concord.

Posted by Sean Harrington on November 24, 2008 at 02:22 AM in Technology and the Law | Permalink | Comments (0) | TrackBack (0)

November 24, 2008

Computer illiteracy no defense for spoliation

A litigant, who was subject to an order to produce his hard drive, argued in mitigation of spoliation of evidence by reason that he was a novice computer user who was having problems with his computer because it was severely infected with viruses, spyware and adware and that he sought professional help in correcting those problems. The Oklahoma Supreme Court reversed an order declining to impose sanctions. The following is adapted from that court's November 10, 2008 opinion.

> The litigant first sought help from a friend, who was not successful in resolving the problems. He then hired a professional to repair the computer. Although he maintained that at no time were evidentiary materials intentionally deleted from the computer, the record reflected that at least three kinds of "wiping" software were downloaded onto the computer during the period that the parties were actively negotiating to obtain the information contained on the computer's hard drive.
>
> Specifically, AbsoluteShield File Shredder was used and a file named "cable.doc" was removed; later the programs CyberScrub 3.5 and Window Washer were installed and the Window Washer program ran several times thereafter. The record reflects that the CyberScrub 3.5 program was last accessed on the same date that a motion to compel was granted by the trial judge.
>
> The record further reveals that, after the motion to compel was granted, the litigant contacted a computer security company, Jarvis Incorporated, and asked about hiring a computer expert to work on his computer. On Jarvis's recommendation, the plaintiff hired another technician to work on his computer. The litigant told neither Jarvis nor the technician that the computer was the subject of a court order and/or that certain files needed to be preserved before it was worked on. The technician testified that he could have preserved the hard drive before working on it by making a "clone" of it if he had known it was needed. Indeed, the technician had removed the hard drive and worked on it for approximately one week and used a "drive wiper" program called Terminus 6 on the hard drive.
>
> The litigant admitted that the technician used the Terminus program and admitted targeted destruction of specific files by the technician due to the desire to retain settings on his computer. Barnett says that it was the technician's decision to use the wiping software.
>
> A neutral court-appointed expert found no evidence that files associated with viruses had been destroyed with the Terminus program and further noted that a log identifying the files deleted by the Terminus program had itself been deleted. The expert's report stated that there were six documents with links in the Recent Documents folder of plaintiff's computer that had no matching document on the hard drive, indicating that those files had been deleted.

A concern that I have is that wiping utilities are becoming more and more commonplace, even being packaged with ordinary utilities that ship with new computers or come with ISP services (*e.g.*, MSN, which makes SpySweeper, McAffee and a number of wiping & anti-forensic utilities available). The popularity of these utilities, as well as encryption, has increased because of the growing awareness of identity theft, among other reasons. Even disk defragmenting tools, such as DiskKeeper, create a nightmare for forensic analysists attempting to located deleted files on a target system.

Whereas, in the past, such utilities required a knowing use (*mens rea*), the use of such utilities today may not be an indication of intent to spoliate. This means that the standard may shift more and more --as the case above illustrates-- from scienter to negligence. Therefore, counsel will increasingly need to observe strict data preservation protocols when litigation becomes reasonably forseeable and to communicate these obligations to clients promptly.

Some obvious questions that are often raised include:

- Must clients be instructed to immediately cease *using* a computer --at the first hint of reasonably forseeable litigation-- until the hard-drive can be forensically imaged? If so, what about the accumulating data that is created after the imaging date?
- If a client takes reasonable steps to preserve extant potentially-responsive data, must the client disable the use defragmenting utilities and other anti-forensic utilities that arguably are necessary for maintaining the optimum efficiency of a computer (especially considering that litigation may last several years)?
- Assuming the h.d.d. wasn't imaged, If a client has taken reasonable steps to preserve the *obvious* potentially-responsive data, should the client also have been expected to identify and preserve files that have been deleted but are still recoverable (given that further use of the computer will overwrite these files)?

For counsel seeking to discover ESI, the availability of that evidence may decrease as a result of the widespread use of anti-forensic utilities, but the shifting jurisprudence may allow for adverse jury instructions based on the missing evidence, which instructions possibly could be more damaging than the destroyed evidence, itself.

Posted by Sean Harrington on November 24, 2008 at 03:19 AM in Caselaw, Technology and the Law | Permalink

October 14, 2008

eDiscovery lamented as cost prohibitive, unwieldy

Patrick Oot, a lawyer for Verizon interviewed by *The Economist*, claims almost every case involves e-discovery and spits out “terabytes” of information—the equivalent of millions of pages. Almost every case? That may be his experience, but as an industry professional, it's not mine and I'm still amazed: many lawyers -- especially in family law-- haven't yet had a case where they've been asked to or found it necessary to image a single hard-drive. Some tell me they're holding out for as long as possible.

Recently, a few reports have been published, highlighting a phenomenon that I and, I suspect, many of us anticipated: that the cost and burdens of e-discovery would become eventually become unwieldy and unmanageable, even for the firms with an infrastructure and regular need to deal with it. But, not everyone paints the picture as bleakly --certainly not the EDD firms that benefit.

A telephone research survey sponsored by EDD firm Fios, Inc. concluded: technologists and lawyers are working more closely than previously thought; the most significant investments are being made in legal hold and archiving tools; and the 2007 amendments to the federal Rules didn't have the impact feared.

However, a joint survey, released in September, by the American College of Trial Lawyers and the Institute for the Advancement of the American Legal System reports that a majority of those surveyed found that the discovery system in particular is broken and "has become an end in itself," and that "Electronic discovery clearly needs a serious overhaul." Nearly a quarter of those surveyed characterized the civil justice system is "broken." The report claims that 83 percent of nearly 1,500 lawyers responding found costs --not the merits-- of a case to be the deciding factor in settling. A significant 68 percent of the college fellows disclosed that civil cases do not get filed because of the prohibitive litigation costs.

Frankly, I'm not so sure that surveying "college fellows" on the practicality of electronic discovery are the right people to ask these questions of. So, I decided to ask a colleague, Sharon Nelson, for her perspective. Nelson and her husband, John Simek, operate a computer forensics firm in Virginia. She is an attorney, frequent lecturer and co-author of the *Electronic Evidence and Discovery Handbook*.

Nelson concludes --as I have, also-- that, "The truth is often somewhere in the middle." She recalls, "Discovery was a nightmare even in paper - because there was often so much. The problem has grown exponentially with ESI, because there is so much more data. However, a portion of the blame belongs to all of us. We don't 'take out the trash' so our garbage heap of data expands constantly. It is just too cheap and easy to move it all to ever larger hard drives."

As a result, e-discovery has led to a new boom industry of specialized service providers which charge $125-600 an hour. George Socha (based here in Minnesota and who adminsters an annual survey regarded as the industry benchmark) estimates that their annual revenues have grown from $40m in 1999 to about $2 billion in 2006 and may hit $4 billion next year.

"Additionally, there are now at least two tiers of EDD companies - the whales, who are interested only in the mega-firms and their cases, and the smaller fish, who handle the small to mid-range cases of small to mid-range firms," Nelson noted. She also observed that, "There is little interaction between those two worlds - and huge price point differences," and believes that, "A continuing shake-out among vendors is probably likely, especially given the state of the economy."

Further reading:

- Pamela A. MacLean, Cost of Discovery a Driving Force in Settling Cases (*The National Law Journal,* Sept. 10, 2008)
- *The Economist,* "The big data dump" (Aug. 28, 2008)
- Survey Shows eDiscovery Best Practices (Law.com, July 21, 2008)
- *The Sedona Conference*

October 14, 2008

Internet posting of not-yet-tried defendants may create defamation cause-of-action

11/24/2008 Update: dead link (below) replaced with different link. Also, plaintiff's concerns about the damage to her reputation seem legitimate, as I recently discovered (hat tip to Sharon Nelson): On September 10th, *CareerBuilder.com* published the results of a survey that found one in five employers screen their job candidates online, double the amount of employers using social networking sites in 2006. Of the employers that used the sites, 34% dismissed the candidate after what they saw. The main concerns of the employer were candidates posting information about drinking or drugs, posting provocative information or photos, poor communication skills, and lying about qualifications. Conversely, 24% found that the social networking site solidified their desire to hire a person. Factors that made an employer hire a potential candidate were a background supporting the candidate's qualifications, proof that they had good communication skills, and evidence that the candidate was a good fit for the office culture.

A DWI defendant in Nassau County. NY has sued, demanding that her name and photograph posted to the County's Web page --dubbed "Wall of Shame"-- be removed. Read story. Defendant's claim is based primarily on the prospective harm caused when potential employers and others find her name and photo on the Web. Her attorney argues that publication to the "Wall of Shame" of persons who have not yet been found guilty of a crime is a form of punishment, noting "I don't think you need a law degree to understand that this fundamentally goes against a system of justice in which punishment occurs after you've been found guilty."

Last month, another woman sued the county over publication. She had lapsed into a hypoglycemic shock[1] and was subsequently arrested for DWI.

_____

[1] As I have witnessed first-hand, a person experiencing hypoglycemia, when his or her blood sugar is too low, can appear to be drunk. They may sweat, talk confused, become disoriented, stumble, lose their bearings, become aggressive, even "ornery," belligerent or pass out.

Posted by Sean Harrington on October 14, 2008 at 03:11 AM in Articles, Technology and the Law | Permalink

Bush signs Pro-IP Act into law

The PRO-IP Act of 2007, "To enhance remedies for violations of intellectual property laws, and for other purposes" was signed into law on Monday.

The law, backed by the Recording Industry Association of America and Motion Picture Association of America and the U.S. Chamber of Commerce, enhances and expands existing piracy and counterfeiting laws and also creates an intellectual property czar, reporting directly to the president.

- Wikipedia entry
- Electronic Frontier Foundation coverage
- Reuters news release

In related (but somewhat dated) news, the copyright wars have gone criminal. A blogger was arrested in late August for posting songs of a widely known rock group, which songs had not yet been released. *LA Times* article.

An enhanced spin on this story was put out by the legal blog, *May it Please the Court,* which explained:

> The penalties for criminal infringement are determined by its extent: if the infringer has made in any 180-day period ten or more copies of one or more copyrighted works with a total retail value of $2,500, the crime is a felony entailing up to five years imprisonment and/or a fine of up to $250,000 for individuals and $500,000 for organizations. 18 U.S.C. §§ 2319(a), 3571(b). Jail time can be increased to ten years for repeat offenders. Infringement is a crime where it is done "willfully and for purposes of commercial advantage or private financial gain." 17 U.S.C. § 506(a). Recent fines levied in criminal copyright infringement cases have been as much as $250,000.

Posted by Sean Harrington on October 14, 2008 at 02:38 AM in Articles, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

Ninth Circuit Judge Accused of Tampering with U.S. Courts' Web Filtering Software

9th Circuit Chief Judge Alex Kozinski faces a misconduct complaint that accuses him of illegally disabling Web site filtering software in 2001.

As Pamela MacLean (Law.com) reports:

> A potentially more serious problem for Kozinski is [the] resurrection of the 2001 internal bureaucratic fight over court monitoring of use of government computers to download movies and music.
>
> [The] complaint includes among the 80 pages of documents, a scathing October 2007 letter from retired court administrator L. Ralph Mecham, who wrote to the head of the Judicial Conduct Committee for the Judicial Conference of the U.S., which sets policies for the federal judiciary.
>
> Mecham, who managed the federal courts for 21 years, recounted the 2001 episode of Kozinski and former Circuit Executive Greg Walters disabling the monitoring software used for three circuits. His 16-page letter to committee chairman, Judge Ralph K. Winter, says Kozinski's action was considered by government lawyers "not only 'illegal' but constituted at least one felony" citing 18 U.S.C. 1361, destruction of government property.
>
> Mecham wrote that although the 9th Circuit's then-Chief Judge Mary Schroeder knew of the issue, as did the circuit judicial council, no misconduct complaint was brought against Kozinski at the time.
>
> "It is my strongly held view that this total absence of action is the worst example of failure by those responssible for disciplining judges that I have witnessed during my 21 years as AO director," Mecham's letter states.

Read MacLean's article, which contains numerous URL-links for further reading.

Posted by Sean Harrington on October 14, 2008 at 02:50 AM in Articles | Permalink | Comments (0) | TrackBack (0)

September 10, 2008

Courts and "The New Media"

> [O]verall . . . judges seem[] to embrace — like it or not — the notion that engaging and informing the public are now part of their job description. In the digital information age, the public expects all institutions to be transparent in multiple media, immediately and at all times, and courts are no exception. Some federal and state courts are already putting a lot out there — all court documents, streamed audio of hearings, everything except what the judge ate for lunch — and that trend is spreading. J. Rich Leonard, bankruptcy judge in the U. S. District Court for the Eastern District of North Carolina, described a remarkable and popular pilot project in his court that makes digital audio of bankruptcy hearings available online for a nominal fee.

So writes Tony Mauro in Courts and the New Media (*The Legal Times,* Sept. 10, 2008)

- continued -

Another article, *Legal Journalism at the Crossroads,* appearing last week in the D.C. Bar's online newsletter, questions:

> Who will tell the public the story of the American legal system? Increasingly, it seems it's the legal system itself, or more specifically, the players within the system—the courts, law firms, local bar associations, specialized legal news publishers, lawyers, and law professors. The days are waning for in-depth coverage of the courts by the mainstream news media. What has replaced it is an intriguing if confusing mix of law-related Web sites, publications, podcasts, and blogs, many of which are coming from outside of journalism, and all of which are contributing to a new definition of what constitutes legal news in America.
>
> "I'm not saying we're at this point yet, but I think there is some danger in having the legal system practically ignored by the mainstream media and covered exclusively by organizations that have a vested interest in the system and the result," says Mark Obbie, director of the Carnegie Legal Reporting Program at Syracuse University's S.I. Newhouse School of Public Communications.

The article also observes, "Today's reporting on the legal system, and especially the courts, is frequently filtered through sophisticated media platforms, such as . . . daring innovators and citizen journalists who slap a masthead on a Web site and call it legal news."

Sounds good to me.

And, on Tuesday, U.S. Supreme Court Justice Stephen Breyer gave the opening remarks during the UA James E. Rogers College of Law's New Media and the Courts symposium.

> It is a topic of extreme importance – particularly with the rising popularity of citizen reporters, blogs . . . and the tremendous amount of unfiltered information scattered across the Internet[1] . . . [J]udges and scholars are increasingly concerned about ways to inform the public with reliable information about the court system, said Sally Rider, director of the Rehnquist Center housed in the College of Law.

The symposium summary claimed that, "Though some are skeptical about the new media and especially blogs, there exists "tremendous potential in getting across the message that might be oppressed" *Id.*

The court beat assignment doesn't carry the clout it once did.

According to Gene Policinski, the vice present and executive director for The First Amendment Center and a blogger, the world of the traditional reporter has changed rapidly in the past 40 years and the court beat assignment doesn't carry the clout it once did. (click here).

I suspect that bloggers labor under constraints that bloggers aren't bound by. These constraints include their obligation to the *appearance* of objectivity, limitations on word count and --as ABC News's Vic Walter explained to me-- a need to dumb down the message to the lowest common denominator of a broad audience.

Robert Boczkiewicz, a Reuters reporter who covers the federal courts in the Tenth Circuit, corroborated many of the symposium's findings: "In the past at least couple of years," Boczkiewicz recalled, "the amount of coverage of the federal courts in Colorado has gotten less news coverage. The primary reason for that is the cutback in the level of staffing of several news organizations that have traditionally given more attention to the federal courts." Boczkiewicz also lamented that some new media legal reporters have the luxury to spend weeks on one article, while the few remaining court-beat reporters are "lucky to have a few hours to spend on one article."

Indeed, I'd wager that traditional news outlets have, as the author of *Legal Journalism at the Crossroads* implies, downsized *because of* the alternative fora. However, I find it laudible that the public now has access to a much more comprehensive (`though sometimes subjective) coverage of law-related issues from alternative journalists including, as examples, Howard Bashman, Evan Schaeffer, William Bedsworth, Mike Frisch, and Minnesota's Burt Hanson. And, to be candid, most of these sources have no ax to grind; they report news and judicial decisions with expertise and insights that traditional journalists simply don't have.

Further Reading

- Justice Breyer sees two sides of coin in 'New Media, Courts'" (*The Arizona Daily Star,* Sept. 10, 2008)
- Jason Salzman, Bloggers: Reveal Yourselves) (*The Rocky Mountain News,* March 28, 2008) (citing Dan Gillmor, ***Blogger's Polk Award triumph is a banner day for new media***, February 25, 2008)
- Randall D. Eliason, Leakers, *Bloggers, and Fourth Estate Inmates: The Misguided Pursuit of a Reporter's Privilege,* 24 Cardozo Arts & Ent. L.J. 385 (2006)

---

[1] *See, e.g,* Mark Cohen, *Judges wary of the 'unshaven blogger'* (Minnesota Lawyer Blog 02.26.2008) ("[T]he pernicious blogger...has struck fear deep into the hearts of some of the state's judiciary. One of the judges' concerns I have heard raised about cameras in the courtroom is the specter of the 'unshaven blogger' coming in with cell phone camera at the ready. Apparently the judges are worried about being made to look sinister or downright ridiculous by a slip of the tongue or out-of-context snippet of dialogue winding up as a video posted on a blog or YouTube"); *and see* Russ Bleemer, Judges told to ignore rights in abuse TROs, 140 N.J.L.Rev. 281, 294-95 (1995) (judge discussing judges' collective fears of being "tomorrow's headlines")

Posted by Sean Harrington on September 10, 2008 at 04:27 PM in Articles, Technology and the Law | Permalink

September 03, 2008

NJ court: No 'Legitimate' Privacy Expectation in Data on Office Computer

This decision in *People v. M.A.,* was one of first impression in New Jersey, but is consistent with several other jurisdictions, including *U.S. v. Angevine,* 281 F.3d 1130 (10th Cir. 2002); *U.S. v. Simons,* 206 F.3d 392 (4th Cir. 2000); and *U.S. v. Bailey,* 272 F. Supp. 2d 882 (D. Neb. 2003) in holding that an employee has no reasonable expectation of privacy in personal files stored on a company-owned computer and an employer's consent makes a police search lawful.

Moreover, the court applied what appears to be a derivative of the Fundamental Equity Doctrine in holding that, even if defendant had a subjective expectation of privacy because he used a confidential password, that expectation was unreasonable because of the criminal use to which it was put: "A burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as legitimate,'" the court said, quoting the U.S. Supreme Court's ruling in *Rakas v. Illinois*, 439 U.S. 128 (1978).

An intriguing question arises when applying this doctrine to overcome the legitimate expectation of privacy: What if the encryption software used is discovered to have been pirated or in violation of the EULA, but defendant was not otherwise putting the computer use or data to criminal use? Does the Independent Source Doctrine warrant exception apply? What if defendant's alleged unlawful conduct has no relation to the data or computer use --can that conduct be used as a pretext for overcoming defendant's legitimate privacy expectation? Can tortious, but not unlawful conduct, be used as a pretext for overcoming the legitimate privacy expectation?

For related prior blog posts, *see*:

- Domestic Travelers' Laptops Subject to DHS Searches
- Email and Text Messaging Protected from Law Enforcement and Employers
- Reasonable Suspicion not Required for Laptop Search at Int'l Airport
- Third party PC technician's discovery of contraband held admissible
- Surrendering the PGP passphrase
- Evidence Obtained Through Spyware May Be Admissible
- Employees Waive Privilege In Communications Transmitted From Company Computer System

Posted by Sean Harrington on September 03, 2008 at 11:02 AM in Caselaw | Permalink | Comments (0) | TrackBack (0)

August 23, 2008

PCAOB Declared Constitutional

A few weeks ago, I discussed the pending legal challenge that could have threatened to dismantle the Sarbanes Oxley Act. (*See* here). That case has now been decided.

The U.S. Appeals Court for the District of Columbia Circuit ruled 2-1 yesterday and upheld the legality of the Public Company Accounting Oversight Board, rejecting arguments that the PCAOB violates the Separation of Powers doctrine. An attorney for plaintiffs have indicated they will appeal either to the U.S. Supreme Court or seek a rehearing *en banc.* U. S. Securities and Exchange Commission Chairman Christopher Cox said the decision was "welcome news for the commission, investors and U.S. capital markets."

For more reading:

- Sarbanes-Oxley Audit Panel Upheld by Appeals Court
- Appeals court denies challenge to accounting law
- Court upholds Public Accounting Oversight Board
- PCAOB Statement re: *Favorable Decision In Free Enterprise Fund v. PCAOB*

Posted by Sean Harrington on August 23, 2008 at 12:28 PM | Permalink | Comments (1) | TrackBack (0)

August 13, 2008

Domestic Travelers' Laptops Subject to DHS Searches

In April, I discussed the Ninth Circuit decision, *U.S. v. Arnold,* for the proposition that reasonable suspicion is not required for a laptop search at an international airport (*i.e.,* a border).

Today, *The Washington Post* has published an editorial entitled, Search and Replace, arguing that Congress needs to set the rule for how border agents can delve into travelers' laptops. *The Post* points out that the Department of Homeland Security has expanded the the broad discretion of the border exception to domestic travelers' laptop computers and other electronic devices, noting that two federal appeals courts have upheld the same.

Given the confidential nature of client data, privileged data,[1] corporate intellectual property and personal data and given the numerous data breaches that have occurred because of mishandling by government agencies, both data encryption and routine data backups (to a separate repository) seem well advised.

---

[1] This could include, for example, attorney client privilege, work product privilege, Privacy Protection Act privilege (for journalists), *inter alia*.

Posted by Sean Harrington on August 13, 2008 at 12:44 PM in Articles | Permalink | Comments (0) | TrackBack (0)

July 31, 2008

Internet Repository Tapped for D.C. v. Heller decision

According to Law.com (here), an Internet respository of Founding-era documents, *The Constitutional Sources Project*, was utilized extensively by the Supreme Court in interpreting the Second Amendment. The project's co-founder and executive director, Lorianne Updike, trained Justices Antonin Scalia, Stephen Breyer and Samuel Alito on navigating the site, which enabled them to click on different clauses of the Constitution and to locate other relevant documents.

Alan Gura, who argued and won the Heller case, characterized the project as "a powerful source" that helped him track down documents. Opposing counsel, Thomas Goldstein, said the project was important in the effort to "get the constitutional history right."

Posted by Sean Harrington on July 31, 2008 at 12:58 PM in Articles, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

Sarbanes-Oxley Act Challenged as Unconstitutional

The case, *Free Enterprise Fund v. The Public Company Accounting Oversight Board,* was filed in U.S. District Court for the District of Columbia by plaintiffs the Free Action Enterprise Fund and a small accounting firm, Beckstead & Watts, LLP. The 24 page complaint alleges violation of the separation of powers doctrine, the non-delegation doctrine and the appointments clause of the Constitution, because the Public Accounting Oversight Board's members are neither appointed nor removable by the President.

Some commentators, such as the blawg Overlawyered.com (here), have opined:

> The PCAOB has generated endless red tape. Its rules micromanaging companies' internal controls, which require auditors to examine such minute details as which employee has access to which computer password, cost the American economy billions of dollars, contributing to an overall price tag for Sarbanes-Oxley of at least $35 billion a year.

On the other hand, the research firm, Glass, Lewis& Co., found that, in 2003, 4 % of all listed U.S. firms restated their reported earnings to correct mistakes. Under Sarbanes-Oxley, which imposed stricter scrutiny, that number increased in 2006 to nearly 12 %. Since then, it has edged down, as companies have improved their internal financial controls. Some argue that's good for investors and good for management, too, because CEOs make better decisions when they have more accurate financial information to work with.

The Washington Post (here) reports that, if the lawsuit prevails, the entire Act would fall, because it lacks a "severability" clause --if one of its provisions is found to be unconstitutional, the whole law would be stricken.

Update: After doing some further research, it seems the *Washington Post* article wasn't entirely clear that the district court case was already decided against plaintiffs on summary judgment.

Although the court found that plaintiffs Beckstead & Watts had standing as to the Motions to

Dismiss, it reached the merits on all three constitutional claims.

The memorandum decision is here. The appeal docket is here.

As to the Appointments Clause, the district court concluded that PCAOB members are, in fact, inferior officers and, to the extent that plaintiffs claimed PCAOB members should have been appointed by the SEC Chairman (rather than by the entire Commission), plaintiffs lacked standing.

As to the Separation of Powers doctrine, the court noted that the Supreme Court has never held that the Constitution requires the President to maintain direct removal power over inferior officers and here the President has not been "completely stripped" of his ability to remove PCAOB members, because SEC Commissioners can be removed by the President for cause can be removed by the SEC "for good cause shown"

As to the non-delegation doctrine, the court found that legislative delegation effected by the Act is squarely within the bounds of modern non-delegation doctrine, because the auditing, quality control, and ethics standards the PCAOB applies "must either be 'required by [the] Act or the rules of the Commission or necessary or appropriate in the public interest or for the protection of investors." (citing 15 U.S.C. § 7213(a)(1)). The court declared that the foregoing are "intelligible" standards that the Supreme Court has acknowledged in "various statutes authorizing regulation in the public interest."

Note the entry of appearance by Ken Starr on behalf of the plaintiff-appellants.

Posted by Sean Harrington on July 31, 2008 at 12:41 PM in Caselaw | Permalink | Comments (0) | TrackBack (0)

July 09, 2008

File Sharing from Work? Not Good

According to the Washington Post (here), an investment firm employee —possibly sharing media files— was using LimeWire (an Internet peer-to-peer file sharing utility) from his employer's network —yes, his work computer. His folly exposed the names, birth dates and Social Security numbers of about 2,000 of the firm's clients, including a number of "high-powered lawyers" and Supreme Court Justice Stephen G. Breyer. The breach was not discovered for nearly six months.

According to Robert Boback, chief executive of the company hired by Wagner to help contain the data breach and interviewed by *The Post,* such security breaches aren't uncommon. About 40 to 60 percent, he said, of all data leaks take place outside companies' secured networks --usually as a result of employees or contractors installing file-sharing software on company computers.

An interesting inference this *Post* article is that one settlement outcome of litigation arising over data breaches may include a determinate period of free credit monitoring (provided by firms such as FirstAdvantage) for class members whose data has been compromised.

Posted by Sean Harrington on July 09, 2008 at 11:27 AM in Articles, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

June 25, 2008

Email and Text Messaging Protected from Law Enforcement and Employers

A June 18, 2008 Ninth Circuit Court holding in *Quon v. Arch Wireless* establishes that law enforcement needs a probable cause warrant to access stored copies of electronic messages less than 180 days old (regardless of whether they've been downloaded or read) and would also prevent employers from obtaining the contents of employee emails or text messages from the service provider without employee consent. The case was decided under the Stored Communications Act (SCA), which is part of the Electronic Communications Privacy Act (ECPA) of 1986. The SCA prevents "providers" of communication services from divulging private communications to certain entities or individuals.

Historically, prosecutors have argued that, once a recipient accesses his messages -- whether they be email or texts--, the message is no longer in "electronic storage" as the SCA defines it, an argument the Ninth Circuit rejected. Thus, if an archived message was created as a backup copy of an electronic communication sent through an Electronic Communications Service, that copy continues to receive ECS protection, even if it was downloaded, read and "has expired in the normal course" such that the copy is no longer performing any archival/backup purpose. For the same reason, even if an employer pays for the use of third party text or email service, the employer cannot obtain copies of messages from the provider without the recipient's permission.

Additionally, the Ninth Circuit addressed whether text messages are protected by the Fourth Amendment, insofar as prosecutors often argue that, because email and text messages are stored by third parties that have the ability to read them, senders and recipients have no expectation of privacy in those messages and thus are entitled to no constitutional protection from unreasonable searches and seizures. The Ninth Circuit rejected this view, joining the Sixth Circuit in *Warshak v. US*, holding that text messages are akin to letters or packages, and are protected even though the shipper could open them.

Further, the panel considered the effect of acceptable use policies, monitoring policies or other terms of service that state that the service provider or employer reserves the right to monitor or audit the messages. While those policies may give employers or service providers the right to read messages, the question was whether law enforcement could, therefore, do so as well. The Ninth Circuit panel applied its ruling in *United States v. Heckenkamp*, which held that a student did not lose his reasonable expectation of privacy in information stored on his computer, despite a university policy that authorized the university to access his computer in limited circumstances while connected to the university's network. The Court rejected the argument that user consent to access for some purposes destroyed the expectation of privacy for every purpose, including warrantless or unreasonable government searches. (Note: Compare this outcome to the "abandonment theory" applied by a Pennsylvania court, which held that consent given to a third-party PC repair service to install a DVD player (including testing associated therewith) constituted a waiver of expectation of privacy for every purpose - Click here).

Posted by Sean Harrington on June 25, 2008 at 01:38 PM in Caselaw | Permalink | Comments (0) | TrackBack (0)

June 02, 2008

Another victory for First Amendment Website expression

Hat-tip to the Rocky Mountain Appellate weblog.

In a decision issued in *Utah Lighthouse Ministry (UTLM) v. Foundation for Apologetic Info. & Research (FAIR)*, the Tenth Circuit examined the issue of whether hyperlinking can render a non-commercial opinion, critical or parody Website liable for infringement under the Lanham Act. The resulting holdings afforded Website parodies (such as, *e.g.,* People Eating Tasty Animals (PETA))[1] some protection.

Following the Ninth Circuit's reasoning in *Bosley Medical Institute v. Kremer,* the Tenth Circuit concluded that, because the parody Website in question contained critical commentary as well as links to articles critical of plaintiffs and, because the links to plaintiffs' Web site were to its homepage and not directly to its bookstore, the "roundabout path" to the advertising or commercial use of others was simply "too attentuated" to invoke the trademark protections of the Lanham Act.

---

[1] This example appeared in n.5 of the Tenth Circuit's opinion.

April 22, 2008

Reasonable Suspicion not Required for Laptop Search at Int'l Airport

Generally, border search agents are given wide lattitude to conduct searches relative the reasonableness of suspicion[1] and, which provides an exception to the warrant requirement.[2]

Some time ago, I posted a story concerning a border exception to the warrant requirement, where a border agent inspected a laptop and discovered contraband (click here). From the Ninth Circuit, *U.S. v. Arnold,* we have a similar underlying fact situation, except that the question before the court concerns the reasonableness of the intrusion: In its April 21st opinion, the Court held that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border. The Court found unavailing defandant's numerous arguments --some bearing stretch marks-- such as that "laptop computers are fundamentally different from traditional closed containers," and analogizes them to "homes" [2] and the "human mind."[3] Consequently, the Court reversed the trial court's suppression order, thereby permitting prosecution to proceed.

---

[1] *See, generally, United States v. Montoya de Hernandez,* 473 U.S. 531 (1985).

[2] Under the border search exception, the government may conduct routine searches of persons entering the United States without probable cause, reasonable suspicion, or a warrant. For Fourth Amendment purposes, an international airport terminal is the "functional equivalent" of a border.

[3] Defendant's analogy of a laptop to a home was based on a conclusion that a laptop's capacity allows for the storage of personal documents in an amount equivalent to that stored in one's home.

[4] Defendant urged that a laptop is like the "human mind" because of its ability to record ideas, e-mail, internet chats and web-surfing habits.

Posted by Sean Harrington on April 22, 2008 at 01:34 PM in Caselaw | Permalink | Comments (0) | TrackBack (0)

April 10, 2008

Technologically Challenged Lawyer Suspended

An attorney was suspended for three months by the Kansas Supreme Court for, among other things, failing to obtain a login name and password to comply with the U.S. Bankruptcy Court's e-filing requirements.[1]

The respondent-attorney attempted to file a bankruptcy case by submitting paper pleadings rather than e-filing. The bankruptcy court sent Respondent an order advising that petitions and other pleadings must be filed electronically. The court ordered Respondent to attend the required training, pass the examination, and obtain a login name and password within 30 days. Respondent failed to comply with the order.

Subsequently, Respondent attempted to file another (separate) bankruptcy case. A bankruptcy judge advised Respondent in writing that he was not permitted to file a bankruptcy case using paper pleadings and that all pleadings must be filed electronically.

Respondent not only failed to obtain a log in name and password and failed to file the case to comport with court rules, but also did not return the advanced fee after discharge.

The dicsiplinary Memorandum Opinion is here.

Hat tip to *The Legal Profession Blog* for this story.

---

[1]Pursuant to a rule change, the United States Bankruptcy Court required that all pleadings be filed electronically. In order to file electronic pleadings with the bankruptcy court, an attorney must have a login name and password.

Posted by Sean Harrington on April 10, 2008 at 07:36 PM | Permalink | Comments (0) | TrackBack

March 27, 2008

Four online law school grads admitted to SCotUS

Four graduates of an entirely online law school became the first attorneys to be admitted to the U.S. Supreme Court last week. Read full story. To be admitted to the U.S. Supreme Court, each attorney must be a member with good standing of the bar for three years and be sponsored by two attorneys already admitted to the Supreme Court.

The school, Concord Law School, was founded in 1998 and is one of only two or three entirely online law schools. None, however, is ABA accredited. (The ABA's general policy under Standard 304(f) states that "a law school shall not grant credit for study by correspondence." Click here).

Four graduates were admitted in open court: Larry David, an international businessman and attorney in Pasadena, Calif., who volunteers at the Los Angeles County Bar Association Barristers Domestic Violence Project; Michael Kaner, a dentist in Newtown, Pa., who is a consultant on risk management and forensic dentistry; Ross Mitchell, a computer systems consultant in West Newton, Pa., who is advocating online legal education and the expansion of the multijurisdictional practice of law; and Sandusky Shelton, a retired telecommunications manager from Clio, Calif., who handles court-appointed juvenile dependency cases.

Posted by Sean Harrington on March 27, 2008 at 11:17 PM in Articles, Technology and the Law |

March 20, 2008

Internet Archive (archive.org) may provide inculpatory forensic evidence

In case now pending in the district court of Colorado, presided over by that court's embattled Chief Judge Edward Nottingham, the Internet Archive may prove to be a source of incriminating forensic evidence.

Briefly, the case arises from allegations that a resort's ski instructor raped a teenage girl. The girl and her family have sued the resort, noting that it gave assurances that any ski instructor working with children must have a "clean criminal record." Read full story. The accused instructor, in fact, has a lenghty rap sheet.

In its response to the lawsuit, the resort contended that it never promised that criminal checks were performed on employees and supplied copies of its Web pages to support the contention. However, the family's attorney said that the supplied offers-of-proof are phony, noting that a search of old Web pages on www.archive.org revealed that the resort had, in fact, made such representations since 2002. Moreover, he said, the archive site contained no pages similar to the ones that the resort supplied. "As the record now stands before the court, it appears that [the resort's] affidavits are false and misleading, the alleged copy of [the resort's] Web site is fabricated and [the resort] has attempted to destroy evidence."

Posted by Sean Harrington on March 20, 2008 at 04:34 PM in Technology and the Law | Permalink

Technology Advocate Appointed to MN Chief Justice

Gov. Tim Pawlenty announced the Minnesota Supreme Court's next chief justice, naming Eric J. Magnuson of Briggs and Morgan, P.A., formerly of Rider Bennett, LLP. Read full story.

Eric is co-author, along with David Herr, of Appellate Rules Annotated, 2007 ed. (Vol. 3, Minnesota Practice Series), a co-editor and chapter author for the fourth edition of Eighth Circuit Appellate Practice Manual, and co-editor of Matthew Bender's The Art of Advocacy: Appeals. He also co-authored *CM/ECF On Appeal– The Eighth Circuit Affirms* (Oct., 2007).

Eric is recognized nationally as an advocate for technology in the field of appellate advocacy. He's given many technology presentations, including "Making the Law of E-Discovery - Seeking Appellate Review of Non-Appealable Discovery," Minnesota Chapter of the Federal Bar Association Federal Practice Seminar (June 2007); "Technology and Appeals," DRI Annual Meeting (October 2006); "Technology Tools and Resources for Appellate Advocates," 16th Annual Trial Practice Seminar, North Dakota Trial Lawyers Association (May 2006); "Technology and Appeals," Appellate Practice Institute, Minnesota CLE and 8th Circuit Bar Association (May 2005); "Electronic Advocacy," American Academy of Appellate Lawyers Spring Meeting (April 2005); and *Technology Tools and Resources for Appellate Advocates* (2006).

Eric also presented my firm's digital brief technology at the *The Fifth Circuit Summit: Exploring Technology to Serve the Appeals Process* (September 25, 2006).

Hopefully, with Eric at the helm, and Bob Hanson's continuing leadership, technology in appellate practice, including e-filing and digital briefs, will be ushered in.

Posted by Sean Harrington on March 20, 2008 at 03:05 PM in Technology and the Law | Permalink | Comments (0) | TrackBack (0)

March 17, 2008

Another "Blogger Beware" development

Patent Troll Tracker Blogger and lawyer Richard Frenkel is now a defendant in two defamation suits: one by John Ward Jr., a partner in Ward & Smith in Longview, Texas (and son of U.S. District Judge T. John Ward (E.D. Tex.)) and another by Eric Albritton of the Albritton Law Firm in Longview, Texas. Both plaintiffs contend that Frenkel injured their reputation by making false factual assertions on his Patent Troll Tracker blog during the course and scope of his employment at Cisco that plaintiffs conspired with the "Clerk of the U.S. District Court for the Eastern District of Texas" to "alter documents to try to manufacture subject matter jurisdiction where none existed" and that plaintiffs "conspired with others to alter the filing date on a civil complaint," according to the complaints filed in both cases.

One of plaintiff's attorneys asserts that Frenkel's allegations in the blog are not "protected speech" under First Amendment law.

Read full story here.

Posted by Sean Harrington on March 17, 2008 at 01:00 AM in Articles, Technology and the Law |

March 04, 2008

Bill Proposes Internet "Network Neutrality"

"This is the essence of the Ed Markey's (D., Mass.) Orwellian-named Internet Freedom Preservation Act of 2008, which would foist network neutrality on the wild and woolly Internet." So begins this February, 25 2008 Wall Street Journal article, entitled, *Internet Wrecking Ball*, discussing the bill that proposes to regulate or "ration" TCP/IP packets and internet bandwith.

Markey's press release (here) states, in pertinent part:

> The goal of this bipartisan legislation is to assure consumers, content providers, and high tech innovators that the historic, open architecture nature of the Internet will be preserved and fostered. H.R. 5353 is designed to assess and promote Internet freedom for consumers and content providers.

The full text of the proposed bill is here.

A summary of the Act is here.

Posted by Sean Harrington on March 04, 2008 at 10:32 AM in Articles, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

February 19, 2008

Free Public Access to U.S. Court Decisions

Carl Malamud's latest online "public works" project, public.resource.org, is reported to make available later this week all Supreme Court opinions dating back to the 1700s and all U.S. appeals courts decisions dating back to 1950. Some commentators speculate that Malamud's efforts potentially represent a challenge to paid legal research services Thomson and LexisNexis. His northern California-based non-profit group last week took delivery of content from Fastcase, which agreed in November to sell the information with no strings attached. Malamud's group has spent the past several days reformatting the data to post on the Web site.

"We're about getting bulk data and making it available," free of charge, to the public, Malamud told the Conneticut Law Tribune. "I want to see all federal case law downloadable in bulk." He asserted that there are no restrictions on the use of the information after it's downloaded and that it's up to individuals to create Web sites that utilize the information.

Any initiative that "makes case law available for free in new and different ways is something all librarians are in favor of," said Darcy Kirk, associate dean for library and technology and law professor at the University of Connecticut. Read Full Story.

Malamud also recently launched a "PACER recycling site," where users, who have downloaded federal case information at 8 cents per page can upload them to the recycling site to be accessed later free of charge.

Posted by Sean Harrington on February 19, 2008 at 03:34 PM in Articles, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

February 14, 2008

Law Firm's Faulty IT Policy Not Excusable Neglect to Avoid Sanctions

In this U.S. Magistrate's July, 2007 Order (which I just discovered today), the court found that attorneys' non-receipt of emails from the U.S. Court, District of Colorado, caused by a firewall setting, was not excusable neglect to avoid the sanction of attorney fees for the firm's attorneys' failure to appear at a settlement conference.

The court heard evidence from the firm's IT administrator that the firewall setting was modified ð without notice to these particular attorneysð in response to complaints from some of the firm's employees concerning sexually explicit junkmail. Moreover, although the administrator added the Colorado *state* courts to the whitelists, he failed to add the cod.usCourts.gov (U.S. Court, District of Colorado) domain.

Although the magistrate found that the neglect was not willful or wanton, he nevertheless found that the attorneys were, "the responsible persons to adopt internal office procedures that ensure the courtís notices and orders are brought to their attention once they have been received." Thus, under Fed.R.Civ.P. 16(f), they were jointly and severally sanctioned for attorney fees and costs relating to the settlement conference and the additional hearings incident thereto.

This decision, `though not a precedent, is another salient reminder that attorneys are increasingly being required to keep up with technology that often is out-of-scope for their training and expertise or, alternatively, to retain competent staff.

Posted by Sean Harrington on February 14, 2008 at 07:15 PM in Caselaw, Technology and the Law | Permalink

February 07, 2008

Ethical Considerations for Law Firm ESI

Last year, I posted a lengthy article (here) concerning potential ethical obligations that attorneys and computer forensics professional might owe each other and where the separation of duties may be blurred.

Along similar lines, a ethics opinion released recently by the Maine Board of Bar Overseers addressed the ethical implications of using a third-party to process and store a law firm's electronically stored information (ESI). (Hat tip to *The Legal Profession Blog* for this one). The opinion provides, in pertinent part:

> With the pervasive and changing use of evolving technology in communication and other aspects of legal practice, particular safeguards which might constitute reasonable efforts in a specific context today may be outdated in a different context tomorrow. Therefore, rather than attempting to delineate acceptable and unacceptable practices, this opinion will outline guidance for the lawyer to consider in determining when professional obligations are satisfied.
>
> At a minimum, the lawyer should take steps to ensure that the company providing transcription or confidential data storage has a legally enforceable obligation to maintain the confidentiality of the client data involved. See ABA Ethics Opinion 95-398 (lawyer who allows computer maintenance company access to lawyer's files must ensure that company establishes reasonable procedures to protect confidentiality of information in files, and would be "well-advised" to secure company's written assurance of confidentiality); N.J. Sup. Comm. Prof. Ethics Opinion 701 ("Lawyers may maintain client files electronically with a third party as long as the third party has an enforceable obligation to preserve the security of those files and uses technology to guard against reasonably foreseeable hacking.")

In the U.S., there is presently neither a universal code of professional conduct or responsibility nor a national licensing body for computer forensics examiners or legal technologists. Certainly, there is none that I know of for data warehousing. In addition to the suggestions I made in the earlier post (which included working under a well-drafted contract), one consideration in selecting an expert is whether he or she belongs to a professional organization (e.g., IACIS, HTCIA, *etc.*) that imposes a code of ethics on its members and offers hortarory guidelines for separation of duties, among other things.

Posted by Sean Harrington on February 07, 2008 at 03:39 PM in Caselaw, Technology and the Law | Permalink

January 15, 2008

Communications Decency Act held to immunize gripe site operator from liability for hosting allegedly defamatory content authored by third party

In this October 2007 ruling from the U.S. Court for the District of Arizona, the court ruled that, although, "At common law, publishers are generally liable for the defamatory statements authored by third-parties," the Communications Decency Act (CDA) shields gripe site operators from liability of this nature. In so doing, the court evaluated the function of "author," as opposed to, "publisher," noting that it is, “well established that notice of the unlawful nature of the [content] provided is not enough to make it the [website operator’s] own speech” (quoting Universal Commc’n Sys., Inc. v. Lycos, 478 F.3d 413, 420 (1st Cir. 2007)) and that "Defendant’s failure to remove the three statements was an 'exercise of a publisher’s traditional editorial functions' and does not defeat CDA immunity." Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997). Finally, the court noted, "minor and passive participation in the development of content will not defeat CDA immunity, which can even withstand more active participation."

Posted by Sean Harrington on January 15, 2008 at 07:43 PM in Caselaw | Permalink | Comments (0) | TrackBack (0)

January 09, 2008

$8.5M sanction for e-discovery violations

> For the current 'good faith' discovery system to function in the electronic age, attorneys and clients must work together to ensure that both understand how and where electronic documents, records and emails are maintained and to determine how best to locate, review, and produce responsive documents.

So said the Court in *Qualcomm v. Broadcom,* (S. D. Calif.) in its Jan. 7, 2007 Order imposing sanctions and referring six attorneys to the State Bar of California Office of Chief Disciplinary Counsel because plaintiff failed to produce emails that were clearly requested in discovery and witnesses testified falsely on an issue that "became crucial to the... litigation."

One witness identified twenty-one emails that were believed to be both substantially probative and relevant, yet counsel did not produce the emails or conduct a further search. After the trial, Qualcomm's general counsel "admitted Qualcomm had thousands of relevant unproduced documents and that their review of these documents 'revealed facts that appear to be inconsistent with certain arguments that [counsel] made on Qualcomm's behalf at trial and in the equitable hearing following trial' " There were over 46,000 such documents. The Court further noted:

> It is inconceivable that these talented, well-educated, and experienced lawyers failed to discover through their interactions with Qualcomm any

> facts or issues that caused (or should have caused) them to question the sufficiency of Qualcomm's document search and production...the Court finds that these attorneys did not conduct a reasonable inquiry into the adequacy of Qualcomm's document search and production and, accordingly, they are responsible, along with Qualcomm, for the monumental discovery violation.

The Court ordered Qualcomm to pay $8.5M to Broadcom but, because "the attorneys' fees sanction is so large," the Court declined to fine Qualcomm, noting that, "If the imposition of an $8.5 million dollar sanction does not change Qualcomm's conduct, the Court doubts that an additional fine would do so."

The court referred six attorneys to the attorney regulation counsel, finding:

> the Sanctioned Attorneys assisted Qualcomm in committing this incredible discovery violation by intentionally hiding or recklessly ignoring relevant documents, ignoring or rejecting numerous warning signs...the Sanctioned Attorneys then used this lack of evidence to repeatedly and forcefully make false statements and arguments to the court and jury.

Posted by Sean Harrington on January 09, 2008 at 03:58 PM in Caselaw | Permalink | Comments (0) | TrackBack (0)

December 31, 2007

Third party PC technician's discovery of contraband held admissible

In this case, *Commonwealth v. Sodomsky*, an individual delivered his PC to CircuitCity to have a DVD drive installed. Although he did not ask for any software to be installed, he was informed that installation of the DVD drive would necessarily include testing the DVD drive. While testing the DVD-drive, the technician subsequently discovered contraband and reported it to the police. The police seized the evidence under the plain view doctrine.

Significantly, the Pennsylvania Superior Court held that defendant's acquiescence to the installation of a DVD drive was a *de facto* acquiescence to the installation of software (whether he knew it or not). The court reasoned that he, therefore, "volitionally relinquished any expectation of privacy in that item by delivering it to CircuitCity employees knowing that those employees were going to install and test a DVD drive."

In arriving at this conclusion, the court employed the legal theory of "abandonment," whereby an individual evidences an intent to relinquish control over personal property ("whether a person prejudiced by the search had voluntarily discarded, left behind, or otherwise relinquished his interest in the property in question so that he could no longer retain a reasonable expectation of privacy with regard to it at the time of the search") (quoting *Commonwealth v. Shoatz,* 366 A.2d 1216, 1220 (1976)).

Yet, although the court explained that the legal construct "revolves around the issue of intent," it rejected defendant's assertion that he did not *intend* for CircuitCity employees to access his personal video cache any more than he expected them to access his personal financial information or other files. The court specifically noted that defendant "failed to either inquire as to how the DVD drive would be tested or otherwise restrict the employees' access to his computer files." The court also noted that CircuitCity was employing a commercially acceptable manner for testing the DVD drive, rather than setting out to discover illicit contraband.

While I take no position on the ruling of the court, it occurs to me that this is an instance where "ignorance" commands a higher premium than "intent." Another such case was *Long v. Marubeni America Corporation,* 2006 WL 2998671 (S.D.N.Y., October 19, 2006), where that court held that both the attorney client and work product privileges were waived by employees using a company computer system to transmit otherwise privileged

communications to private counsel, which communications were sent from private password-protected accounts (not from the employer's email system). Significantly, a cache of the emails were retained by the company's system as "temporary internet files." Because the company could and did obtain these emails by reviewing its own system, the court held that the waiver was created through employees' failure to maintain the confidentiality of these communications with regard to the company's electronic communications policy, which policy advised employees not to use the company system for personal purposes and warned that they had no right of privacy in any materials sent over the system. The court reached this result notwithstanding its factual finding that employees were without knowledge that a cache of their email communications had been retained.

Thus, in these cases, and including the recent *In Re Boucher* (defendant, who used PGP to encrypt alleged contraband not required to divulge passphrase), we see where a presumption of a reasonable expectation of privacy can be overcome by a defendant's failure to take specific precautions to safeguard property or communications. The phrase, "knew or reasonably should have known" is employed in these cases to mean that lack technological expertise on the part of a layperson may result in waiver.

Posted by Sean Harrington on December 31, 2007 at 04:40 PM in Caselaw, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

Enhanced Creative and Intellectual Property Protection Bill Introduced

"In an effort to strengthen laws protecting creative and intellectual property," the House Judiciary Committee recently introduced bipartisan legislation, known as the "PRO IP" bill, to: strengthen the substantive civil and criminal laws relating to copyright and trademark infringement; establish an Office of the United States Intellectual Property Enforcement Representative (USIPER); appoint intellectual property officers to work with foreign countries in their efforts to combat counterfeiting and piracy: and create a permanent Intellectual Property Division within the Department of Justice to improve law enforcement coordination.

The latter objective is to be accomplished, in part, by "transferring the functions of the existing Computer Crime and Intellectual Property section (CCIPs) that relate to intellectual property enforcement to the new IP Division" and to provide the DoJ with new resources targeted to improve IP law enforcement, including local law enforcement grants and additional investigative and prosecutorial personnel. It also requires that DoJ prepare an annual report that details its IP enforcement activities.

The Press Release is located here: http://judiciary.house.gov/newscenter.aspx?A=887

Posted by Sean Harrington on December 31, 2007 at 02:16 PM in Technology and the Law | Permalink | Comments (0) | TrackBack (0)

RIAA asserting, "that it is illegal for someone, who has legally purchased a CD," to xfer to his PC?

Okay, the quote is not from the RIAA but, rather, taken from this Dec. 30, 2007 WashingtonPost.com article, *Download Uproar: Record Industry Goes After Personal Use*. According to the reporter, Marc Fisher, the Recording Industry Association of America (RIAA), "In legal documents in its federal case against Jeffrey Howell . . ., who kept a collection of about 2,000 music recordings on his personal computer, . . . maintains that it is

illegal for someone, who has *legally* purchased a CD to transfer that music into his computer." [emphasis in the orig.]

The case is *Atlantic Recording Corp. v. Howell.*

In fact, the RIAA Web page concerning piracy does state, in pertinent part:

> [T]here's no legal "right" to copy the copyrighted music on a CD onto a CD-R. However, burning a copy of CD onto a CD-R, or transferring a copy onto your computer hard drive or your portable music player, won't usually raise concerns . . . Enjoy the music.

However, like the Minnesota PGP case that I characterized in another post as widely misrepresented, I believe that the position of RIAA and Atlantic in this case appears to be similarly misconstrued. If one actually reads the supplemental brief, Atlantic makes clear that the gravamen of the claims isn't the possession of a backup copy of legally purchased materials but, rather, the fact that the backup copy resided in a folder share that was utilized by a file-sharing program:

> It is undisputed that Defendant possessed unauthorized copies of Plaintiffs' copyrighted sound recordings on his computer. Exhibit B to Plaintiffs' Complaint is a series of screen shots showing the sound recording and other files found in the KaZaA shared folder on Defendant's computer on January 30, 2006. Virtually all of the sound recordings on Exhibit B are in the ".mp3" format. Defendant admitted that he converted these sound recordings from their original format to the .mp3 format for his and his wife's use. The .mp3 format is a "compressed format [that] allows for rapid transmission of digital audio files from one computer to another by electronic mail or any other file transfer protocol." Once Defendant converted Plaintiffs' recording into the compressed .mp3 format and they are in his shared folder, they are no longer the authorized copies distributed by Plaintiffs. Moreover, Defendant had no authorization to distribute Plaintiffs' copyrighted recordings from his KaZaA shared folder. Each of the 11 sound recordings on Exhibit A to Plaintiffs' Complaint were stored in the .mp3 format in the shared folder on Defendant's computer hard drive, and each of these eleven files were actually disseminated from Defendant's computer. Each of these actual, unauthorized disseminations ofPlaintiffs' copyrighted works violates Plaintiffs' exclusive distribution right under the Copyright Act. In addition, Defendant unlawfully distributed all 54 of Plaintiffs' Sound Recordings by making unauthorized copies of the recordings available to other KaZaA users for download.

Id. at 15-16. [citations to the record and authorities omitted; emphasis supplied].

Notably, Atlantic complained that Howell had spoliated evidence of his alleged wrongdoing, an allegation that we're seeing raised more and more often in litigation, as lawyers start catching on to electronic discovery practices:

> One of the best ways to test a defendant's denial of responsibility for illegal file sharing would be to look at the contents of the defendant's computer hard drive, which would show, among other things, the existence of peer-to-peer software programs, the user's chosen preferences for the use of such programs, the dates of use of such programs, the profile of the individual using such programs, and any sound recordings that were downloaded using such programs. A forensic examination might also provide indications of particular instances of distribution from Defendant's shared folder. That information, however, has now been intentionally "wiped" from Defendant's computer. Defendant's intentional destruction of this evidence severely and irreparably prejudices Plaintiffs' ability to prove their claim against Defendant and warrants harsh sanctions.

Supplemental brief at 14.

Posted by Sean Harrington on December 31, 2007 at 01:28 PM in Articles, Caselaw, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

December 19, 2007

Surrendering the PGP passphrase

Anyone here remember *State v. Levie,* 695 N.W.2d 619 (Minn.App. 2005) ?

In *Levie,* the defendant-appellant's seized computer contained PGP, a cryptography program, which was inaccessible to the investigator. In rejecting Levie's bid for a new trial, said the court, *inter alia*:

> We find that evidence of appellant's internet use and the existence of an encryption program on his computer was at least somewhat relevant to the state's case against him.

As a result, this case stirred waves in techie circles & blogs accross the nation and was unfairly characterized by journalists as, "Minnesota court takes dim view of encryption." (*See, e.g.,* here or here).

I posit that the case was unfairly mischaracterized because the inaccessible PGP archive, by itself, did not result in an adverse jury instruction and the totality-of-the-circumstances was the apparent standard adopted by the trial court. *I.e.,* the record showed that Levie took a large number of pictures of a minor child with a digital camera and that he uploaded those pictures onto his computer soon after taking them. 695 N.W.2d at 624.

Prof. Orin Kerr came to a similar (albeit differently reasoned) conclusion in his blog post, *The Myth of Crypto as a Crime*:

> Obviously, the idea that using encryption necessarily reflects criminal activity is rather silly; Internet users use encryption all the time for all sorts of legitimate reasons. As many critics of the new decision have noted, it makes no sense to see encryption as inherently linked to crime. But contrary to the blogospheric common wisdom, *no court ever said it was.*

[emphasis in original]. Kerr reasoned, instead, that the court regarded Levie's use of PGP as evidence that he was a sophisticated computer user, which might explain why the police found no child pornography or nude child photos on his computer.

In cases like these, attorneys often may wonder, "Can a court force a defendant to give up his passphrase?" (*side note:* I always include, in routine e-discovery interrogatories that I prepare for my attorney-clients, specific requests for the passwords and password phrases to all encyrpted archives and other repositories containing potentially responsive ESI). This question is certain to arise more frequently in the near future, including in civil cases (and especially in domestic relations cases).[1]

To help answer that question, the U.S.D.C. for the District of Vermont court declined to compel a defendant to surrender his PGP passphrase, finding that compelling a defendant to surrender his PGP passphrase would violate his Constitutional right not to incriminate himself.

The case, *In re Boucher,* involved child pornography, as you might have expected. Yet, the case law involving the compulsory surrender of encryption passphrases is quite unsettled.

If this case is appealed, it has the potential of creating an important precedent.

---

[1] Unfortunately, perhaps, we should not be looking to domestic relations case law for guidance on issues of substantive constiutional law (such as the privilege against self-incrimination). *See, e.g.,* David N. Heleniak, *The New Star Chamber,* 57 Rutgers Law Review no. 3 (Spring 2005), 1009, discussing the "due process fiasco" of family law and

characterizing family courts "an area of law mired in intellectual dishonesty and injustice." In the article, Heleniak identified six commonplace deprivations of fundamental due process: seizure of children and railroading innocent parents into jail through denial of trial by jury; denial of poor defendants to free counsel; denial of right to take depositions; lack of evidentiary hearings; lack of notice; and improper standard of proof). In family law, "the burden of proof may be shifted to the defendant," according to a handbook for local officials published by the National Conference of State Legislatures.

Posted by Sean Harrington on December 19, 2007 at 04:56 PM in Caselaw, Technology and the Law | Permalink | Comments (0) | TrackBack (0)

December 17, 2007

Blogger's Use of Trademark Protected as News Reporting

In its October 22, 2007 Order granting defendant Philip Smith's motion for summary judgment, the District Court of South Carolina dismissed defamation, trademark infringement, and invasion of privacy claims brought by plaintiff BidZirk LLC, an auction listing company.

The claims arose out of the *pro se* defendant-blogger's publication of articles on his blog, featuring plaintiff's trademark, that were critical of plaintiffs' eBay auction listing business. Plaintiffs asserted that defendant's use of their mark in an article critical of plaintiff's business tarnished their famous trademark in violation of the Federal Trademark Dilution Act ("FTDA"). The Court held plaintiff's trademark dilution claims failed because defendant used the mark in connection with "news reporting and news commentary," a non-actionable use under the Federal dilution statute.

Pursuant thereto, a party cannot be found guilty of diluting the mark of another if the mark is used in "news reporting or news commentary." 15 U.S.C. § 1125(c)(4)(C). The Court held that Smith's use of the trademark was, in fact, a protected use in the course of "news reporting or news commentary.". The court noted that, while "not all bloggers are journalists, some bloggers are, without question, journalists." The Court had examined "the content of the material, not the format, to determine whether it is journalism." The Court found that it was not written solely to denigrate plaintiffs but, rather, it was written for the purpose of conveying information to the public about the use of auction listing companies, based on the author's personal experience and supported by his research. It also provided a checklist to aid consumers in selecting such companies. These attributes "evidences [an] intent to report what [Smith] believed was a newsworthy story for consumers."

The court further dismissed plaintiffs' defamation claim, finding the challenged statements non-actionable statements of opinion. Said the Court, "Opinion statements, defamatory or otherwise, are not actionable unless they contain provably true or false connotations." The statements were an opinion statement that could not be fairly characterized as true or false and, which statements included terms that have, "different meanings to different people." Thus, because the statement was not capable of being characterized as false, there was no liability for defamation.

Finally, the Court dismissed plaintiffs' invasion of privacy claim, arising from a link found on Smith's blog to a picture of plaintiffs found elsewhere on the Internet, accompanied by Smith's commentary. According to plaintiffs, the accompanying text implied that they were 'irresponsible and overcommitted' and impermissibly cast them in a false light. The Court rejected this claim, finding that South Carolina does not recognize a claim for false light invasion of privacy and, even if it did, the claim would fail as the article did not cast plaintiffs in a false light and ("Nothing about Smith's statements would be highly offensive to a reasonable person," an essential prerequisite to a false light invasion of privacy claim").

Similarly, plaintiffs' 'wrongful appropriation of personality' invasion of privacy claim failed: A

required element of such a claim is the “intentional [non-consensual] use of the plaintiff’s name, likeness, or identity by the defendant for his own benefit,” which was missing here. Smith did not use a picture of plaintiffs but, instead, only linked to one found on another site. In addition, plaintiffs waived any privacy right they had in the photograph in question by consenting to its use on the other non-password protected internet site. Finally, there was no apparent benefit to Smith by his use of the link.

The Court *sua sponte* sanctioned plaintiffs’ attorney, Kevin Elwell, under Rule 11, for filing a *lis pendens* against Smith’s condominium. The Court fined Elwell $1,000, which he directed be paid directly to Smith.

Posted by Sean Harrington on December 17, 2007 at 04:42 PM in Caselaw | Permalink | Comments (0) | TrackBack (0)

November 19, 2007

State Trial Court Records Now Available via Web

From the Court Information Office, for immediate release (Nov. 16, 2007)

[Those] interested in looking up a Minnesota trial court record will find the task easier as of noon, today, when access to some trial court records became available through the web site of the Minnesota Judicial Branch. (<http://www.mncourts.gov> www.mncourts.gov) Records for the Supreme Court and the Court of Appeals became available through the web site earlier this year. Until now, however, anyone interested in looking up a trial court record could only do so by going to a public access computer terminal at a courthouse.

The new service allows a viewer to search criminal cases by case number, defendant name or attorney name. Name searches will be limited to cases where at least one charge has resulted in a conviction. The on-line search will also not list addresses.

Civil, family and probate cases can be searched by party name, case number or attorney name. The system will also allow for searches of court calendars by party, business name, case number, judicial officer or attorney name.

"Our staff has been working hard for several years to create a single, state-wide court record system," said State Court Administrator Sue Dosal. "Remote access to court records via the Internet is one of the many new benefits creation of a single system will allow."

The service, Minnesota Public Access Remote (MPA), is a public view of the new trial court records system, the Minnesota Court Information System (MNCIS). MNCIS, which was created by merging 10 different databases and multiple case management applications, includes more than 9 million case records dating back to the mid-1970s. The final two pieces of the system, Ramsey Country court criminal case records, and Dakota County Court records, will be added to the system in early 2008.

The new statewide case records system allows the Judicial Branch to share court records with other justice system agencies, including police, prosecutors and corrections officials.

Court officials are discouraging use of the MPA service for criminal background checks. The Minnesota Bureau of Criminal Apprehension offers a criminal background check service that links prior criminal history through fingerprints to verify identification of the individual. The MPA service for court records cannot provide this level of verification.

Court officials cautioned that name searches conducted through the MPA service could be unreliable because the person identified in the search could have the same name, birth date or other identifiers as someone else. In addition, criminal offenders frequently use aliases, including the names
of others.

The court system staff has been working to eliminate duplicate records and mistaken entries as the new system has been built. Court officials are hoping people who find an error in a court record will notify the courts so the record can be corrected. Viewers will not

be able to modify the case records. Only court administrators can authorize changes.

"Many, many people have worked very hard over several years to convert a fragmented, hard to search, outdated case records system into this new, state-of-the art case management system," said Sue Dosal. "In the coming years, the creation of MNCIS will allow us to add many new capabilities and services that will benefit court employees, court policy makers and the tens of thousands of people who interact with Minnesota's courts each year. We envision adding services such as e-filing of cases, remote payment of court fines and fees, up-to-date accounting information and much, much more."

"Robert Hanson, our Chief Information Officer, and his Information Technology staff and the hundreds of court employees who worked on this project have developed a system that will benefit Minnesotans for years to come."

Posted by Sean Harrington on November 19, 2007 at 10:10 AM | Permalink | Comments (1) | TrackBack (0)

November 05, 2007

Labor Cost Advantages of "Offshore" Locations Decline in 2006 According to 2007 A.T. Kearney Study

Following last weeks informative CLE presentation on legal process outsourcing (LPO) by Jeffrey A. Proulx, we should be mindful of the 2007 A.T. Kearney study that finds costs slippage in the previous year attributable to off-shoring. The report found that although the wage advantage of offshoring locations for office services is set to last for another 20 years, it is on the decline as offshore wages for IT, business process and call center services have risen. Paul Laudicina, managing officer and chairman of A.T. Kearney., reported:

> What is most striking about the results of this year's Global Services Location Index is how the relative cost advantage of the leading offshore destinations declined almost universally, while their scores for people skills and business environment rose significantly . . . These findings reinforce the message that corporations making global location decisions should focus less on short-term cost considerations and more on long-term projections of talent supply and operating conditions.

Because of the infancy of legal outsourcing models in India and abroad, the Kearney study probably is equally applicable thereto as it is to IT or call-center services at the present. However, as legal outsourcing diversifies and matures, as is predicted,[1] indepedent studies will need to be applied to these divergent models.

---

[1] Forrester Research has estimated that the number of jobs outsourced in the legal services area will grow to 35000 by 2010 and up to 79000 by 2015.

Posted by Sean Harrington on November 05, 2007 at 05:46 PM in Technology and the Law | Permalink | Comments (0) | TrackBack (0)

September 12, 2007

North Dakota Provides e-Access to Bar Disciplinary Proceedings

Some believe strongly that open access to case information, such as bar disciplinary proceedings, is necessary in order to determine whether self-regulation adequately serves the public interest. *See, e.g., Attorney Discipline Web Data Uneven,* Nat'l Law Review, Sept. 10, 2007.

A Web site maintained by the North Dakota Supreme Court provides a statement of issues and briefs in advance of oral arguments and then the audio of oral arguments afterwards. Click here for one case example.

For related topics, *see also* Availability of Online Resources May Be One Reason for Reduction in U.S. S.Ct. Caseload and Google aids public record accessibility.

Posted by Sean Harrington on September 12, 2007 at 03:58 PM in Articles, Technology and the Law | Permalink

August 27, 2007

Use mediocre computer forensics expert and discover that the "Safe Harbor" provision is very shallow!

In April, Damien Riehl brought us the story of the Eight Circuit's ruling in *Greyhound Lines, Inc. v. Wade* that there was no abuse discretion in a trial court's denial of sanctions for spoliation, where the movant failed to demonstrate intent and prejudice. In another post, last month, I discussed the precarious possibilities of forensics experts, who can ruin a case.

Bringing these two topics together, we have the case of *Doe v. Norwalk Community College,* where the U.S. District Court in Connecticut imposed spoliation sanctions for a party's failure to prevent the destruction of evidence. Defendants sought shelter under safe harbor provision of Fed.R.Civ.P. 37(f), but the district court disallowed the defendants to take advantage of the provision, since they made no attempts to preserve relevant evidence. The credibility of the computer forensics experts (or non-experts, depending how one might characterize them) decided the outcome of this case. >> read more >>

After two years of litigation, plaintiff Jane Doe persuaded the court that the defendant college was withholding electronic evidence. The college was ordered to produce the computers of key witnesses for inspection by Doe's computer forensic expert. The expert inspected the college computers over a two day period. Delay's inspection showed that several of the computers had no data, they were literally all zeros. Doe then filed a motion for spoliation sanctions, alleging "the hard drives of key witnesses in this case were scrubbed" or "completely 'wiped' of data" and, which resulted in several affidavits by Doe's expert and the college's counter-expert (its in-house Information Technology technician).

The trial court scheduled two evidentiary hearings during which the experts testified and were cross-examined about the suspicious circumstances of the missing ESI. During one of these hearings, the college produced another alleged expert, the Information Technology Systems Manager. Both of the college's experts testified, *inter alia,* that they did not believe that the state's two year document retention policy applied to them or to "normal computer usage," directly contradicting the hearing testimony of the college's Dean and the college's principle expert produced a litany of reasons for why two computers could be "full of nothing": He began with the assertion that it was the wrong computer; then that it was imaged, but not wiped; and, as a last resort, that the "all zeros" problem was the result of "computer failure." The most compelling and interesting aspect of the spoliation proceedings was the exposè of the term "wiped." [1]

Plaintiff's expert correctly stated that wiping is a "process that overwrites existing data on the hard drive, making this information unrecoverable," and that the "all zeros" condition of the hard drives was indicative that the hard drive had been intentionally scrubbed of all data. *Id.* at n.3 This is because computers write and read information as binary bits of either ones or zeros (electrically 'on' or 'off'). Any combination of eight 'on' or 'off' bits comprise a byte (a typical hard drive today has hundreds of billions of bytes). Information can only be stored when both ones and zeros are used in varying permutations. (Thus, if a hard drive or any other ESI device contains all zeros (or all ones), it contains no information). The college's expert, took exception with the term "scrubbed," and attempted to substitute the word "imaged," where the college's IT department modifies the structure of the hard drive (without scrubbing it). He further suggested that one particular hard drive, which may have appeared to have been "scrubbed," was because it was in the process of failing, which he testified could produce inconsistent or corrupt results. *Id.* at n.6.

Unpersuaded, the court accurately defined "scrubbed' or "wiped" as "more than overwriting or 'reimaging;' it means eliminating all data from the hard drive, such that none of the old data can be read or still remains on it." *Id.* at 11. Contrary to the college's expert's testimony, a computer which has been imaged or one that is failing, would not contain all zeros. Some information (some combinations of ones and zeros among the billions of bits on a hard drive) would remain. The trial court explained it this way:

> Delay found that it contained all 0's, indicating that every sector had been overwritten. Delay testified that, if the drive had data on it but was failing, as Bissell testified, then data would be seen on it with Delay's forensic software, which instead recognized that the hard drive was unpartitioned and contained no data. Moreover, Seaborn's new computer had traces of other users' information on it, thus showing an inconsistent result in NCC's process of re-imaging hard drives. Even if it was consistent with NCC's policy, the fact that Seaborn's new computer showed other users' information indicates that "imaging" does not eliminate everything from a hard drive, but leaves some data from old users on it, prompting the question why Seaborn's old computer-or Schmidt's computer-did not have any evidence of other users on it. The answers provided by the defendants-a failing drive or "re-imaging"-are rejected by the court as not credible.

The irregularities in PST files that Plaintiff's attorney uncovered also led the trial court to suspect that relevant evidence had been intentionally destroyed by several of the college employees. He discovered the Microsoft Outlook PST files, which house electronic mailboxes, of four individuals had inconsistencies "that indicate [ ] that data has been altered, destroyed or filtered ." For example, one person's PST file contained no Deleted Items and only one Sent Item and the Inbox and Sent Items contained data starting August 2004, "even though other activity is present starting in 2002."

The trial court did not credit the testimony of the defense experts. Overall, they served to make a bad situation worse.

The trial court not only rejected the defense expert testimony but, it also rejected the legal arguments of defense counsel (including that an effective legal records hold could not be implemented without revealing the true name of Jane Doe). The court said defendant's counsel should have conferred plaintiff's counsel. Defense counsel's arguments as to when the duty to preserve commenced were also not countenanced.

Ultimately, the court found that the defendants' actions were at least grossly negligent and concluded that a party to litigation can only invoke the good faith provision when that party has taken affirmative steps to prevent the spoliation of evidence. The trial court granted Doe's motion for an adverse jury instruction based on this grossly negligent failure of the college to preserve ESI and awarded Doe her expert witness's costs.

This case aptly illustrates why the quality of experts can make or break a case. Don't rely on an in-house or jack-of-all-trades IT Tech, who tries to fast-talk a judge with "computerese" and specious theories. It may fool many attorneys, but it is likely to not stand up under cross-examination by an attorney working with a qualified expert.

---

[1]*See, e.g., United States v. Krause* (*In re Krause*), 2007 WL 1597937, 2007 Bankr. LEXIS 1937 (Bankr. D. Kan. June 4, 2007) (A debtor, an attorney proceeding *pro se* in a bankruptcy, was caught destroying evidence using a popular software program)

Posted by Sean Harrington on August 27, 2007 at 07:50 PM in Articles, Caselaw | Permalink

August 03, 2007

Computer Animations at Trial: A Persuasive Tool to Be Utilized with Care

"Animation is a new and powerful evidentiary tool, but must be used with great care." [1] Although this article primarily concerns Computer Animations, some general assertions are made with respect to demonstrative evidence in all forms. Although Minnesota cases are discussed, I will cite the Federal Rules, rather than local state rules.

> "If you have a good animation, it's such a difficult thing for the other side to fight," said David Golomb, a Manhattan attorney who has served as president of the New York State Trial Lawyers Association. He calls it "devastating evidence"

_____

[1] State v. Stewart, 643 N.W.2d 281, 295 - 296 (MN 2002) (citing Gregory P. Joseph, *A Simplified Approach to Computer-Generated Evidence and Animations,* 156 F.R.D. 327 (1994); Fred Galves, *Where the Not-so-Wild things are: computers in the courtroom, The Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance,* 13 Harv. J.L. & Tech. 161 (2000).)

_____

Demonstrative evidence is evidence in the form of an illustration, rather than substantive evidence and is used widely in both civil and criminal cases.[2] Examples of demonstrative evidence include plaster casts or molds, scale models, maps, charts, diagrams, drawings, police composites, mug shots, sketches, photographs, microscopic enlargements, videotapes, computer reconstruction or simulation, scientific tests or experiments, x-rays, movies, sound recordings, forensic animation and graphs. Visual aids of this type are intimately tied to the credibility of the witness who testified with them, and although they are not separate pieces of evidence, like substantive evidence, they sometimes may be made available again to a jury for viewing during deliberation.

Visual Aids are Sine Qua Non to almost every type of trial presentation

> "The attorney must constantly ask, how can I make this testimony more concrete? Or, how can I help the jury visualize this point? . . The answer will often be found in the development of demonstrative evidence." Steven Lubet, Modern Trial Advocacy: Analysis and Practice (2d ed. 1997)

Trial lawyers have experienced that jurors retain 87% of what they see but, only 10% of what they hear. Presenters using visual aids are 43% more persuasive than those, who rely on words alone.[3] Presenters using visual aids experience 400% higher information retention from their audiences than presenters, who deliver purely verbal presentations.[4] As a result, effective trial lawyers have almost always relied upon visual aids, which have progressed from simple illustrations to photographs to video to computer animations and, more recently, holograms.

Use a Combination of Demonstrative Evidence

Tom O'Connor explains, in a recent Law Technology News article, *How Can a Litigator Go from the Dark Ages to Enlightenment in One Quick Step,* that:

> In the early days, we found that using a variety of visual aids in court was the most compelling to juries. A well planned combination of standard exhibit boards, video and computer-based exhibits is better than trying to fit all your evidence into one type of display.

Tom's point is that this was an early lesson that holds true today. Consider using a combination of physical models that jurors can closely examine or hold, magnetic boards, projected displays, animations, photographs and timelines.

Make Advance Arrangements with and Engage Your Expert Witnesses

Your expert witnesses must approve of and be familiar with and comfortable with the demonstrative exhibits that you intend to provide in concert with their testimony. In the case of computer animations, iterative development is imperative. The final animation must exactly compliment the expert's opinion and proposed testimony. Early involvement of animation in a case is often beneficial and, consequently, it may be prudent to retain an animator prior to expert witnesses. The animator may also serve as a liaison of sorts between the litigator and expert witness, fusing the litigator's art of persuasion with the expert's cold facts into a presentation that both may agree upon.

Another way to intimately involve the expert is to provide annotation equipment, such as a touch screen, light pen or telestrator. Annotation makes a low-key but substantial contribution by allowing either the litigator or the expert to mark up images generated by an evidence camera or laptop computer and displayed on a monitor or projection screen. This allows pointing out what is important in the display, drawing emphasis to a particular aspect, or connecting lines to show a nexus or to help expedite opening statements, witness testimony and closing arguments.

Make Arrangements in Advance with the Court

At an ABA Techshow presentation in March 2006, I recall both judges Christina Habas (District Court, Denver County) and Herbert Dixon (Superior Court, District of Columbia) emphasizing the importance of coordinating, in advance, the use of technology for trial.

Essentially, this means little more than contacting the court coordinator or division clerk to work out a time to come into the court room prior to trial to work out issues of wiring, orientation and visibility for both the judge's bench and jury box and audio (if applicable). It's important to work out whether you will be permitted to dim the lights during a projected presentation or whether it would be best to bring in one or more flat-panel big screen televisions for the judge and jury that are capable of displaying sharp, bright, crisp images.

One overlooked aspect of this pre-flight preparation is to be mindful of the positioning of clumsy equipment and confined spaces. If too many types of display technologies are present, constant moving of equipment (to keep the jury line-of-sight open) and tripping over wires and cables will disrupt the flow the case.

Admissibility of Computer Animations

Perhaps, the biggest and most overlooked concern is admissibility. To be admissible, demonstrative exhibits must "fairly and accurately" represent the real subjects at the relevant times and their probative value must outweigh any prejudicial effect. Based upon these standards, courts have allowed video and computer animation demonstrative evidence to keep pace with technology advances and the "CSI effect" of jurors.

It is important to distinguish between animations offered for "illustrative purposes only" from those claimed as simulations, recreations or mathematical modeling. In Lake Superior v. Hammel, 715 N.W.2d 458, 481-82 (Minn. App. 2006), the appellants argued that the district court erred by admitting a computer animation showing the means and methods that a large aquarium tank could have been constructed. Appellants contended that the animation was prejudicial because it showed a perfect result. Judge Kalitowski explained:

> When the district court denied appellants' pretrial motion to exclude the animation, it admitted the animation for illustrative purposes only and did not allow it in the jury room for deliberations. Rejecting the challenge to the animation again as a basis for appellants' motion for new trial, the district court explained that appellants claimed the tank was not constructable as designed while respondents claimed that the structure could have been erected using appropriate means and methods. Thus, the court stated that the animation's purpose was to illustrate the process that respondents claimed could have been employed to successfully build the structure. Appellants provide no evidence to suggest that the animation was inaccurate, was considered as substantive rather than illustrative evidence, or resulted in prejudice to them. Because the district court thoroughly examined the admissibility of the animation on two occasions and instructed the jury to consider the animation for illustrative purposes only, we cannot say that the district court abused its discretion by admitting the animation.

(quotations ommitted) (quoting Behlke v. Conwed Corp., 474 N.W.2d 351, 358-59 (Minn.App. 1991)).

If an animation is offered for illustrative purposes, only, the most common objection is to foundation, demanding adequate testimony to establish the accuracy of the date, structures, motion, sound and other aspects of the animation. Therefore, it is imperative for litigators to lay a proper foundation in introducing such evidence with experts or other witnesses. The impact of animated exhibits is so great that, if there are insufficient indicia of reliability under Rule 901, then Rule 403 and Rule 611 considerations will weigh against use of the animation.

Objections as to unfair inferences being drawn from or depicted with relation to the evidence may include:

- **Viewpoint:** A computer can frame an animation from a point at the scene where no witness was or could have been or show more of a scene than than could have been viewed by an eyewitness, thereby construed as misleading.
- **Speed:** The speed of motion in an animation may be objectionable when there is no foundation to show the motion depicted is accurate (such as the speed of a colliding vehicles)
- **Motion:** Current software offerings utilize algorithms and require animators to make choices as to when and where an actor changes direction in a scene. An incorrect choice can lead to an inaccurate representation of the motion.
- **Terrain:** Low budget animations will use flat terrain, which may not be representative of the actual scene
- **Sound:** The sound in computer animations may be objectionable when there is no foundation to show that the sound is accurate.

Another set of objections concerns information in the animation that is not in evidence. This can include, for example, fog or ice depicted in a vehicle accident scene, where neither has been established in corroborating, admissible evidence. *See, e.g.,* Kelly v. Ellefson, (Minn. App. 2005) (No. A04-615, unpublished) (*rev'd on other grounds* 712 N.W.2d 759 (Minn. 2006)), (district court abused its discretion by admitting animation that was not disclosed until the morning of the first day of trial; was shown to jury without cautionary instructions; and was misleading, suggesting facts not admitted into evidence or corroborated by any other testimony). In a published case, State v. Stewart, 643 N.W.2d 281, 295 - 296 (MN 2002), the court explained:

> [W]hile it is true that the animation may have made it easier for [the expert] to testify and may have been very effective in depicting the shooting, the animation's effectiveness was enhanced through artists' renditions of facial expressions and movements that did not merely re-create what was in the record, but created impressions depicting deliberate, intentional actions favorable to the state's theory of the case. Because the animation's contents exceeded what was in the record and created impressions that went right to the heart of what the state needed to prove as to intent, and because the animation exceeded the purpose for which it was admitted, the district court erred in admitting the entire animation.
>
> * * *
>
> Animation is a new and powerful evidentiary tool, but must be used with great care. McCormick has cautioned that one party's staged reproduction of facts creates the danger that "the jury may confuse art with reality" and that "the impressions generated by the evidence may prove particularly difficult to limit." 2 John William Strong, McCormick on Evidence 19 (5th ed.1999). Because of its dramatic power, proposed animations must be carefully scrutinized for proper foundation, relevancy, accuracy, and the potential for undue prejudice.

Under Rule 703, while the data relied on by an expert in reaching an opinion need not be admissible, evidence that is normally inadmissible may not be communicated to the jury. If the animation is a visual representation of inadmissible bases for the expert's opinion, it can be excluded under the Rule.

Lastly, on the subject of admissibility, another must-read is Commonwealth v. Serge, 837 A.2d 1255 (Pa. Super. 2003), a case out of Pennsylvania, regarded around the country as one of the most instructive opinions regarding the admissibility issues of computer animations, illustrations, demonstrative evidence and simulations.

Technology is No Substitute for an Effective Litigator

Budget minded attorneys may believe that they can and should present and manage so-called "high-tech" courtroom presentations. However, a litigator must avoid running afoul of the lawyer-as-witness rule and should never be called upon to testify as to the preparation of and underlying data of a demonstrative exhibit. Moreover, most commentators suggest that hiring a consultant allows the litigator to focus on the case rather than the technology. Even a technologically savvy judge is unlikely to tolerate an inexperienced litigator

fumbling with a laptop or projector for long. Moreover, the jury may associate the lack of preparedness with the attorney and the client's cause, whereas, if such mishaps are handled by or attributable to a technology consultant, the negative inference, if any, is attached to the third-party consultant. Although good technology consultants should be invisible during trial, simply having one on hand to deal with mishaps demonstrates to the jury that the litigator was, in fact, prepared and believes in the client's cause.

On the other hand, both judges and juries can resent litigators and their teams of consultants, if it appears that the litigator's strongest element of persuasion is near total reliance on technology (a/k/a "cyber bullying"). There is a careful balance to strike between satisfying modern juries' expectation of technology (the so-called "CSI effect"), providing realistic demonstrative evidence (very often less interesting than "CSI") and overdoing it (cyber-bullying).

Both the judge and jury will expect the litigator to be passionate about the cause, to understand the facts and legal issues and for the oral presentation (including demeanor, gesticulations, tone, body language) to compliment the strength of the demonstrative evidence. If the litigator is unprepared, appears disinterested, is unpersuasive or does not appear convinced of the client's cause, the judge and jury will not be fooled by even the most polished high-tech presentation.

_____

EndNotes

[2]Melvin Belli is generally credited with popularizing the use of demonstrative evidence in civil cases.

[3]Wharton Research Center, Univ. of Pennsylvania (1981)

[4]Minnesota Management Information Systems Research Center (1986)

Posted by Sean Harrington on August 03, 2007 at 12:43 PM in Technology and the Law | Permalink

July 10, 2007

Liability of EDD and Computer Forensics Consultants: Separation of Duties

Recently, my wife and I attended an advanced training seminar in Las Vegas for a document management system (DMS) that we support. During the lunch break of the second day, I questioned the instructor about why the software has no utility for managing metadata. He explained that there wasn't a market need for it. I then pointed out that, by importing documents into and managing them with this tool, metadata was being altered. He thought for a moment and then agreed. Yet, in his focused world of DMS, he seemed genuinely unaware of the controversy and evolving law regarding electronic data discovery (EDD) and electronically stored information (ESI). It was no surprise, then, when I asked him if he was advising attorneys not to manage their electronic discovery artifacts with DMS that he replied, "I don't advise them to do anything! I don't want to get sued."

In the IT profession –and especially in the legal technology arena –technology is changing so fast, that most legal technology consultants spend a fair amount of time attending or presenting at conventions and training seminars, such as the annual ABA TechShow ,® LegalTech ,® the annual ILTA conference and our many local CLEs.

A popular mantra at these gatherings is that attorneys can no longer afford to be ignorant of technology. More than ever, practicing attorneys are being exhorted to cross the boundaries of their discipline, despite the fact that law schools still aren't preparing students for the technology challenges that lie ahead.[1] Consider the following:

- E-lawyering (Web site and blawgs) are now considered a must have for all sizes of firms;[2]
- attorneys are warned that they must realize the liabilities of rendering legal advice *via* a blog;[3]
- attorneys must consider whether an attorney-client relationship exists by accepting e-mailed materials from previously unknown, potential clients where the email address was obtained from a law firm Web site;[4]
- in some jurisdictions, counsel now has an affirmative duty to be cognizant of metadata when sending or receiving electronic documents;[5]
- Minnesota attorneys have been forewarned to prepare for the implementation of electronic filing;[6] and
- trial attorneys must meet the expectations of contemporary jurors (the "CSI effect")

However, as my opening statement suggests, the converse is also happening: as the law and technology are now beginning to collide, legal technology consultants are quick to point out that they do not possess (and do not desire to possess) the requisite expertise to contemplate the *legal* affect of their advice.

Consider the following scenarios:

> **I.** A DMS integrator/vendor represents to a mid-sized lawfirm that DMS is for the management of documents of *any* kind. The firm's lawyers and/or IT department (if they have one) handle the ESI (discovery artifacts/documents) of clients and/or opposing party using DMS for convenience, archival and internal review across the network. Should the DMS vendor have mentioned that managing ESI with the tool alters the ESI? Should the firm attorneys and/or IT staff have reasonably known that managing discovery artifacts might alter the integrity of the data?
>
> **II.** A divorce attorney's client is subject to a preservation order regarding all documents on the hard-drive of the client's computer. The attorney consults with an IT specialist, who is a friend of the family. She uses Symantec® Ghost to obtain a copy of the documents on the

client's computer and puts the Ghost image on a CD-ROM, hands the CD to counsel and goes home. Meanwhile the client continues to use the computer, which has Window Washer® and TweakXP® installed, both common programs advertised to optimize performance of a PC. Later that night, Window Washer runs silently in the background, removing internet cache and scrubbing slack file space, including files that were "deleted" but were recoverable (until now) and, which were potentially responsive. When the discovery requests begin to roll in, counsel attempts to view the content of the CD but, cannot open the Ghost image, because: (a) she doesn't have a license for Ghost; and (b) she doesn't have a compatible and spare PC unto which to deploy the Ghost image. Therefore, not only are these files and documents no longer "readily accessible," but other potentially responsive data that existed the day the preservation order was issued is now long gone from the client's PC.

III. A tech-savvy attorney hires an independent e-discovery vendor to assist him at a Rule 26 (f) meet-and-confer. During the conference, they agree that the parties' personal computers, laptops, PDAs, jump drives, CD-ROM archives and work computers all may contain potentially responsive data. During a subsequent deposition, the attorney –with the assistance of his expert—learns that the bulk of this data exists in two places: on opposing party's personal computer and work computer. The parties stipulate to use the same expert to image these two machines. The expert attaches a write block device to the C:-drive of each computer and performs a low-level sector-by-sector image of the hard hard-drive. During subsequent analysis, very little responsive data is obtained. The attorney expands the search criteria with the express understanding that the costs of analysis increase, accordingly. Nothing turns up. Why? Opposing party used a SATA-compatible external hard-drive not only for data, but also to for the operating system's "pagefile" (f/k/a "swap file"). Using a commonly available utility, the drive-letter assigned to a partition of the external drive containing the page file was hidden from browsing through Windows™ Explorer. The "expert" was not trained for and did not look for this possibility in the Windows registry.

IV. A large sized firm's IT administrator overheard and had been included in on some discussions regarding metadata. The firm's document management system supports the removal of metadata from all files and, the administrator, meaning well, enables the feature but, fails to document this anywhere in the firm's written, established and senior management-approved data retention policy. Months later, in an unrelated event, the firm is sued for malpractice by a fiduciary, who claims that propriety content that he included in a Word document as tracked changes somehow was leaked to the opposing party (inadvertently) and soured the deal. However, now that all metadata has been stripped from all versions of the document that the firm had, the firm is unable to establish that its inability to produce is not the result of gross neglect or intentional spoliation.

All four of the above scenarios could result in a impromptu, unplanned settlement, spoliation sanctions and/or losing the case.

If lawyers choose to defer comprehension of technical issues to vendor-experts and legal technologists choose to defer comprehension of legal issues to their attorney-clients, who's covering the middle ground where the separation of duties is blurred? [7]

In my quest to first articulate the question and then set about to answer it, I polled a few of the brightest minds in the business: Craig Ball , attorney and computer forensic expert; Sharon Nelson , attorney and computer forensic expert; George Socha , litigator and electronic discovery pioneer; and Martin Samson, litigator and internet law expert.

In my view, to begin answering these questions, we must accept a basic premise: Those, who provide electronic discovery consulting services, are one of the very few experts, who sometimes advise lawyers on aspects of case management (whereas expert witnesses, such as a forensic psychiatrist, only interpret and testify). E-discovery consultants are expected to do any or all of the following:

- articulate and implement data retention policies for the corporate clients of law firms;
- draft preservation memoranda;
- assist attorneys in crafting narrowly tailored discovery requests (which necessarily requires an understanding of the rules governing discovery, relevance, overbreadth, etc.);
- assist in responding to discovery requests;
- assist in Rule 26(f) meet-and-confers;
- assist in the taking and giving of depositions;

- assist in the presentation of evidence at trial;
- defend the data collection and analysis methodologies;
- and carefully track and follow caselaw developments in the areas of ESI admissibility, safe harbor provisions, spoliation sanctions, *etc.*

In my [perhaps minority] view, E-discovery consultants need to understand many principles ordinarily left to the wisdom of an attorney, such as the equal inference doctrine, to be able to discern the probative value and relevance –*i.e.,* the value– of their findings in a particular case.

At the time of this writing, I am aware of no published opinions that provides any bright line analysis or guidance regarding the separation of duties. Of the colleagues that I polled, none was aware of any case resulting in a published opinion but, one was aware of a few suits against e-discovery vendors that had been settled or were moving towards settlement; another was certain of numerous instances of EDD vendors or computer forensic examiners visiting mayhem and misfortune upon a case. With the recent proliferation of persons allegedly proficient at computer forensic analysis and copy shops, who have transmogrified themselves almost overnight into purported electronic discovery processing facilities, disaster is certain. However, through the exercise of due diligence, both counsel and the expert can focus on the case at hand and avoid meeting each other at opposites ends of a bargaining table –or worse- in the courtroom.

Selecting Experts

The level of due diligence exercised by the expert generally consists of maintaining technical aptitude and discipline; adhering to industry standard best practices; never taking shortcuts; staying current with technology; delivering consistently high customer service (*e.g.,* responsiveness, effective communication and candor); and, last but not least, not offering the services as an attorney (even if the expert is a licensed attorney) and accepting work only from judges and lawyers to avoid implications of unauthorized practice of law (UPL).

The level of due diligence exercised by counsel in selecting experts will depend on the criticality of the task. If things go awry, counsel may be able to shift some burden if he or she can demonstrate requisite due diligence in selection, delegation, direction and supervision of experts. To the extent that counsel submits himself or herself blindly to the technical directives of an expert that drive certain aspects of a case, the expert's ability to provide directives may be a function of the effective specification of requirements by counsel at the outset and iteratively (throughout the case); and/or the expert's understanding of legal principles.

Many lawyers will take the hard position that the responsibility for comprehending the legal ramifications of technical directives is non-delegable and resides solely with the attorney. Perhaps, this view is attributable to professional territorialism but, in large part, under the obligations of Rule 11 and the applicable Rule of Professional Conduct, the *legal* responsibility for decisions made during the course of litigation do belong to the attorney. Yet, while it may seem unfair to place such a burden on a legal technologist, it seems similarly unfair to expect an attorney to have an intimate understanding of every technical aspect of the systems in question. For the foregoing reasons, selection of the right expert is an essential component of due diligence.

One excellent resource to consult is a jointly-authored whitepaper, *Finding and Researching Experts and Their Testimony*, which addresses the strategic use of search engines, expert directories, license & certification information, discussion post boards and other resources in order to find experts, gather information about them (whether your own or the opposing party's), and assess the admissibility of their testimony. It also includes tips on how the information uncovered might be utilized. Some potentially-relevant Web sites -- both free and fee -- are mentioned.

Additionally, Sharon Nelson and her husband, forensic expert and speaker, John Simek, have published a short paper entitled, *Finding Wyatt Earp, Your Computer Forensics Expert,* wherein they give common sense advice on how to select an expert without needing to take out a business loan. The basics are some or all of the following (which are elaborated upon in their paper): (1) look for meaningful forensics certifications; (2) look for related technical certifications; (3) get the experts *curriculum vitae* early and study it; (4) avoid the seeming jack-of-all-trades; (5) expect the expert to have court qualifications and is prepared to testify; (6) confidentiality: how casual does the expert discuss previous cases and can she be trusted to, answer "no comment," if questioned by the press during your case?; (7) geography: consider the location of the expert, his ability to perform services at a distance; and the associated costs; (8) communication skills: the expert must be able to communicate fluently in English and in lay terms to explain to you (and the jury) his or her findings; (9) costs. While rates billed by a forensics expert are, necessarily, a cost consideration in your case, extraordinarily bargain rates may be an indication of sub-par qualifications. Good forensics experts are not cheap; and (10) references, references, references. Although you're looking for a measure of confidentiality with respect to prior cases, an expert should be able to provide references of previous or existing clients, who can attest to her customer service, timeliness, ability to stay within forecasted budget, *etc.*

Perhaps, there are three things I might add to Sharon and John's list (`though, arguably, one or all could be subsumed into one of their enumerated categories):

> (a) Seek an expert who, not only can communicate ideas, concepts and findings effectively to you and the jury but, also one who is not inclined to produce a voluminous compilation of raw data and drop it in your lap for you to decipher. Your expert should be prepared to provide you with a detailed report that provides meaningful findings, charts, graphs and other information in a usable format, so that you're not continuing to pay an extended hourly rate for him or her to translate what's contained in the report.
>
> (b) To elaborate or, perhaps, clarify the jack-of-all-trades warning: Indeed no one can be an expert on Lotus Notes *and* older MacIntosh computers *and* SGI® IRIX *and* Microsoft® Exchange™ Server *and* Oracle *and* Informix *and* VMX mainframe *and* obsolete Sun Sparc Arrays *and* IBM/Rational ClearCase.™ Further, it is probably unrealistic for you to locate one such person for each different case (`though most cases will deal with contemporary Windows™ operating systems). An effective and genuine EDD vendor or computer forensics technologist is not one, who represents to know all these systems but, rather, who has a broad enough background that he or she can study the systems in question, articulate the requirements in an expedited manner and then source the appropriate person or firm that specializes in the task at hand. In this capacity, the vendor functions as a liaison between you and a pantheon of subject matter experts and, as the liaison, will oversee and audit the data collection, chain-of-custody, analysis and review pursuant to proven methodologies and industry standard best practices.[8]
>
> (c) As Mark Lanterman of Computer Forensics, Inc once explained to me, your expert's testimony about how he or she collected the data and what was found will not be vulnerable to attack by opposing party if the techniques are sound: This is unlike opinion testimony by a forensic psychiatrist. Most often, the testimony boils down to what was found –either the data is there or it was not there. Be concerned if your expert regards and presents findings as subjective opinion, as this may be an indication of faulty data collection and analysis methodologies.

Requirements, Mutual Assent, Contractual Obligations

The second element of due diligence is defining the scope of work, expertise, duties, obligations, limitations of obligations, confidentiality and assumptions. These terms, conditions and exclusions are normally set forth in an Engagement Contract. One resource that I recommend is Nelson, Olson & Simek, *The Electronic Evidence and Discovery Handbook* (ABA, Law Practice Management Section, 2006). Forms 2.1 through 2.6 are invaluable to both counsel and experts in crafting a mutual agreement. To ensure mutual assent, the agreement should be one that both parties contribute to –not one that counsel presents to the expert with a pen and the instruction, "Review and sign here."

When I engage a client and have agreed to work together, I provide a request for information (RFI), which is a good faith effort on my part to gather and identify requirements. Requirements gathering is the fundamental building block –the cornerstone –of every successful project. While I am thorough in the requirements gathering phase and expect clients to also be both candid and thorough, a certain amount of flexibility must be built in; the requirements usually change over time, as the case progresses.

Next, we draft a detailed statement of work. This is the meat of the project, that identifies the contours of the expected work and time required with as much accuracy as possible. This document, also, will evolve over the life of the case.

The third governing document, which rarely evolves, is the vendor engagement contract. In my contracts, I clearly set forth:

- a summarized scope of work, which is usually an closed-ended exclusive enumeration of the services that I have been asked to provide or reasonably believe I will need to provide and a statement that I am not rendering legal advice and that no advice given by me should be construed as legal advice and that the responsibility for all legal decisions made in a case ultimately belong to counsel of record;
- the estimated costs and fees;
- the assumptions;
- nature and scope of third party services, if any;
- two-way confidentiality provisions;
- modification/amendment/waiver provision;

- governing law;
- invalidity/severability of provisions;
- successors and assigns;
- entire agreement and notice recital;
- indemnification;
- records auditing and retention policy; and
- enforcement provisions.

Conclusion

There is no bright line that separates the duties of the electronic discovery vendor or computer forensics expert and counsel in a given case. Avoidance of disputes and success of the project depend on due diligence, good faith collaboration, clear expectations and effective communication on the part of both parties. If a dispute does arise, specifically, if the taking of action or refraining from taking of action based upon the advice given by an expert to counsel has an adverse effect on the case, the determination of liability (negligence) between the parties will likely depend on each party's ability to demonstrate due diligence.

Endnotes

[1] Steven C. Bennett, *Teaching Tech Skills to Lawyers,* The Nat'l L.J. 13 (2006) ("Most law schools . . . offer little formal technology skills training. Introductory legal writing classes eventually teach students to use computerized research but, most schools prefer a 'paper first' approach. . . . Other forms of technology skills training are rarely offered. Essentially, what law students learn about technology, they learn on their own.")

[2] American Bar Assoc., *Public Perceptions of Lawyers Consumer Research Findings,*2002 (reputation of the profession is at an all time low but, lawyers can improve the profession's image by responsibly providing legal information to the public *via* the Internet); *and see* the ABA's *Best Practices Guidelines for Legal Information Web Sites,* approved by the House of Delegates in 2003; Jim Calloway, *Every Law Firm of Every Practice Setting and Size Needs to Have a Web Site,* Dec. 2005.

[3] *See, e.g.,* Sean Harrington, *Beware All Ye, Who Blog,* official blog of the MSBA Computer and Technology Law Section, April 2007.

[4] David Hricik, *The Speed of Normal: Conflicts, Competency, and Confidentiality in the Digital Age*, Computer L.Rev. and Technology J., 73, 74-76 (2006)

[5] Stay tuned: The ABA Standing Committee on Ethics and Professional Responsibility opined that it is generally permissible under the Model Rules to examine metadata in documents received electronically. (Formal Opinion 06-442: Review and Use of Metadata, August, 2006). State ethics rules, however, impose varying obligations. The New York State Bar Association Committee on Professional Ethics has opined that N.Y. DR 4-101 essentially requires the removal of metadata before transmitting electronic documents to prevent the disclosure of metadata containing client confidences or secrets. (Opinion 782-12/8/04). Alabama has followed New York. Both states hold that the lawyer who has inadvertently received metadata has a duty to avoid use of the inadvertently disclosed information. Under Alabama's rule, "Absent express authorization from a court, it is ethically impermissible for an attorney to mine metadata from an electronic document he or she inadvertently or improperly receives from another party."

[6] Chief Justice Anderson, State of the Judiciary 2006 & 2007 (same)

[7] *The Minnesota Lawyer Blog* recently confronted this question in a May 9, 2007 entry, concluding, "The results seem to speak to a quandary about who is qualified for this task. IT staff are likely to understand the technological developments, but not the legal ones. Attorneys, vice-versa. As a result, support staff are called on to be generalists capable of working both sides of the street." The conclusion was based on a poll of Webcast participants conducted by Fios, an Oregon-based electronic discovery and litigation service: "Who in your firm is responsible for directing traffic at the intersection of law and technology?" The answers, coming from an audience split between law firms and corporations with in-house counsel was inconclusive: 12% General counsel; 16 % IT staff; 24% staff attorneys; 4 % paralegals; 30% litigation/practice support staff; 14%

partners; and less than 1% associates. The poll further revealed that, within firms, support staff are primarily responsible for tracking these changes 52 percent of the time, while within corporations it's more likely to be a staff attorney (35 percent) or someone from IT (22 percent).

[8] A number of organizations have published best practices, including, *e.g.,* the Information Security and Forensics Society (ISFS), the "Scientific Working Group on Digital Evidence" (SEGDE), the *Computer Security Incident Handling Guide,* published by the National Institute of Standards and Technology (NIST), the Information Systems Audit and Control Association (ISACA), Forum of Incident Response and Security Teams (FIRST), *inter alia.*

Posted by Sean Harrington on July 10, 2007 at 04:36 AM in Technology and the Law | Permalink

July 03, 2007

Groundbreaking Decision Challenges Admissibility of E-Mail

Groundbreaking Decision Challenges Admissibility of E-Mail - That's the characterization that my colleague, Sharon Nelson, has given this May 4th memorandum opinion from *Lorraine v. Markel American,* out of the U.S. District Court for the District of Maryland. Here, U.S. magistrate judge Paul Grimm (unusually presiding by the parties' consent under § 636(c)) provided a 101-page prolix analysis of how and when electronically stored information (ESI) should be admitted into evidence in terms of the evidentiary foundations required under the recently amended Rules of Evidence. He explained that, whenever electronic documents are offered as evidence, the party proffering the electronic information must consider the following:

- whether the electronic evidence is relevant (Rule 501);
- the authenticity of the information (Rule 901(a));
- whether the information is hearsay, including relevant expectation, if the document is offered for its substantive truth (Rule 801);
- the original writing rule (Rules 1001-1008);
- and whether the probative value of the document is substantially outweighed by the danger of unfair prejudice or other considerations (Rule 403).

Although, the court noted that the rules may not apply to every evidence, counsel should ensure that they have satisfied the relevant criteria prior to submitting electronically stored information as evidence for a motion or at trial.

Both parties in *Lorraine* had filed cross-motions for summary judgment, which motions were supported with hard copies of e-mails. Although neither party, apparently, objected to the other's use of the e-mail, Magistrate Grimm *sua sponte* observed that Fed.R.Civ.P. Rule 56 requires such motions be supported with admissible evidence and concluded that the email copies were not. Accordingly, he denied both motions without prejudice and seized the opportunity to issue the memorandum opinion delineating admissibility problems of electronic evidence.

The opinion provides, not only a review of the requirements for admitting electronic evidence under the Federal Rules of Evidence, but also a practical discussion of some of the technology and document management issues raised thereby. Magistrate Grimm further noted that, while there has been extensive discussion of the rules regarding e-discovery, very little has been established regarding admissibility: Electronic documents aren't automatically admissible just because they were produced by one or either party. *See, e.g.,* Solovy & Byman, *Don't Let Your E-Evidence Get Trashed*, Nat'l Law Journal (June 2007).

Once you've assembled an array of ESI evidence, the task is only half complete; you must now contemplate admissibility. Solovy & Byman suggest a three-step approach: "seek a stipulation; barring that, propound a request for admission; and barring that, be prepared to establish authenticity and hearsay exceptions at trial." Others may elect to send the request-for-admissions first as, perhaps, a way to send a subtle hint to opposing counsel to start thinking about stipulations well in advance of trial.

Obviously, if counsel is using requests-for-admissions to authenticate ESI before trial, you'll have to attach the exhibits to the requests: One method is to attach printed copies, affixed with exhibit stickers. *See fig. 1-1.*

---

figure 1-1.

1. Admit that each of the following, attached hereto as an exhibit to the within request-for-admissions, is a true and accurate reproduction of the original document identified

(a) Exhibit A: August 06, 2005 memorandum of Kyle Smith, M.D. to Phyllis Milton dated; and

(b) Exhibit B: Manuscript draft No. 23, dated January 15, 2005 of Phyllis Milton.

In document-intensive cases, there may exists hundreds of documents consisting of thousands of pages that need authentication. An alternative method of handling these is to provide the documents as PDFs[1] (sans metadata) on a *closed-session non-rewritable* CD-ROM or DVD-ROM. *See fig. 1-2.*

---

figure 1-2

1. Attached hereto as Exhibit A is a list of documents identified by Bates number, date, author, and subject matter. An image of each document in PDF format has been provided on the CD-ROM attached hereto as Exhibit B. Regarding each such document, an electronic version of which exists thereon Exhibit B, please admit:

(a) The electronic version of each document identified by Bates Number in Exhibit A is a genuine, true and correct copy;

(b) The genuineness and authenticity of the electronic version; and

(c) The electronic version is admissible as a medical or business record pursuant to [Minnesota Rule].

See also forms 5.1 ~ 5.25 in the appendix to Nelson, Simek & Olsen, *The Electronic Evidence and Discovery Handbook*; §§ 6:73 & 6:76 from Schaeffer's *Deposition Checklists and Strategies*

I recommend that counsel initial or sign the CD-ROM prior to submission and ask that opposing counsel initial or sign the CD-ROM and return with the answered admissions to ameliorate any future dispute about what electronic documents were on the CD and had been authenticated and stipulated to between the parties. Alternatively, if you concerned about the unlikely event that a dispute will arise and you'll be in a lawyer-as-witness conflict regarding what was on the CD-ROM, you may want to entrust this process to a third-party, reputable e-discovery vendor, who maintains a chain-of-custody and, if necessary, a database of the MD-5 hashes of the files at issue.

While we're on the subject of propounding discovery requests, another industry colleague, Craig Ball, reminds that we need to devote more time to thinking about ***what*** the evidence is (instead of whereon it resides).

> Too often, we fixate on the containers — the e-mail, spreadsheets and databases — with insufficient regard for the content. This isn't just a rant against producing parties. I see the failure as well in requesting parties determined to get to the other side's tapes and hard drives but unable to articulate what they're seeking. Saying, "I want the e-mail" is as meaningless as saying, "I want the paper."
>
> E-mail, voicemail, ledgers or lipstick on the mirror are just media used to hold and convey information. It's the transaction and the content that make them evidence. The form matters, but only for reasons of accessibility (Can I view or hear it?), preservation (How do I protect it?), utility (Can I search and sort it?), completeness (Is something added or absent?) and authentication (Can I rely on it?).
>
> Pondering the essential nature of evidence can't remain the exclusive province of law review commentators and law school professors. As never before, trial lawyers in the trenches must think hard about just what is the evidence? What are we really looking for? What gets us closer to the truth?

Craig Ball, *E-Evidence: Who Let the Dogs Out?,* Law Technology News

---

[1] Bear in mind that, if opposing party originally produced the ESI for you in PDF form and you altered the data in any manner (such as OCR *via* Acrobat Professional, which deskews the image and can degrade clarity (in addition to adding hidden text that is the OCR)) or remove metadata, you have just altered the electronic file. Ordinarily, this shouldn't be an issue, as far as best evidence is concerned but, if it is pointed out that the image

was altered in any fashion, it could cause a non-tech savvy judge to be concerned that other portions of the image had been altered or redacted and he or she may be inclined to rule the images as inadmissible.

Posted by Sean Harrington on July 03, 2007 at 04:27 PM in Caselaw | Permalink

July 02, 2007

Legal Writing and technology: Odd Bedfellows

In my previous post, I introduced the debate concerning the benefits of legal records accessibility on the Web versus suggestions that some records contain personal and confidential information that, perhaps, should not be readily accessible. Today, let's visit the subject of the judiciary's growing reliance on Web resources from Wikipedia to YouTube[1] and the accompanying concerns that jurists and legal scholars are beginning to express.

[updated July 10, 2007]

Research by the New York Times revealed more than 100 rulings citing an encyclopedia written by nobody and everybody: Wikipedia. The tally, dating back to 2004, includes 13 from the circuit courts of appeals.

Despite its ranking as among the 20 most popular Web sites, the online encylopedia's reputation suffered when several instances emerged of entries being tampered with by pranksters or containing errors.[2] And, although some colleges and professors forbid students from citing Wikipedia as a central source, it has established credibility in some courtrooms, creating controversy with legal scholars, who disapprove of such unreliable sources. In an opinion announced July 2, 2007, *Lands Council v. McNair,* 07-35000 (9th Cir., July 2, 2007), the Ninth Circuit consulted Wikipedia to evaluate the weight of a secondary authority authored by environmentalist/activist Derrick Jensen. In a 2005 case before the Tennessee court of appeals worth hundreds of thousands of dollars, the site was used to help define the meaning of the word "beverage." *English Mtn. Spring Water Co. v. Chumley,* 196 S.W.3d 144 (Tenn. App. 2005). It was also cited recently in a federal district court in Florida to offer background on the term "booty music." In one instance (cited by the Times), a decision from a Chicago appeals court cited Wikipedia in a drugs case - even though the judge, Richard Posner, had first-hand experience of its unreliability: an entry claimed the conservative commentator Ann Coulter had been his law clerk. (Judge Posner had never met her).

However, Wikipedia is only the latest in a series of technological features that lend themselves towards unreliability. Another area that I've seen this --one that I specialize in-- is digital briefs: An article, Bradley J. Hillis, *Electronic Briefs in Trial and Appellate Courts,* (2000), urging the use of digial briefs suggests that they, "may change the way judges analyze legal precedent by encouraging them to go from the case the attorney initially linked to the cases cited in that case, a sort of deeper foundation of the law, or even encouraging judges to search the Web to check factual assertions."

Perhaps. But, what if the site that the link points to is one operated by or prepared by the attorney? How does the judge know if the case presented by a link is, indeed, the actual text of the opinion? How does a judge know if this isn't a way to introduce materials to the court that were not properly preserved in the record on appeal (*e.g.,* a link to an acceptable document but one, that itself, has embedded links to photographs, articles, or other media not admitted into the record)? And, what about the permanency of the links?

Indeed in one digital brief that I recently filed in the Tenth Circuit (a petition for rehearing *en banc*), I had set up a complete docket of the entire trial court and appeal on a Web site. Every citation in the petition, including some authorities, linked to PDFs on the Web site and, in so doing, was completely within that court's guidelines for hyperlink use within briefs. On the other hand, the Opening Brief and Reply Brief were entirely self-contained briefs on CD-ROM, utilizing Acrobat's destination tool and pointing to PDFs (authorities, trial court filings, *etc.*) that were on the CD or embedded within the main document.

Concerns of URL permanency have been raised by others, previously: Coleen Barger, an associate professor with the University of Arkansas' William Bowen School of Law, gave a presentation, *The Great Disappearing Act: Preserving URLs in Judicial Opinions,* to the AALL Annual Meeting and Conference in 2005 and, which was based on her earlier treatise, *On the Internet, Nobody Knows*

You're a Judge: Appellate Courts' Use of Internet Materials, 4 J.App.Prac.&Process 417 (2002). She posed many questions but concluded, ultimately, that "Too many recent opinions rely upon questionable or non-available sources, and such misplaced reliance certainly cannot be what judicial authors wanted or intended. *Id.* at 419.

Professor Michael Whiteman, an associate professor of law and associate dean for law library services and IT at the Chase College of Law, addressed related issues in *Appellate Court Briefs on the Web: Electronic Dyamos or Legal Quagmire?,* 97 Law Libr. J. 467 (2005). In his treatise, he enumerates many of the benefits to both lawyer and jurist of digital briefs and e-filing, yet points out that, "Ironically, the benefits of shifting to e-briefs may actually diminish our ability to successfully archive the information we are attempting to preserve." His concerns, as he later explains, is related to future changes to the format in which these files were created and may no longer be readable by future technology standards. (He recalls, as an example cited in Kunsch, *Diogenes Wanders the Superhighway: A Proposal for Authentication of Publicly Disseminated Documents on the Internet,* 20 Seattle U. L. Rev. 749, 773 n.115 (1997), difficulties accessing data from a 1960 census where the records were stored on tapes that could be read with a UNIVAC type II-A drive, which became obsolete in the seventies).

In conclusion, prudence should be exercised by both attorneys and jurists in citing authorities and in choosing and the implementation of technologies to submit and preserve works to courts. In a future law review article, I will dicuss the muliplicity of e-filing and e-brief requirements, standards, loopholes, techniques and ethical considerations. I will argue for the need to develop standards in both federal and state courts, which standards must be dynamic and must adapt to the evolving technologies.

As a final note, both "Legal writing" has its own Wikipedia entry and "Electronic Briefs" has its own Wikipedia entry. Rely on them at your own risk!

---

[1] *See, e.g., Central Manufacturing, Inc. v. Brett Bros.,* (7th Cir., May 02, 2007) (citing http://www.youtube.com/ watch?v=4Cu1WXylkto)

[2] *E.g.,* In 2005, John Seigenthaler, a writer, was falsely accused of being linked to the assassinations of John F Kennedy and his brother, Robert, by a Nashville delivery driver playing a joke on a co-worker. Seigenthaler, who had served as an administrative assistant to Robert Kennedy and was one of the pall bearers at his funeral, was not amused.

Posted by Sean Harrington on July 02, 2007 at 11:03 PM in Technology and the Law | Permalink

June 13, 2007

Google aids public record accessibility

Google announced recently that it is assisting states in making available public records that are now unavailable or difficult to easily access online. Google hopes to persuade federal agencies to employ the same tools, an effort that worries consumer privacy pundits, while receiving praise from open government advocates. Google announced that it has already partnered with Arizona, California, Utah and Virginia to remove technical barriers that had prevented search engines, including Microsoft, Yahoo and Google, from accessing tens of thousands of public records (education, real estate, health care and the environment). The newly available records will not be exclusive to the search engines owned by Google, Yahoo and Microsoft.

Despite the obvious benefits of this Google initiative for those conducting Web searches, privacy advocates said they are worried about unintended consequences, cautioning that some records may contain personal and confidential information that should not be widely available. The debate has been ongoing for some time.[1]

In unrelated news, the Reporters Committee for Freedom of the Press announced that "Federal Court Moving Away from Secret Dockets"

> The Reporters Committee for Freedom of the Press commends as a good step forward in reducing court secrecy the U.S. Judicial Conference's vote today urging federal courts to acknowledge sealed cases in their electronic dockets. The Conference - the chief policy-making body for the federal court system - today strongly recommended all federal trial courts with electronic docketing systems clearly indicate to users that cases are sealed instead of displaying a notice reading "No such case." In announcing the change, Chief Judge Thomas F. Hogan of the U.S. District Court in Washington, D.C., credited the Reporters Committee with uncovering the existence of the off-the-docket cases, which he said were unknown to many court officials.

[1] *See, e.g.,* Merrill Douglas' January 02, 2006 article, discussing the pros and cons of unfettered online public access to court records that formerly required a trip to the courthouse to obtain.

Posted by Sean Harrington on June 13, 2007 at 08:17 PM in Technology and the Law | Permalink

.

June 06, 2007

Professor Hricik's views on metadata

This past March at the ABA TechShow, I had the pleasure of listening to and briefly meeting Professor David Hricik. I also follow the Legal Ethics Forum here on Typepad, where he posts.

It's not often that legal technology and legal ethics --both of great interest to me-- intersect. One of those intersections, which we've discussed herein our Section, is that of metadata. Prof. Hricik recalls discussing that subject with Professor Monroe Freedman, recently, and this is a summary of their discussion, as told by Prof. Hricik:

> It was quite interesting, and I'll not be able to do the conversation justice here, but wanted to try to crystalize why we disagree on the metadata issue, but agree quite firmly on the broader issues of the adversary system.
>
> To begin, I think we were both *not* surprised to learn that each of us strongly believes in the adversary system. (He mentioned a popular thinker, Professor Simon of Columbia, who thinks lawyers should try to "do justice" and that struck me as quite odd, for example. Doing justice isn't my job when I'm representing a client, and any lawyer who sets out, in our system, to do that, is not a lawyer I'd want to hire or would recommend to a client.) I don't think that when serving as an advocate I have a general obligation to help my opposing counsel, and indeed, quite the opposite: if I can use his mistake to his client's disadvantage, I am happy. (Oh, I could tell war stories here. My favorite one though is when plaintiff's counsel just before a case was set for trial in Texas state court amended the petition to include a federal claim, and off we went, after several years of meandering in state court, to federal court.) Anyhow...
>
> Why do I think metadata is different. Why do I believe that I shouldn't rummage through a Word document sent to me by an opposing counsel to see if it includes confidential information.
>
> I think, and my forthcoming article's title tells you this, that the difference is that I am acting intentionally to uncover something that I know should not be there. It's not passive acts by me in responding to their activity, but is instead actions by me in taking steps (granted, relatively simple ones), to find what I know shouldn't be there. In discovery, that's fine, but not in daily practice. In addition, the errors of law that we take advantage of are of a different kind -- I find it unreasonable to expect lawyers to keep up with all this technology (it will always be ahead of them - see the post on Vista below). And, the cost to clients is another issue. To make scrubbers fool-proof, they'd have to be on every computer (laptops, home computers, client's computers...).
>
> To me, this puts mining for embedded data "beyond" the inadvertent fax, when I simply look at something that's sent to me. To get the benefit, I have to actively look for information that I know should not be there, but which I'm hoping through neglect or technological failure still is. The better analogy to me is opening up the brief case left on the deposition table and rummaging around for documents. Or, rummaging through a pile of papers left by mistake on the conference room table after the lawyer left, hoping to find a critical document. That puts it past a mistake, and into intentionally taking advantage of other people's failures.

Posted by Sean Harrington on June 06, 2007 at 05:34 PM in Technology and the Law | Permalink

May 18, 2007

CDA and DMCA ambiguities addressed by the 9th Cir.

In *Perfect 10, Inc. v. CCBill, et al.,* the U.S. Court of Appeals for the Ninth Circuit clarified persistent ambiguities about how a portion of the federal Communications Decency Act (CDA) applies to state law. Specifically, Section 230, which has been a defense for Internet service providers, bloggers and Web publishers, broadly immunizes providers of an "interactive computer service" from liability for content that others post. The 9th Circuit concluded that § 230 can also shield service providers from liability when they are confronted with allegations that their users violated state law (such as right of publicity and trademark statutes). Disputes involving federal copyright and criminal laws, however, remain exempt from such immunity.

The opinion also addresses the Digital Millennium Copyright Act (DMCA), including the provision of non-liability of Web hosts for the content their users post, as long as they take down the offending content promptly upon being notified by the copyright holder and meet a number of other standards (*e.g.,* not receiving "direct financial benefit" from infringing content). The court clarified that providers do not have to actively police their systems for infringement. The DMCA requires the complainant sending so-called takedown notices to include specific information in their requests to service providers, such as identifying the infringing content and certifying, under penalty of perjury, that the person sending the notice is "authorized to act on behalf of the owner of an exclusive right that is allegedly infringed." The court concluded that service providers are not obligated to comply with requests that fall short of those standards and expressed concern about First Amendment free-speech violations that could occur if a provider removes content that doesn't actually infringe on copyrights.

Posted by Sean Harrington on May 18, 2007 at 06:25 PM in Caselaw | Permalink

May 17, 2007

Availability of Online Resources May Be One Reason for Reduction in U.S. S.Ct. Caseload

According to Chief Justice John Roberts, the number of cases heard by the U.S. Supreme Court is declining in part because circuit courts can locate previous legal decisions online in cases where they might have once turned to the Supreme Court for guidance. >> full article text >> This admission, combined with the recent rule change concerning unpublished opinion citation, adds an interesting twist to the ongoing debate concerning the availability of online opinions, online briefs and electronic access to court records.

Posted by Sean Harrington on May 17, 2007 at 06:05 PM in Articles | Permalink

May 07, 2007

Limitations on Computer Forsensics Examiner's Access Results on Dismissal of Pornography Charges

In *State v. Brady,* decided April 13th, an appeals court affirmed the dismissal of child pornography charges against Daniel Brady, Sr.

The trial court had appointed Dean Boland to serve as a computer forensics expert witness for defendant. Boland, a licensed attorney, had previously served as an expert witness. The trial court issued a protective order transferring the alleged contraband evidence to permit defendant's attorney to render effective assistance of counsel and also that Boland was also authorized to possess the evidence, pursuant to Ohio's obscenity statute, which permits possession of certain contraband material if used for a "proper purpose" by a "prosecutor, judge, or other person having a proper interest in the material." Accordingly, the prosecution provided the evidence to Boland in early June of `05.

On June 24, 2005, the FBI executed a search warrant on Boland's residence and seized his computer and several compact discs, which contained the alleged contraband at issue. The affidavit in support of the warrant alleged Boland violated 18 U.S.C. § 2252A, which, unlike its state counterpart, does *not* contain an exemption for a "proper person" using the material for a bona fide purpose. As the appeals court noted, Boland testified during a hearing in the case against Brady, "upon the advice of counsel and due to the threat of additional federal prosecution, he could not possess another copy of a compact disc containing the allegedly illegal images in this matter." He further testified that he could not conduct a proper investigation of any Web sites from whence the images allegedly came. Boland explained, he could not use his expertise to create potential exhibits for Brady's trial. Although the prospect was raised that Boland could have reviewed the evidence at the prosecutor's office, this would not allow Boland to create exhibits for trial. Boland further explained that he uses specific software for his analysis that the prosecutor's office does not possess. Additionally, even though Boland would be in the prosecutor's office, it could be argued that he "received," albeit temporarily, child pornography in violation of 18 U.S.C. §§ 2252(a)(2)(A) and/or 2252A(a)(2). Another of Boland's concerns was visiting Web sites where the allegedly illegal images may have originated. He believed he might be subject to federal prosecution for conducting illegal internet activity at the prosecutor's office. Finally, Boland testified regarding his concern that he would not be able to record any of his work at the prosecutor's office for fear of federal prosecution, therefore, he would have to memorize his entire analysis of possibly hundreds of images for his trial testimony. The trial court found that viewing the images at the prosecutor's office was not a viable solution and, in consideration of the totality of the circumstances, granted Brady's motion to dismiss and dismissed all 50 counts of the indictment related to pornography.

On review, the appeals court concluded that the FBI's actions violated defendant's constitutional due process right, which actions made it impossible for defendant to utilize expert witness services. The court found that "not only was Brady denied the expert services of Boland, he was denied the expert services of all potential experts." (Boland testified that no other expert witness would risk federal prosecution to assist Brady. Further, Boland testified that, in his opinion, Brady's counsel was duty-bound to inform potential experts about the possibility of federal prosecution and that, in light of this requirement, it would be nearly impossible to find a competent expert). This appeals court concluded that Boland had a legitimate reason to be concerned that 18 U.S.C. §§ 2252(a)(2)(A) & 2252A(a)(2) operated to prohibit him from receiving any images of child pornography that have traveled in interstate or foreign commerce, "including by computer." 2007 WL 1113969 (Ohio App. 11 Dist.) www.sconet.state.oh.us/rod/newpdf/11/2007/2007-ohio-1779.pdf

Posted by Sean Harrington on May 07, 2007 at 06:24 PM in Caselaw | Permalink

MSBA Computer and Technology Law Section

The Official Blog of the Minnesota State Bar Association's Computer and Technology Law Section.

April 13, 2007

Beware, all ye who blawg

Lawyers Warned; Beware the blog

"A growing number of law firms are "e-lawyering," offering immigration assistance, legal services for divorce and wills online . . . many law firms are giving e-mailed legal advice and using informational blogs . . . These practices are creating new liability exposures." >> full article text >> This article suggests a checklist of considerations before one considers "e-lawyering." One consideration not contemplated therein, however, is the prospect of UPL: Even if, *arguendo,* you are licensed in one state, what UPL liability is there, if any, for an attorney-client relationship (express or implied) established with a Web site visitor from another state, where your legal advice was not narrowly tailored to your practicing state?

Another consideration is the more recent statement issued by the Chubb Group of Insurance Companies, which provides guidelines for law firms that want to get into the business of blogging, without compromising their insurability. Chubb's position is that that bulletins posted on Web logs are acceptable, so long as answers are not provided to questions that could be construed as seeking advice. Chubb's clarification followed the publicity created by a March 16 New Jersey Law Journal report that the carrier refused to cover a blawg proposed by Freehold, N.J., firm, Lomurro Davison Eastman & Munoz. When partner James Paone II called Executive Risk Specialty, a unit of Chubb, he was told "this is not a risk they are interested in undertaking." Word spread like wildfire (especially in blawgs). Chubb explained that it released its April 4 statement to correct "confusing media reports about the company's willingness to insure blogs." The company said that informational blogs, which are essentially news, "pose a minimal level of risk from Chubb's underwriting perspective, but that advisory blogs, such as those in question-and-answer format, potentially establish attorney-client relationships that can lead to malpractice suits." Chubb said that its underwriters will evaluate each submission on a case-by-case basis.

Posted by Sean Harrington on April 13, 2007 at 05:34 PM in Articles | Permalink

April 13, 2007

Employees Waive Privilege In Communications Transmitted From Company Computer System

In *Long v. Marubeni America Corporation,* 2006 WL 2998671 (S.D.N.Y., October 19, 2006), the court held that both the attorney client and work products privileges were waived by employees using a company computer system to transmit otherwise privileged communications to private counsel, which communications were sent from private password-protected accounts (not from the employer's email system). Significantly, a cache of the emails were retained by the company's system as "temporary internet files." Because the company could and did obtain these emails by reviewing its own system, the court held that the waiver was created through employees' failure to maintain the confidentiality of these communications with regard to the company's electronic communications policy, which policy advised employees not to use the company system for personal purposes and warned that they had no right of privacy in any materials sent over the system. The court reached this result notwithstanding its factual finding that employees were without knowledge that a cache of their email communications had been retained. *But see Lara Curto v. Medical World Communications, Inc.,* et al., 2006 U.S.Dist. Lexis 29387, (E.D.N.Y. May 15, 2006), where use by employee of company laptop at home to send personal email communications to counsel from a personal email account does not waive any attorney client or work product privileges that may exist therein, notwithstanding computer usage policy that warned employees that they had no right of privacy in Company computer equipment, the contents of which could be inspected by the Company.

Posted by Sean Harrington on April 13, 2007 at 12:49 PM in Caselaw | Permalink