

Ungaretti & Harris LLP
E-Discovery Update

**Monitoring Electronic Information
Stored in Text Messages**

by Richard H. Tilghman IV

Many companies have formal written policies allowing the monitoring of information sent via the company's network. A recent case from the Ninth Circuit Court of Appeals highlights the importance of strictly enforcing such policies.

In *Quon v. Arch Wireless Operating Company, Inc.*, the plaintiff alleged that his employer, the City of Ontario Police Department, violated his Fourth Amendment rights in searching his text messages without consent. The department had a written policy providing that use of its computer networks and associated equipment was limited to City business. The policy also provided that Internet and network activity could be monitored without notice and that network users should have "no expectation of privacy in using these resources."

Despite this policy, the department did not monitor text messages unless employees went over a monthly limit on the amount of characters allotted to each employee. When an employee exceeded his or her monthly allotment, the department's practice was to require the employee to pay for the overage charges, but the department did not

review the messages to determine whether they were business-related.

The Court reversed a jury verdict in favor of the defendants, holding that department employees had a reasonable expectation of privacy in their text messages, and that the department's search of text messages was unreasonable. The Court's decision was based, in part, on the fact that the department did not strictly enforce its policy of monitoring electronic communications to ensure that text messages were business-related. The Court looked behind the department's written policy to the "operational reality" of the department's practices, finding that the department had not enforced a policy of reviewing employee's text messages to ensure that the messages were business-related.

While the *Quon* case deals with Fourth Amendment issues that may not be applicable to most non-public businesses, it underscores the importance of enforcing policies regarding use of company networks. As the City of Ontario learned the hard way, the failure to strictly enforce a policy can lead to adverse consequences, as courts often look to the "operational reality" of an organization's policy to determine the policy's true scope.

**Limiting Discovery Requests
in Order to Reduce Costs**

by Emily M. Dierberg

In pursuing the production of documents during litigation, parties sometimes choose to submit excessive, overly broad document requests instead of sending well reasoned and appropriately tailored requests. This was important when documents were exchanged only in paper form. But now, the Federal Rules explicitly include the production of "electronically stored information."¹ Now, overly broad document requests result in the production of vast arrays of data including terabytes of emails, metadata, native file format documents, backup tapes, voice mails and information stored on PDAs. The costs in producing such documents can be excessive. But there is also a risk in merely asking for that much material. A party may be forced to produce the exact same kind of documents or the court may even shift additional costs to a requesting party. Thus, certain situations do not justify the sometimes overreaching requests for ESI.

Contents

Monitoring Electronic Information Stored in Text Messages
by Richard H. Tilghman IV

Limiting Discovery Requests in Order to Reduce Costs
by Emily M. Dierberg

Tag It and Bag It –
Key Principles to Consider When Drafting a DDRP
by Tina B. Solis

Who Picks up the Check for E-Discovery?
Cost-Shifting and Why It's Important
by James M. Carlson

Tech Corner –
Limitations on In-House Collection of Data
by Heidi Goldwater

Federal Rule 26 provides protection from unduly burdensome or expensive e-discovery requests.² A court may deny a discovery request or require a requesting party to pay expenses if the burden or expense of the proposed discovery outweighs any likely benefits, or if the request is not sufficiently tailored in scope. Further, a court may impose a sanction on an attorney or party violating Rule 26(g)(1).³

To reduce costs and comply with the discovery rules, practitioners and parties must therefore tailor and make specific their e-discovery requests. Requests for ESI must include specific date and subject matter limitations. This narrows the quantity of discovery for the producing party and provides parameters for the producing party in conducting effective searches for relevant documents. Counsel should also be able to justify the relevance and materiality for each request.

Sometimes just attempting to work with opposing counsel can result in reduced costs. In fact, the Sedona Conference Cooperation Proclamation (July 2008)⁴ advocates cooperation among parties as a way of reducing the costs of litigation. Also, in *Mancia v. Mayflower Textile Servs. Co.*,⁵ to make discovery costs proportional to what is at stake in the litigation, a Federal Court Judge ordered parties to meet and confer prior to discovery to:

- Estimate the likely range of provable damages and fees that could be awarded at trial, and based on that range, attempt to quantify a workable discovery budget.
- Discuss the quantity and type of discovery already provided and the additional discovery still sought in order to determine whether plaintiffs' legitimate discovery needs could be fulfilled in a less burdensome and duplicative manner.
- Attempt to agree about what additional discovery should be provided.

In sum, the abundance of electronic information makes pre-litigation discovery planning more important than ever before. Following these simple steps and narrowing your e-discovery requests will reduce costs, provide a more efficient discovery process, and eliminate any threat of sanction or cost-shifting.

¹ Fed. R. Civ. P. 34(a)(1)(A).

² A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. Fed. R. Civ. P. 26(b)(2)(B). Further, every discovery request must be signed by at least one attorney of record and by signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry, the request is consistent with the rules of procedure and warranted by existing law, not interposed for any improper purpose (such as to needlessly increase the cost of litigation) and is neither

unreasonable nor unduly burdensome or expensive. Fed. R. Civ. P. 26(g)(1).

³ If a certification violates this rule without substantial justification, the court must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both. This sanction may include an order to pay the reasonable expenses, including attorney's fees. Fed. R. Civ. P. 26(g)(3).

⁴ See www.thesedonaconference.org.

⁵ No. 1:08-cv-00273-CCB, 2008 WL 4595275 (D. Md. Oct. 15, 2008).

Tag It and Bag It – Key Principles to Consider When Drafting a DDRP

by Tina B. Solis

Many companies are extremely concerned about retaining every single document in today's electronic age. Courts, however, typically do not sanction a company for failing to produce documents that no longer exist because they were destroyed pursuant to a digital document retention policy ("DDRP"). Rather, courts have sanctioned companies for failing to produce documents in their possession that are responsive to the litigation. In these challenging economic times, companies must keep in mind for every document retained, a company's cost increases in terms of time and resources should litigation ensue. If done correctly, a company can eliminate these "legacy" documents, save space and storage costs, and maintain proper document retention.

In order to strike a balance between controlling costs and having an effective DDRP, a company should categorize its various documents—or tag them—and after considering the three principles set forth below and determining that none of them apply, destroy them—or bag them—pursuant to the company's DDRP.

Principle One: Make Sure the Documents Can Be Destroyed

Before proceeding with the destruction of electronic documents, a company should first determine if they can be destroyed. Are the documents subject to any statute requiring them to be kept for a certain period of time? For example, a public company must keep its financial records for a requisite amount of time. If any of your company's documents are subject to any statutory requirement, this should be discussed with outside counsel and explicitly set forth in the DDRP to ensure compliance.

Principle Two: Make Sure There is No Business Need for the Documents

Are there any business needs for these documents? For example, often times there are certain categories of documents that a company's employees routinely need to retrieve. In those situations, the applicable categories of documents should be set forth along with the retention

period for each type of document. For those documents with no business significance, they should be routinely destroyed in a short amount of time pursuant to the company's DDRP.

Principle Three: Protect Against Destroying Documents During Litigation

Is there pending or reasonably foreseeable litigation? If litigation is threatened or pending, a litigation hold must be enacted, as it should be set forth in the policy, to stop the destruction of all responsive documents.

If none of the three principles stated above apply, a company's DDRP should provide for the routine and regular destruction of those documents. Such a policy will keep a company's costs in check should litigation begin. If destruction of older ESI is accomplished with the assistance of an uniformly implemented DDRP, then a company can save costs and still protect its documents.

Who Picks up the Check for E-Discovery? Cost-Shifting and Why It's Important

by James M. Carlson

One of the major problems with requesting and producing electronic data is the inherent costs in handling the information. Vendors can charge significant amounts to search, collect, and ultimately produce electronically stored information. There may be additional costs just to allow for review of the information. While these costs can be prohibitive, they rarely outweigh the value of the information. But requesting parties must understand that they may have to pay for the information they request for production. Knowing and understanding these risks can prevent parties from being stuck with a large discovery bill. This article addresses the process of "cost-shifting" or when the costs of requesting electronic discovery are incurred by the requesting party.

In federal courts, the party responding to discovery requests typically incurs the expense of collecting documents.¹ However, a responding party can move the court for an order protecting it from undue burden or excessive expense. In doing so, a party requests the court to "shift the costs to the non-producing party."² Cost-shifting is of particular concern when a party is requesting that the opposition produce a vast sea of electronic data. In deciding whether or not to "shift costs," courts look at the following factors:³

1. *The likelihood of discovering critical information.* Here, courts will tend to discourage cost-shifting if it is very likely that the information sought is critical and likely to be discovered.
2. *The availability of such information from other sources.* If a party can recover the data from other information rather than forcing the opposition to spend to produce the information, then cost-shifting is more likely.
3. *The amount in controversy as compared to the total cost of production.* Courts will not respond well to a costly discovery production that will cost more than the amount at issue in a lawsuit. In such a situation, a court will likely shift costs to the requesting party or strike such discovery requests in their entirety.
4. *The parties' resources, as compared to the total cost of production.* Courts are very sensitive to a "small fry" party being harassed with costly and burdensome requests. Here, a large company who can more easily carry the burden of cost may likely have to handle more of the costs.
5. *The relative ability of each party to control costs.* This factor addresses what resources are available to each party as well as which prospective vendors may be available to each party. The party who can more easily navigate production may be faced with paying for more of the costs.
6. *The importance of the issues at stake in the litigation.* For this factor, a court will decide whether or not there is an overwhelming public policy factor that would encourage production of the information.
7. *The importance of the requested discovery in resolving the issues in the litigation.* Here, the court will determine whether or not the data at issue is actually the "smoking gun" or merely a supplement to discovery. The more important the discovery is the more likely a court will force the production of the data regardless of cost.
8. *The relative benefits to the parties of obtaining the information.* This factor focuses on which party will benefit most from the production. Almost always the requesting party is more likely to benefit. However, if the information may also aid the producing party, then it may be more than fair to require the producing party to also assist in paying for the discovery.

Before blindly requesting every last byte of data from the opposition, a requesting party should review the above eight factors and decide whether or not they themselves may end up paying for such broad-reaching discovery.

¹ *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978).

² Fed. R. Civ. 26(c); *Oppenheimer Fund, Inc.*, 437 U.S. at 358.

³ *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 284 (S.D.N.Y. 2003); *Wiginton v. CB Richard Ellis, Inc.*, 229 F.R.D. 568 (N.D. Ill.)

Tech Corner – Limitations on In-House Collection of Data

by Heidi Goldwater

Have you been served with a discovery request for litigation? Are you wondering how to handle the collection and production of the requested documents? Should you use your in-house IT personnel for the collection of data? There are many reasons, why your own IT staff by themselves may not be the best option. However, having your IT personnel work with discovery professionals and counsel is a recipe for success.

Why Your IT Personnel Can Help

First, no one knows the current infrastructure and design of a network more than the people who actually set it up and manage it daily. These same people, while not usually well versed on electronic data collection protocols and the court’s evidentiary requirements, are helpful because:

- They know the systems;
- They understand where the data is hiding and who to go to in order to find the data; and
- They understand how to work with a company’s decision makers.

As helpful as those characteristics are, there are other points where in-house IT personnel can be lacking. First, they may not understand the crucial importance of documenting the collection and chain of custody for the data. Such documentation is absolutely crucial in order to use the data as evidence at trial. Second, the proper production of data requires precise knowledge of how the searches are to be executed. This may require an agreement from counsel on what the key search terms for collection are and what are the deadlines for the production. In-house IT personnel may not be well versed in understanding how to complete those tasks. Finally, whomever is collecting the data needs to find out the format in which data will be produced. This means

understanding any agreed upon native file system. Again, in-house IT personnel may not be up to speed on these issues.

Even simple collection issues can be difficult for in-house IT personnel. Most corporations simply do not have the tools to process ESI. They need to work with an outside vendor to process the data and cull it down to just the responsive documents, all while meeting the specific demands and deadlines of the discovery request. This is not something that would usually fall under the IT umbrella.

When In-House Limitations Become Dangerous

If an employee leaves a company or is terminated, you may think that having your IT personnel search the former employee’s computer is a good idea. It may not be. Your IT personnel may think it’s a good idea to poke around for data and key documents, but all they will actually do is alter the metadata of what is on the computer. If there is potential future litigation with the former employee, it is critical that you preserve their computer in the state it was in on the employee’s last day. Under these circumstances you would want to employ a reputable forensic vendor who can forensically image the machine.

The Right Solution

Using common sense and working with counsel, discovery experts and inside IT personnel would be the ideal situation. Often times, IT departments are not localized and discovery vendors may be hired to assist with collection and processing. Each situation is different and needs to be well thought out before the first megabyte of data is collected.

Please visit
www.uhlaw.com/about/contactus
to receive future editions of the
E-Discovery Update via email.

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

James M. Carlson, Editor	312.977.4143	jcarlson@uhlaw.com
Tina B. Solis	312.977.4482	tbsolis@uhlaw.com
Kamau A. Coar	312.977.4343	kacoar@uhlaw.com
Jessica K. Thomas	312.977.4498	jkthomas@uhlaw.com
Emily M. Dierberg	312.977.4122	emdierberg@uhlaw.com
Steffany L. Hreno	312.977.4347	slhreno@uhlaw.com
Nile N. Park	312.977.4125	npark@uhlaw.com
Richard H. Tilghman IV	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 2009 UNGARETTI & HARRIS LLP
www.uhlaw.com