

Ungaretti & Harris LLP
E-Discovery Update

What is ESI and How Should We Handle It?

By Kamau A. Coar

Amendments to discovery rules and recent caselaw have highlighted an increased importance placed on electronically stored information (ESI). It is clear that producing paper documents in litigation is not nearly enough, and that critical information can be and is often located in data stored electronically. All of this leads to the obvious question of what constitutes ESI.

As the courts sift through each new lawsuit raising questions about what forms and types of ESI should be produced, the definition of ESI becomes clearer. In the meantime, many judges rely heavily on what parties agree to produce. What forms and types of ESI have to be produced in a given case turn less on precedence and more on what a party says and how that party acts. A party has to fully understand what ESI it has, what ESI it wants in discovery, and what ESI it wants to protect in order to effectively serve and protect its interests. Not understanding the importance of metadata - as a crucial part of ESI -

can be the difference between a successful lawsuit and an extremely costly one.

For example, metadata has been considered relevant and discoverable by federal courts for several years. See *e.g.*, *In re Verisign, Inc. Securities Litigation*, 2004 WL 2445243 (N.D.Cal. Mar. 10, 2004). But courts have also made clear that they will not compel the production of certain ESI, such as metadata, when a party did not make that a part of its request. *Autotech Technologies Ltd. Partnership v. Automationdirect.com, Inc.*, 248 F.R.D. 556 (N.D. Ill., 2008); *D’Onofrio v. SFX Sports Group, Inc.*, 247 F.R.D. 43, 48 (D.D.C. 2008); *Wyeth v. Impax Labs., Inc.*, No. Civ. A. 06-222, 248 F.R.D. 169, 170-72, 2006 WL 3091331, at *1-2 (D. Del. 2006). If a party does not ask or specifically request metadata, it may miss critical information to its case.

Why Format Is Key

It is also important to understand the format ESI comes in. See *e.g.*, *In re Payment Card Interchange Fee and Merchant Discount Antitrust Litig.*, 2007 WL 121426 (E.D.N.Y. Jan. 12, 2007). In this case, the court found that “requiring the Individual Plaintiffs to re-produce data that they have already produced in searchable form (albeit possibly not searchable in every way that the defendants would like), or that they have already substantially processed for such production, would impose an undue burden on them.”

After recent amendments in both 2006 and 2007, Rule 34 now provides that a document request “may specify the form or forms in which electronically stored information is to be produced.” The rule also states that, if necessary, the responding party may be required to translate the requested information into a reasonably usable form. The ESI format chosen can have significant affect on the cost of production, as well as the efficiency and usefulness of the data. Confronting this issue in the early stages of discovery can save considerable time and money.

Until the courts completely clarify what is ESI and what has to be produced in litigation, understanding what ESI is available and its importance is critical to effective litigation. But even as these questions are answered, courts have expressed a reluctance to change what

Contents

What is ESI and How Should We Handle It?

Kamau A. Coar

The Discoverability of Text Messages in the Wake of Quon v. Arch Wireles

Steffany L. Hreno

The Smoking Voicemail: Applying E-Discovery Best Practices To Evidence Stored By Voicemail

Richard H. Tilghman

Instant Messages-Discoverable and Dangerous: How the Law Treats IMs And What Companies Can and Should Do

James M. Carlson

You Don’t Know What You’ve Got ‘Til It’s Gone...The Discovery of “Deleted” Electronic Data

Jessica K. Thomas

litigation parties have already agreed to. One court held that an amendment to the discovery rules “does not justify the abdication of the parties’ agreement”, especially given the security concerns raised by Defendants about maintaining the confidentiality of electronic documents. *In re ATM Fee Antitrust Litigation*, No. C 04-02676, 2007 WL 1827635 (N.D.Cal. June 25, 2007).

As soon as litigation begins, it is critical to have a full understanding of what information is available. A party has to understand what information it has, as well as what information it wants. There are some cases where it is not important who specifically accessed a document, when, and other specific details ESI provides over hard copies. In other cases, that information is vital. Understanding ESI and the ramifications of any agreements made on the production of ESI can radically alter what information is exchanged in litigation, and consequentially the result of that lawsuit.

The Discoverability of Text Messages in the Wake of *Quon v. Arch Wireless*

By Steffany L. Hreno

Venturing into what it described as “a new frontier” of electronic communications law, the 9th Circuit’s recent decision in *Quon v. Arch Wireless Operating Co., Inc.* sharply limits the ability of employers to obtain copies of text messages sent by employees on company-financed accounts. The court’s ruling bars employers who contract their email and text messaging services to outside service providers from reading their employees’ electronic communications without their consent.

The decision came in the case of Jeff Quon, an Ontario, California police officer whose boss obtained copies of the text messages Quon had exchanged on a department-issued pager directly from the City’s service provider, Arch Wireless, and reviewed them to determine whether Quon’s monthly overage charges resulted from personal communications. The court unanimously held that in doing so, the Ontario Police Department violated the Fourth Amendment’s prohibitions against unreasonable search and seizure. Despite the department’s formal policy maintaining the right to read the electronic communications of its employees, the *Quon* Court found that “operational reality” at the department was that employee emails and text messages were not subject to audit so long as the employees paid for any overages. Under these circumstances, the court held, “Quon had a reasonable expectation of privacy in the

text messages archived on Arch Wireless’s server.” The *Quon* decision, however, does not merely apply to situations involving governmental entities bound by the prohibitions of the Fourth Amendment. In a separate part of its ruling, the court held that under the Stored Communications Act (“SCA”) of 1986, Arch Wireless provided an “electronic communication service” (“ECS”) to the City of Ontario. The SCA defines an ECS as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. §2510(15). Such services are prohibited from “knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service,” unless, for example, that person or entity is “an addressee or intended recipient of such communication.” *Id.* §2702(a), (b). When Arch Wireless knowingly turned over the text-messaging transcripts to the Ontario Police Department, which was not “an addressee or intended recipient of such communication,” the *Quon* Court held that it violated the SCA.

The SCA has broad implications for all e-discovery, particularly in civil litigation. Unless made with the consent of a party to the communication or, in some cases, the consent of the subscriber, courts have uniformly held service providers may not disclose the contents of text messages and other electronic communications to civil litigants even when presented with a subpoena. *See, e.g., In re Subpoena Duces Tecum to AOL, LLC*, slip copy, 2008 WL 1956266, at *4 (E.D. Va. Apr. 18, 2008) (finding subpoena unenforceable “consistent with the plain language of the Privacy Act because the exceptions enumerated in § 2702(b) do not include civil discovery subpoenas”); *O’Grady v. Superior Court*, 139 Cal.App. 4th 1423, 1441 (Cal. App. Ct. 2006) (“A subpoena is not enforceable if compliance would violate the SCA. Any disclosure violates the SCA unless it falls within an enumerated exception to general prohibition.”).

As a result of the SCA, civil litigants seeking discovery of text messages must generally identify the parties to the communications and request copies directly from them. As the *O’Grady* Court noted, “Where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions.” *O’Grady*, 139 Cal. App. 4th at 1446.

A recent opinion from the Eastern District Court of Michigan sets forth detailed parameters for the review and production of discoverable text messages between

civil litigants. In *Flagg v. City of Detroit*, slip copy, 2008 WL 787061 (E.D. Mich. Mar. 20, 2008), the plaintiff sought the production of text messages to support his claim that the defendants' lax investigation into his father's unsolved homicide deprived him of the opportunity to bring a wrongful death suit against the murderer. Over the defendants' strenuous objections, the court found that the plaintiff was entitled to pursue the production of certain text messages sent or received by specific City officials during relevant time frames. Because the discoverability of the text messages necessarily turned upon their content, the court specified a detailed protocol for their review and production.

The *Flagg* opinion ordered the defendants to supply their service provider with the "PIN" numbers corresponding to the text messaging devices used by the City officials who sent or received the messages in question, thus allowing the service provider to willingly produce the text messages to the court under seal for *in camera* review. Two magistrate judges would then review the text messages and make initial determinations as to their discoverability, after which the parties would have the opportunity to present their objections. Finally, the court ordered, any text messages ultimately determined to be discoverable by the plaintiff would be produced subject to a strict protective order.

Although lawyers for several of the individually named defendants, including the Mayor of Detroit and his former chief of staff Christine Beatty, have filed motions arguing that the SCA bars the disclosure of these text messages to the plaintiff, the application of the SCA is dubious at best where the subscriber is the City Council of Detroit, not the particular individuals who used the devices. However, even if the *Flagg* Court reverses itself in light of the *Quon* decision, finding that the SCA prevents the plaintiff from obtaining the text messages directly from the City's service provider, the court retains the authority to compel the parties to the text messages to produce them in accordance with normal discovery procedures.

As the differences between the *Quon* and *Flagg* decisions reveal, the discoverability of text messages in civil litigation remains a nuanced issue and an open question. As Judge Wardlaw recognized in *Quon*, "The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier...that has been little explored."

The Smoking Voicemail: Applying E-Discovery Best Practices To Evidence Stored By Voicemail

By Richard H. Tilghman

Imagine the following scenario:

You represent XYZ Corporation in a patent case where your client seeks lost profits from the defendant's use of a computer chip that infringes on your client's patent. The week before your damages report is due, you get the following voicemail from your damages expert: "Good morning, this is Mary Anne Smith calling about my damages report. In working on my report, I realized that we don't have any evidence about XYZ's manufacturing capacity to make the 50,000 computer chips we're claiming as our lost profits baseline. When I spoke to XYZ's operations manager, he was skeptical that they could have made 50,000. Since this seems like a tricky issue, in my report I am going to assume that XYZ could have made 50,000 chips. I'm guessing you'll have someone from the company testify on manufacturing capacity since I haven't seen any evidence on the issue."

Your general practice with voicemails is to simply hit the delete button at the end of the message and jot down a note about the message, if necessary. Can you do that with this message? The answer is "no." If requested, such a voicemail is relevant and discoverable evidence. If the voicemail doesn't lead to a prompt settlement, it is also likely to be admitted at trial.

Although case law on the discoverability of voicemail is sparse, there is no logical reason that voicemail should be treated differently than other forms of data. Although often overlooked as a form of discoverable evidence, voicemail can be quite powerful evidence since it is more colorful than words written on a page. As companies continue to integrate their voicemail and e-mail systems to allow voicemails to be automatically forwarded to an employee's inbox, voicemails are likely to begin playing an even bigger role in litigation.

Therefore, there are several important points to keep in mind when managing voicemail:

- ◆ Counsel should remind employees, experts, and other potential witnesses that voicemail is as discoverable as other forms of electronic communication.

- ◆ Companies should include voicemail files in their document retention policy and adhere to that policy until litigation is anticipated.
- ◆ Once litigation is anticipated, a hold order should be put in place that suspends destruction of any potential evidence, including voicemails.
- ◆ When searching files for “documents” responsive to the opposing party’s request, employees should be instructed to search their voicemail files.
- ◆ Finally, counsel should be mindful that voicemails can contain extremely powerful evidence and pursue it aggressively in litigation where the opposing party’s voicemails may contain relevant information.

In short, the best practices for managing and pursuing electronic data apply equally to voicemail. Therefore, as with other forms of electronically stored information, it is important to establish a consistent policy for managing voicemail.

¹Under Federal Rule of Civil Procedure 34, the definition of “electronically stored information” includes “sound recordings.”

Instant Messages-Discoverable and Dangerous: How the Law Treats IMs And What Companies Can and Should Do

By James M. Carlson

Companies have long known about the perils of instant messaging. In the past, however, institutions have assumed that such problems were limited to distracting their employees. Now, companies need to address whether or not Instant Messages (“IMs”) constitute documents that must be produced during litigation. Indeed, courts are beginning to rule that IMs are just as discoverable as any other type of in-office communication. The legal trend is that IMs are discoverable, and in fact, they must be produced by a party to litigation. Moreover, companies may need to preserve IMs prior to initiating a lawsuit that involves the subject matter of the IMs. As a result, companies must maintain clear guidelines about instant messaging, not just to protect the productivity of the employees, but to ensure that a company does not destroy documents

relevant to a lawsuit. The result of such destruction may mean negative court rulings, sanctions, or even judgments against the offending party.

Courts Will Likely Treat IMs Like Any Other Type of Communication or Document—Especially if the IM Has Been Saved

The 2006 amendment to the Federal Rules of Civil Procedure explicitly included “electronically stored information” within the groups of documents that parties need to disclose, and produce, throughout the litigation process. Nevertheless, parties have attempted to argue that IMs should not be produced during litigation and are not covered by the Federal Rules. The argument is that IMs are a somewhat unique piece of digital information and that they are difficult to capture, save, and produce in a manageable form. Courts have largely dismissed this argument. This is particularly true if the IM is somehow saved electronically—whether in the IM program or via a word processing application. In fact, Courts will typically treat IMs just as they would any other category of document—whether it be a paper document or an electronically stored document.

For example, the Federal District Court in Maryland has explicitly ruled that “e-mail messages and similar forms of electronic communications” do not require a new body of law to be dealt with by court. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007). Therefore, IMs, and in fact other types of electronic communications, must be dealt with in the same fashion as other evidence. *Id.* In fact, at least one court has allowed the expedited discovery of IMs including the use of a computer forensic expert to preserve IMs before they could be lost. See *Quotient, Inc. v. Toon*, 2005 WL 4006493 (Md. Cir. Ct. 2005).

IMs Can Be Saved and Recovered

Companies should not assume that IMs are simply real-time conversations that are lost once they are over. This is incorrect. They can be saved and they can be retained. First, there are numerous pieces of software that can record IM conversations. Second, the users participating in the IM conversation have the option of saving the IM locally or “cutting and pasting” the entire conversation into a word processing file to be saved later.

Companies sometimes assume that IMs are based upon “casual” and anonymous Internet contact and are

therefore not discoverable. This is also incorrect. There is no “anonymous immunity” just because someone has chosen an “alias” on the Internet. Courts have found that Internet users who choose to violate the law by transmitting harassing or defamatory communications waive any right to conceal their identity and avoid punishment or liability for their actionable conduct. See *Polito v. AOL Time Warner, Inc.*, 2004 WL 3768897 (Pa. Com.Pl.,2004).

What Must A Company Do to Protect Itself?

Knowing that IMs are very likely discoverable, companies need to be in the position to act accordingly and protect themselves. Interestingly, companies in the financial services industry are governed by the Securities and Exchange Commission (SEC) and the National Association of Securities Dealers (NASD), and therefore, they must retain all IM conversations for at least three years. See NASD Notice to Members 03-33. Not all companies are so strictly regulated, and as a result, a company gets to make many of the decisions about IM retention policies on their own. These decisions need to be made sooner rather than later given the growing presence of IMs in the work place. A company should consider the following:

- ◆ **Consider Blocking IMs:** Should a company even allow IMs in the first place? Perhaps. It may make sense for a company to block all access to IMs whatsoever. This includes noting the company’s anti-IM policy within its employee handbook and even installing programs that specifically block IMs. Completely blocking all IMs, however, is becoming more and more difficult as there are numerous web-based applications for IMs – such as Meebo.
- ◆ **A Company’s Digital Document Retention Policy (“DDRP”) Must Address IMs:** A company’s DDRP must address a retention time period and/or destruction policy for IMs. To leave this format out of the DDRP simply omits an important category of information and potential evidence.
- ◆ **Realize the Limitation of Policies:** Instant Messaging can be addictive, and despite a company’s best efforts you must anticipate that there will be breaks in the policy. The company must be prepared to deal with outliers.

- ◆ **Allow Business Related IMs:** In many cases, companies use IMs as a productive communication tool in promoting business. In those cases, the company should try to standardize and regulate such IMs. Primarily, those IMs related to business should be stored, retained for an agreed upon time period, and then promptly destroyed.
- ◆ **Let Employees Know That Big Brother Is Watching:** Finally, it is important to inform your employees that their IMs may be reviewed and recorded. As such, employees may be “induced” to avoid using IMs for non-work conversations while at work.

You Don’t Know What You’ve Got ‘Til It’s Gone...The Discovery of “Deleted” Electronic Data

By Jessica K. Thomas

As advanced computer systems become more readily available to the average user, litigation attorneys find themselves needing to become more familiar with ways of recovering electronic data from these systems. When developing an electronic discovery plan, one of the key questions to ask is how to search for and recover purportedly “deleted” data.

Many times, information that a user has marked as “deleted” can still be obtained through a variety of approaches. For example, the information may still exist on the company’s network, copies may have been captured on back-up tapes, and fragments may exist on the hard drive. While every litigation attorney is perennially in search of the elusive “smoking gun” of the case, the search for deleted data will also uncover a plethora of far less important data. E-mails, drafts of documents, and dated materials are a fraction of the irrelevant data deleted from the user’s system. So how can attorneys effectively differentiate searches for the useful and the useless?

First, immediately request that all document destruction activity be halted and that all electronic data be preserved, including the mirroring of hard drives and laptops. Many times the issue of searching for deleted data does not arise until mid-way through the discovery process and valuable information may have already been

lost. If you have taken these steps at the outset of the litigation, you can ensure that the framework is in place for a computer forensic expert to search for any deleted data, should the need arise.

Second, determine what it is that you are searching for among the deleted data. The easiest way to unnecessarily escalate costs is to embark on a frolic detour into a vast and unfamiliar computer network. Moreover, the more limited and specific your request is, the more likely it is to survive a challenge in court on a motion to compel. Search limitations based upon network users, certain laptops, specific time frames and types of documents may all be utilized to narrow the search for deleted data.

Third, evaluate the economics of the case. Is this a case where damages are limited to a specific amount with a tight litigation budget? Or is this a case where a consequential damages limitation may be thrown out due to fraud? This should be weighed against the likelihood of the existence of key data having been deleted or destroyed. Depending upon the potential damages recoverable, the retention of a qualified computer forensic analyst may be necessary.

Fourth, employ a reputable computer forensic analyst. Obviously, any expert retained is an additional litigation cost to be carefully controlled. However, most reputable experts will assist you in the most cost effective ways to find the information you believe has been deleted while taking the appropriate steps so that chain of custody concerns are eliminated.

As the average user's knowledge and understanding advances regarding the discovery of electronic data, attorneys must continue to familiarize themselves with

ways of recovering potentially deleted information. By following the guidelines set forth above, attorneys will best serve their clients and maintain the integrity of the legal system.

Welcome

We would like to welcome Tina Solis as the new Co-Leader of the Ungaretti & Harris E-Discovery team, a role she will share with Jim Carlson. Tina is a Partner who concentrates her practice in Commercial Litigation and has extensive experience with E-Discovery. She has extensive experience in a wide array of business disputes, including contract actions, business breakups, law firm dissolutions, shareholder remedies, commercial fraud, trade secret litigation, unfair competition, business torts, and employment defense.

Ms. Solis has handled numerous cases involving various electronic discovery issues. She has also recently been named among the 2008 Illinois Super Lawyers' "Rising Stars" in business litigation by *Law & Politics* and *Chicago Magazine*.

In Our Next Issue:

- ◆ **Information for handling ESI right before trial and other issues.**
- ◆ **A new feature: *Tech Corner: Helping you better understand the technology around you.***
- ◆ ***We welcome your feedback. please feel free to contact Jim Carlson at jmcarlson@uhlaw.com***

For further information on the E-Discovery and Document Management Group or this update, please contact one of our members:

James M. Carlson	312.977.4143	jcarlson@uhlaw.com
Tina B. Solis	312.977.4482	tbsolis@uhlaw.com
Jessica K. Thomas	312.977.4498	jkthomas@uhlaw.com
Kamau A. Coar	312.977.4343	kacoar@uhlaw.com
Steffany L. Hreno	312.977.4347	slhreno@uhlaw.com
Richard H. Tilghman	312.977.4881	rhtilghman@uhlaw.com
Heidi Goldwater	312-977-9215	hgoldwater@uhlaw.com

This **E-Discovery Update** has been prepared by Ungaretti & Harris LLP solely for informational purposes and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon this information without seeking professional counsel.

© Copyright 2008 UNGARETTI & HARRIS LLP

www.uhlaw.com