

Capturing Quicksilver: Records Management for All That Other Stuff

Written by Sharon Nelson and
John Simek

Presenters:
Peg Duncan
Sharon Nelson

April 2-4, 2009
www.techshow.com

Have you caught the Twitter bug yet? If not, you can be assured that some within your company or law firm have indeed gotten the bug. And what are they saying, when sending their “tweets” via Twitter? Stupid stuff like “walking the dog” and “when did I get so darn fat?” But they are also saying “our competition is EVIL” and naming names. And “we’re working on a special R&D project that will rock the stock market, guaranteed.”

Do you have a “pish posh” reaction to Twitter? Maybe you should rethink that feeling, if you do.

Recent headlines:

From the *Washington Business Journal*: “How Tweet It Is”

From the *Wall Street Journal*: “Twitter Goes Mainstream”

From the *National Law Journal*: “Beware, Your ‘Tweet’ on Twitter Could Be Trouble”

Subheader: Latest networking craze carries many legal risks

And is a tweet done on company resources a “record” for purposes of retention requirement and, ESI preservation/production? Yes, absolutely.

If you find that scary, you’re not alone. For a while, record managers thought they had the universe pretty well covered with e-mail and company approved programs. After a while, some of them caught up with instant messages. But Twitter, unified messaging, VoIP, blogs, RSS feeds, etc. etc. have given almost everyone a Goliath-size headache.

Let’s start at the beginning, with some Wikipedia definitions. We’ll assume that most folks now know blogs, voicemail and instant messages, but other terms here may be new to some. Those of you who are well and truly wired can skip over these.

A **wiki** is a page or collection of Web pages designed to enable anyone who accesses it to contribute or modify content, using a simplified markup language. Wikis are often used to create collaborative websites and to power community websites. The collaborative encyclopedia Wikipedia is one of the best-known wikis. Wikis are used in business to provide intranet and Knowledge Management systems.

RSS is a family of Web feed formats used to publish frequently updated works—such as blog entries, news headlines, audio, and video—in a standardized format. An RSS document (which is called a “feed”, “web feed”-or “channel”) includes full or summarized text, plus metadata such as publishing dates and authorship. Web feeds benefit publishers by letting them syndicate content automatically. They benefit readers who want to subscribe to timely updates from favored websites or to aggregate feeds from many sites into one place. RSS feeds can be read using software called an “RSS reader”, “feed reader”, or “aggregator”, which can be web-based or desktop-based. A standardized XML file format allows the information to be published once and viewed by many different programs. The user subscribes to a feed by entering the feed’s URI (often referred to informally as a “URL”, although technically, those two terms are not exactly synonymous) into the reader or by clicking an RSS icon in a browser that initiates the subscription process. The RSS reader checks the user’s subscribed feeds regularly for new work, downloads any updates that it finds, and provides a user interface to monitor and read the feeds.

Unified Messaging (or **UM**) is the integration of different streams of communication (e-mail, SMS, Fax, voice, video, etc.) into a single unified message store, accessible from a variety of different devices. Unified messaging is a subset of a fully integrated Unified communications system.

While traditional communications systems delivered messages into several different types of stores—voicemail systems, e-mail servers, and stand-alone fax machines—with Unified Messaging all types of messages are stored in one system. Voicemail messages, for example, are delivered directly into your inbox. You see them right beside your e-mail when you open up Outlook, offering powerful new ways to collaborate more effectively. For example, you can forward a voicemail or fax. You can even take notes in your voicemail message or search for old voicemail messages.

Twitter is a free social networking and micro-blogging service that allows its users to send and read other users' updates (otherwise known as **tweets**), which are text-based posts of up to 140 characters in length.

Updates are displayed on the user's profile page and delivered to other users who have signed up to receive them. Senders can restrict delivery to those in their circle of friends (delivery to everyone being the default). Users can receive updates via the Twitter website, SMS, RSS, or email, or through an application such as Tweetie, Twinkle, TwitterFon, Twiterrific, Feedalizr, and Facebook.

Second Life (abbreviated as **SL**) is a virtual world developed by Linden Lab that launched on June 23, 2003 and is accessible via the Internet. A free client program called the Second Life Viewer enables its users, called Residents, to interact with each other through avatars. Residents can explore, meet other residents, socialize, participate in individual and group activities, and create and trade virtual property and services with one another, or travel throughout the world, which residents refer to as the grid. Second Life caters for users aged over eighteen, while its sister site Teen Second Life is restricted to users aged between thirteen and eighteen.

So how do Records Managers deal with this constantly evolving world?

New technology bedevils RM. Worse yet, the minute RM catches up to technology, technology leapfrogs ahead with something else to cause consternation. Now that we have the definitions under our belt, let's look more closely at these new technologies . . .

Back to Twitter:

Douglas Winter, who heads the electronic discovery unit at Bryan Cave, stresses that tweets are no different from letters, e-mail or text messages – they can be damaging and discoverable, which is especially problematic for companies that are required to preserve electronic records, such as the securities industry and federal contractors. Yet another compliance headache is born.

Tom Mighell of Fios suggests that we may find a post from a proud employee that says “To you naysayers, our disc brakes are fine. I’m an engineer on that product. We went to 5X tolerance on the label, so you can be rougher on them than you think. Don’t worry.” As Tom points out, after that post, “you’ve got potential product liability in 140 characters.”

Nolan Goldberg, of Proskauer Rose, has noted that you can get yourself in a lot of trouble in Twitter’s 140 word limit. Many folks don’t realize that “tweets” (Twitter postings) create a permanent record and that the tweets can go anywhere. Add to that the fact that, like IMs and e-mails, these quick electronic messages are often composed when someone is angry or frustrated – sometimes leading them to display poor judgment. Though Twitter does not release the number of folks registered to use it, industry experts report that 3.4 million unique visitors visit Twitter each month – and that number is growing exponentially.

Twitter is by no means alone. There is also Yammer, and present.ly – and surely many more to come. Enterprise versions are just beginning to emerge, but there is currently precious little policy to govern them. For the most part, microblogs are being treated as blogs from a corporate policy perspective.

Blogs

As blogs have exploded in popularity over the last few years, so have cases in which employees have disclosed trade secrets and insider trading information on their blogs. Blogs have also led to wrongful termination and harassment suits.

Just how many bloggers are there in the U.S.? According to Technorati (<http://technorati.com/blogging/state-of-the-blogsphere/>), there are more than 22 million bloggers in the country. More than 12% of the populations blogs. According to *Fortune* magazine, 12% of the Fortune 500 are blogging. Not everyone has something worth saying, but they are saying it prolifically all the same.

There should, of course, be a company policy about blogging at work or about work. Many companies sanction blogs – Microsoft has hundreds of them. A recent case has suggested that employers may have the right to prevent employees from accessing blogs while at work, which may fend off some of the dangers associated with blogging. *Nickolas v. Fletcher*, 2007 U.S. Dist. LEXIS 23843 (E.D. Ky. Mar. 30, 2007).

If blogs are allowed at work, the company needs to maintain blog archives where retention is mandated under laws or regulations. Blogs do indeed create a paper trail, for better or worse. Corporate blogging vs. individual employee blogging present different challenges – one clearly speaks for the corporation. The other may or may not, depending on the circumstances.

One notable recent case, from October of 2008: at the Transportation Security Administration’s official blog, a former officer blogged about a Newark officer arrested for stealing from passenger’s luggage, assuring readers that TSA has zero tolerance for theft and citing the number of officers terminated for theft. This was followed by probing comments from blog visitors

disputing the number of officers terminated and asking for hard data about compensation for victims. Not necessarily welcome comments for TSA. Blogs, clearly, can be a Pandora's box.

Enterprise blogs require security and authentication and audit trails. Likewise, it should be possible to search them, issue reports, etc. Control over enterprise blogs can be appliance based, an enterprise application or though software as a service (SaaS). As the example above shows, an enterprise will certainly want to consider whether to allow comments!

Audit trails should capture all changes, including new posts, changed or deleted posits, and comments and discussion. They should capture context, including who posted/commented, what posts are read and what posts are trackbacked.

One wit has suggested a very simple corporate blog policy: "Don't be stupid."

Wikis

Let's examine the granddaddy of wikis, Wikipedia. It has received such stature that a search for it on LEXIS brings up more than 130 results. Wikis are now commonly used in companies, particularly in team efforts so that team members can collaborate in one space. But who is monitoring wiki activity or treating postings as records? We have only anecdotal evidence thus far, but the answer seems to be "not many."

Jesse Wilkins, from Access Sciences Corporations, says wikis are used for documentation, knowledge bases, project management, meeting management, research analysis, event planning, as a corporate directory and as an encyclopedia.

Critical to management of wikis is the ability to audit, to capture all changes, additions, corrections and deletions. Reports can also be issued to determined who has made what changes, among many other things. Wikis are now often accessible by phone, creating another set of headaches as potential evidence may exist on phones. Wikis, by their nature, are often unwieldy and subject to uncontrolled growth and minimal pruning.

Some well known enterprise wiki vendors include Atlassian Confluence, Brainkeeper, eTouch SamePage, Socialtext Enterprise Wiki, Traction TeamPage and Twiki.

Social Networks

The lifeblood of many employees is their social networks, including MySpace, Facebook, Linked In and Plaxo. Besides being a gigantic 'time suck,' these sites abound with risks for business as most businesses do not monitor their employees' sites and therefore all the risks associated with blogs apply here. Many experts believe that companies are well advised to use filters to block access to all social networking sites at work. At the very least, this action will keep the posts from being company records. On the other hand, genuine business usage of these sites has grown tremendously and it may be very difficult to allow business usage and forbid personal usage, no matter what a company's policy may say.

A 2008 independent survey commissioned by FaceTime Communications (based in the U.K. but we have no reason to suspect the answers would be much different here) found that roughly 80 percent of employees use social networks at work – and for BOTH personal and business reasons. The work-related purposes were for professional networking, researching and learning about colleagues.

As may be obvious, checking the social networking sites of potential employees may be wise, as an employer may get some sense of trouble brewing in the future, a lack of discretion, angry entries, a TMI (too much information) proclivity, etc.

Is employer monitoring of social networking sites really happening in the wild? The authors did an ad hoc online survey – though everyone said an employer had a right to monitor, no one actually knew of an employer who WAS monitoring personal sites. Likewise, others in the field have not yet been able to cite a case where social networking was involved to the detriment of the employer, but the consensus is clear – just wait a bit – it’s coming.

Instant Messaging

The devil is in the details. Some IM packages record the IMs – others do not. AOL, for instance, has an enterprise-wide IM program, which can be set up for compliance purposes to retain the messages. But there is also an AOL IM program that individuals can download (if the company has not employed technology to prevent this) and send/received IMs that will be recorded only on the employee’s local hard drive. And there are IM packages that don’t record anywhere at all. Untangling the variants of IM is a nightmare. And let us assure you that an employee who wants to do something bad will assuredly use web-based e-mail and web-based IMs. This is usually how company data leaks to the outside world, especially to competitors.

A recent survey by the American Management Association says that 50 percent of workers have downloaded and are using free IM tools. The vast majority of these users are not “controlled” by the enterprise at all – in fact, only 31% of the companies have IM policies (never mind actual controls!) in place.

It is not as easy to control IMs as you might think. While employers can prevent employees from installing unauthorized software to their computers, most commercial providers offer web-based access to their IM networks meaning that there is nothing to install and nothing to block – short of blocking the entire domain. Some IT administrators will try to block the ports IM clients use to send traffic, but alas, even this doesn’t work well anymore, because many of the IM clients are “port-seekers,” which will keep trying ports until they find an open one. Even more wily, some of them will use the default port for accessing the web so that the traffic looks like web surfing rather than IM. It’s enough to make management cry. It is of course difficult to lock down the laptops of the road warriors. And smart phones today support the IM networks – yet another avenue to block.

An effective IM policy should dictate whether IMs are to be used for business only, personal use only, or some combination of both. It should specify whether attachments can be sent and any limitations. Are internal communications only allowed? Or communications with the outside

world? If IMs need to be archived, the policy should specify the procedures. Jesse Wilkins, a principal consultant with Access Sciences Corp., A RIM consulting firm, has the following to say about the tools and technologies to assist in managing instant messaging:

“These broadly fall into two approaches: gateways and enterprise IM (EIM). Gateway applications and appliances offer much of the functionality that is missing from traditional commercial networks but is required for effective management of IM traffic and communications. Gateways also provide some ability for users to communicate across networks, with support for several of the most common commercial networks.

EIM solutions take a different approach, replacing the commercial networks with a single enterprise-wide client. This allows for more granular control over what functionality users have and how policies are enforced. EIM administrators can pre-populate users’ “buddy lists” up to the inclusion of the entire corporate directory. And EIM solutions also provide secure encrypted communications, a key security issue for organizations concerned about sensitive communications.

Both gateways and EIM solutions include centralized archiving of supported networks’ traffic; attachment filtering and virus scanning; controls on content transmission and on which users and groups can exchange information; enforcement of user-naming policies and identity management; and the ability to prevent internal users from communicating to external ones. Gateways and EIM solutions can also be used together to provide the best features of both solutions.”

According to experts, the vast majority of businesses are utilizing IMs. To comply with the basic requirements of Sarbanes-Oxley (SOX), instant messages must be integrated into records management. SOX section 404 requires an annual evaluation of internal controls and procedures for financial reporting, as well as an assessment for the effectiveness of the control. If IMs are involved, they must be logged, archived and available upon request.

The National Association of Securities Dealers (NASD) demands that IM communication must be either managed and maintained according to its 3010 and 3110 rules, or not allowed at all. Rule 3010 says that companies must supervise the communications between staff and the public and ensure compliance with company-defined policies. Organizations must sample IMs and have the capacity to quarantine incoming and outgoing messages, recording and logging the samples. The New York Stock Exchange issued its own memo, citing instant messaging as a medium that must be monitored for compliance.

NASD members must treat an instant message as an e-mail or written record for retention purposes. Both NASD and SOX section 802 require tamper-proof records for all electronic communications, including instant messages. Electronic storage media must preserve the records in non-rewritable, non-erasable format.

The Securities and Exchange Commission (SEC) requires companies to ensure specific retention periods and to be able to quickly search and retrieve selected archived information, including instant messages. Messages must be stored for a minimum of three years. Companies need to

retain records for the SEC's legally specified time or for the time outlined by industry-specific regulations. The SEC also requires that a duplicate copy of the records be stored separately from the originals in tamper-proof format. Commonly, data used to be transferred off-site, but more and more, data is transferred electronically to a remote location.

The Gramm-Leach-Bliley Act (GLB) includes provisions to protect consumer's personal financial information held by financial institutions. This includes the security of information communicated by IM and e-mail.

The Health Insurance Portability and Accountability Act (HIPAA) applies to all organizations that have access to patient information. HIPAA requires protection of patient confidential information and suggests that any oral, written or electronic communication be captured and stored, including instant messages.

Various data breach laws in the states require that any breach be reported (and there are corollary requirements as well) including breaches via e-mail or instant messaging.

Voicemail

Voicemail has been a relatively new phenomenon in ESI. When Federal Rule 34(a) was changed to specifically include sound recordings, it made clear that voicemails were subject to the same preservation and production requirements as other hard copy documents and ESI. In general, minus specific retention requirements by law or regulation, a company may determine how long to retain its voicemail. But if it exists, it is subject to preservation and production under the federal rules: note that in *Del Campo v. Kennedy*, 2006 WL 2586633 (N.D. Cal., Sept. 8, 2006) the court ordered the preservation of voice recordings until the parties developed and agreed upon a document preservation plan.

In 2006, Merck & Co., Inc. was ordered to preserve all voicemail related to the Vioxx litigation. Note that it was suggested that Merck might have used voicemail rather than e-mail in order not to leave a written trail. There certainly seems a high probability that this happens a lot in businesses, making the preservation of relevant voicemail even more critical in the event of actual or reasonably foreseen litigation. Merck claimed that its system couldn't preserve the e-mail without massive burden and expense. The judge was unmoved and ordered the preservation.

The problems presented by voicemail become even more complicated when unified messaging comes into play. Unified messaging can operate in more than one way. It may simply offer a notification to a user, who effectively "picks up" the voicemail from a central repository. But it can also dump the voicemail into e-mail as an attachment, which considerably complicates the process of retention and discovery. This increases the data volume and presents indexing difficulties which will make electronic discovery more challenging.

We have seen the argument made that searching through voicemails is too burdensome because voicemails must be transcribed. New technologies have solved that problem as they can convert voicemail to text for review. See the next section on VoIP for further information.

Voice over Internet Protocol (VoIP)

VoIP offers a lot to business, in reduced costs and efficiencies. There are no phone lines and no phone taxes. However, it comes at a price, facing an increased risk of security and hacking threats. Many records management policies overlook VoIP's very existence. As a general rule, where policies exist, the retention time period for voice messages is less than that of written messages.

When VoIP messages are stored using unified messaging, a caller's voicemail is generally stored as a .wav file in the recipient's e-mail. However, once deleted, it is often stored on a backup server, along with deleted e-mail messages. Before VoIP, voicemail messages resided on the phone company's server or directly on the recipient's phone as a local recording on a magnetic tape. In one case, the phone company determined how long the message was retained. With respect to magnetic tape, the user would listen to the recording and then delete, with new messages overwriting the deleted messages. VoIP voicemail is really a lot more like e-mail than traditional voicemail.

VoIP systems can be configured to simultaneously record and store messages. The manner in which this data is retained is usually under the direct control of the company. Often, redundant backup systems mean that copies of the messages may be found in several places. Though VoIP specific court decisions do not yet exist, it is very likely that the decisions regarding recording phone messages from the previous era will control – in which case, parties may be found guilty of spoliation for failure to preserve recorded conversations, as happened in *E*Trade Secs. LLC v. Deutsche Bank*, AG2005 U.S. Dist. LEXIS 3021 (D.Minn. 2005).

How to review and produce? Ah, there's the rub. And what of the constant argument that reviewing any kind of recording is over-burdensome? The old way of reviewing was to hire cheap labor to transcribe the recordings. However, there is now speech to text software, using advanced speech-recognition technology.

An even greater improvement is phoneme software, using the smallest components of spoken language. English uses only 42 phonemes. Much faster than speech to text software, this software can do an hour's worth of human listening in about one minute. One caution however – the accuracy rate is dependent on the quality of the source audio files.

It is important to determine where VoIP data will reside within the corporation's network. With the e-mail? Will it be backed up with other data? Treating VoIP data differently may have distinct advantages – namely, that the data can be erased sooner than other data unless there is a legal or business reason to retain it.

Text Messages

Text messages have been in the news a lot lately. President Barack Obama demanded, and received, a phone to replace his BlackBerry (model as yet not publicly disclosed, though the betting money is that it is a Sectera Edge, manufactured by General Dynamics from a repurposed Palm Treo 750) which allows him, among other things, to send encrypted text messages. Though

undoubtedly very secure, no phone is “unhackable” and it a sure bet that there are folks whose full time occupation will be to try to hack that particular phone.

In *Flagg v. City of Detroit*, **2008 WL 787061 (E.D. Mich. Mar. 20, 2008)** the court determined that text messages exchanged among officials of the City of Detroit via city-issued text messaging devices were discoverable under the standards of FRCP 26(b)(1). The holding certainly demonstrates the challenge of conducting e-discovery across information systems that inevitably blend personal information with business communications.

To make matters more complicated, a subsequent decision in this case, *Flagg v. City of Detroit*, **252 F.R.D. 346 (E.D. Mich. 2008)**, the court demonstrated reluctance to squarely face the issue of whether SkyTel’s disclosure of the text messages would violate the Stored Communications Act (though the court indicated that it probably would) and whether the court could nonetheless compel production. As an alternative, the court directed the Plaintiff to serve a Rule 34 Request for Production instead, the court’s authority being much more clear under that Rule.

In the end, Detroit Mayor Kwame Kilpatrick and his paramour (and chief of staff), Christine Beatty, were felled by steamy text messages.

In contrast to *Flagg*, in *Quon v. Arch Wireless Operating Company, Inc.* (9th Cir. 2008) the court held that an employer had no right to read employees’ pager text messages without their knowledge and consent. The court also held that a cell phone provider may not turn over the contents of the text messages to the employer under federal law. The case involved Jeff Quon, an officer in the Ontario County police department who exceeded the 25,000 character limit for text messaging. The department put employees on notice that their Internet and e-mail usage would be monitored, but did not notify the employees that their text messages would be viewed. The police chief requested a transcript of the text messages to determine whether the messages were used in relation to work, and the service provider sent the police department transcripts of the messages. Quon then sued for violation of his Fourth Amendment protection against unreasonable searches and seizures. The court considered many factors to reach its decision, including whether Quon knew his communications were not private and whether Quon had allowed the department to view his text messages. The court found that the service provider violated the Federal Stored Communications Act, which prohibits providers from giving up the contents of communications on its service. The court also found that Quon had a reasonable expectation of privacy (very important in this case that text messages were not regularly monitored and therefore that the expectation of privacy might have been created) and that viewing Quon’s text messages to determine whether the messaging was work related was not reasonable.

Clearly, there will be continuing decisions in this area before the landscape is clear as court attempt to balance privacy interests and the discoverability of business communications.

Toss or Keep?

From our viewpoint as folks involved in computer forensics, if you don't have to keep data and can't think of a reason why you should keep it, toss it. You'll save a fortune if you become embroiled in litigation. Shrinking the data to search will shrink the volume of responsive data that must be reviewed.

What about the laws? Complicated, very complicated. Federal agencies have it simpler than the rest of us – they are primarily governed by regulations of the National Archives and Records Administration (NARA), 44 U.S.C. Chapters 31 and 35, and the Office of Management and Budget (OMB) Circular A-130. But the private sector has a labyrinth of thousands of regulations and laws (more than 20,000!) mandating retention for specified periods.

Some of the emerging technologies are fluid (comments on blogs, ever-expanding discussions on wikis, changes on social networking sites, etc.). How do you manage something that isn't static and that has multiple authors? Snapshots are one method – and risk assessments are performed to determine how often snapshots must be taken. Training is helpful – employees need to understand that they are creating “records” when they use these technologies and think before they create records, bearing the risks of the records they create in mind.

Let's go back to risk assessment for a moment. NARA says agencies must determine whether the loss of content within these emerging applications may result in:

- Litigation
- Increased litigation risk
- Liability
- Impairment of program operations
- Inability to detect fraud, false statements or other illegal behavior
- To account for the stewardship of information or property

In the private sector, records managers will also be interested in protection of proprietary data, avoiding harassment or adverse workplace actions, steering clear of defamation or libel suits, etc.

Let us give you a great example of smart policy. If you constantly train employees in the proper and improper use of, say, instant messaging, and one rogue employee sends a sexually-charged IM, then you as the employer may have a defense against a sexual harassment claim. Now there's where an ounce of prevention is worth a pound of cure!

When to schedule archiving is highly variable. You certainly want to archive a wiki when its work is concluded, but how often along the way must you archive? Commonly, changes are archived daily or upon record creation. NARA suggests that “one efficient method of capturing the browser-readable content is to harvest it. In the case of wikis, blogs and portals that have been scheduled as permanent, harvesting is an effective capture mechanism. For RSS feeds, however, unless they can be harvested with the help of an “aggregator,” the content of a feed should be retrieved from a server as XML (with schema and style sheet) . . .”

As with all enterprise-wide records management program, it is critical to bring RM from “ad hoc to adherence to policy,” never an easy task, and harder still with these new quicksilver

technologies. This requires support from the top, communication, training, incentives and compliance monitoring.

The Web 2.0 World

It's a brave new world, and most corporations are having a heck of a time dealing with it. It can involve huge costs, business disruptions, public embarrassment and, gulp, legal liability. Management of Web 2.0 records is limited at best, often chaotic and duplicative. This is a huge challenge for record managers.

Even the National Institute of Health is using Twitter to share funding information. And how are they harvesting and preserving that data? We have no idea. The tech world moves so fast that once you're on top of it, it has already passed you by again.

The 2008 FaceTimes Communications survey referenced earlier found that only 31 percent of respondents store IM communications. Only 25% store audio conferences and 20% archive corporate Web conference.

If requested to produce IM communications for a lawsuit, 51% of IT managers say they could not do it. 38% say they have no such capability and 13% say they might be able to do it but not in any practical time frame.

The survey didn't ask about some of the other technologies referenced in this paper, but it is safe to say that, if IMs are a problem for many companies, these other technologies are going to be much more of a problem.

A radical book published in England is Managing the Crowd: Rethinking Records Management for the Web 2.0 World by Steve Bailey. His basic premise is that our world of data-deluge records management is no longer sustainable. He contends that the lines between personal and business use of technology has become hopeless blurred. He suggests that users would rather search for information than manage it. Users, he believes, will increasingly choose to store information externally. Bailey questions whether records management is no longer fit for the purpose for which it was intended (we told you it was radical).

Web 2.0 requires RM 2.0, which Bailey sees as independent of specific hardware, software and location. He says the system should use Web-based technologies but be extensible – and “future-proof.” From his perspective, all information is worth of initial inclusion and assessment – it is deemed to be of value until proven worthless. He believes in user tagging (folksonomies) rather than classification scheme and metadata schemas. Fascinating stuff, which is sure to engender a lot of controversy.

And ponder this Web 2.0 risk scenario from Michael Cobb: “Suppose you're the CIO of a company that dominates its market to the point where competitors are grumbling about monopolistic practices. Some of your employees decide to “help” by going on the offense, denigrating these grumbling competitors in off-site blog posts and wiki entries, tagging negative stories on the Web, posting slated questions on LinkedIn, fostering criticism on FaceBook and so

on. Then the company is hit with a lawsuit by its competitors for engaging in an alleged smear campaign. Your general counsel proclaims innocence and tries to limit the scope of discovery, but is compelled by law to agree to hand over all relevant ESI.”

Again, interesting. Your opponents will have trolled the Web for data. Can you claim ignorance? Must you produce these off-site communications by your employees? Can you afford not to know about Web 2.0 data? These are questions that are giving CEOs the willies.

Conclusion

The law relating to emerging technologies is vastly underdeveloped, which presents a formidable challenge to records managers. If you have any guiding principle, make it this: Content, not form, drives retention requirements. Policies governing records in your law firm or business should address all forms of communications – and you’ll need to review these policies at least annually in light of newly evolving technologies. Looking for solace? Think job security. No business today can be without records managers and the lawyers who counsel them.

© 2009 Sensei Enterprises, Inc.