

# Capturing Quicksilver: Records Management for All That Other Stuff

Written by Peg Duncan

Presenters:  
Peg Duncan  
Sharon Nelson

April 2-4, 2009  
[www.techshow.com](http://www.techshow.com)

## **Get out ahead of your employees.**

During a panel discussion about the Web 2.0 in the federal government in early January this year, Linda Cureton, the CIO of NASA's Goddard Space Flight Center, said, "Web 2.0 tools are like a train barreling down the tracks, and chief information officers at agencies should be wary about getting run over by the new technology. You can be the CIO that tries to jump on a railroad track and run past a speeding locomotive and not get run over, or you can be a CIO that lays track to outline what the technology can do for your agency. This technology will run you over if you don't get out in front of it and figure out how it can solve your agency's needs."<sup>1</sup>

This doesn't mean that security and risk management are ignored, or that the decision to adopt the technology isn't based on some expectation that it will improve productivity, services, knowledge capital or meet some other business requirement. It may look like Facebook and play like Facebook, but the content still has to be managed if any of it meets the definition of a business record.

If you do install internal Instant Messaging (IM) or Web 2.0 tools, educate your employees and your management team about the records management implications. Making them aware will go a long way to avoiding problems. The awareness-building campaign and education will be different for employees and for management.

## **2. Apply the "90/10" rule to Information Management.**

It is impossible to capture and manage everything. That said, 100% of the communications of key decision makers, whether e-mail, IM or carrier pigeon, will have to be captured in some industries to comply with federal regulations. However, the employees' community wiki can be archived for a short period of time and discarded unless it is subject to a legal hold.

In an AIIM<sup>2</sup> webinar, the consulting firm Doculabs proposed a tiered approach that balanced the risk with the level of effort to manage electronically stored information (or ESI). In descending level of risk, different types of ESI are handled differently:

1. Keep as records that which is currently formally classified
2. Redefine as records that ESI with a higher risk which is currently not formally classified
3. Keep as non-records but move to rigorous Electronic Content Management / Records Management (ECM/RM) system
4. Keep as non-records but manage in specialist system (e.g., E-Mail Management (EMM), Digital Asset Management (DAM))
5. Keep as non-records but manage in collaborative Document Management (DM) system
6. Keep on (better managed) share Drives

---

<sup>1</sup> CIOs like Web 2.0 tools for sharing information, Doug Beizer, Federal Computer Week, January 14, 2009, <http://fcw.com/articles/2009/01/14/cios-embrace-web-2-dot-0-tools.aspx> retrieved, URL retrieved January 21, 2009

<sup>2</sup> Association for Information and Image Management

7. Don't worry about them—they aren't worth it—keep or dispose according to general rules<sup>3</sup>

The risk assessment is based on the content (subject matter) rather than the format (for example, IM) of the information.

*Illustration i:* In light of recent failures in one of its products, a manufacturing company uses portal technology to track complaints from customers and the internal follow-up, with the aim of being transparent and open. Customers have access to the site as a by-product of registering on-line for their warranty, so only legitimate customers can enter the site to post information and check the status of the response. As in the paper world, each complaint has a file number associated with it and the ERM controls its life cycle from creation to archive to eventual destruction.

- 3. Establish a scope statement for each wiki and blog that describes its “mission statement”.**

Presumably a corporation would only implement Web 2.0 technologies if there were some business reason. The bulk of the content should therefore be business oriented (although at the beginning it is reasonable to offer a sandbox facility for social items). The mission statement for each blog or wiki will help determine whether it fits into the Records Management scheme, and if so, where. Again, it is the content that determines whether it is a record, not the format.

- 4. Look for Enterprise Records Management Systems that can be configured to manage multiple repositories of different forms.**

According to Gartner’s 2008 issue of MarketScope for Records Management<sup>4</sup>, there are a number of products on the market that integrate with multiple repositories, including e-mail, e-mail archives, Sharepoint sites and file shares. Vendors are aware of the need to accommodate instant messaging as it has moved into the mainstream and become part of business culture.

- 5. Restrict access to external social networking sites.**

Some companies and government agencies have experimented with social networking sites as a means to improve communications with their clients. Some law firms encourage their lawyers to

---

<sup>3</sup> A Roadmap to Litigation Readiness, presented on January 21, 2009  
<http://www.aiim.org/Events/Webinars-onDemand-Information-Management-Document-Records.aspx>

<sup>4</sup> MarketScope for Records Management, 20 May 2008, Kenneth Chin, Gartner RAS  
Core Research Note G00156666  
<http://mediaproducts.gartner.com/reprints/oracle/article24/article24.html>

blog on their areas of expertise, and the U.S. government has some pioneers working in the virtual world, including:

- NOAA's Virtual Island on YouTube
- Hygeia Philo, CDC's public health avatar in the Second Life world
- NASA's collaborative space exploration CoLab explored on YouTube

Because there is no direct control by the corporation of any "record", agencies must rely on strong policies governing behaviour and scope of content in virtual worlds, as well as trust in the judgment of the individual blogger and the player behind the avatar.

Copies of the external blog can be taken from time to time and "archived" within the company in much the same fashion as some websites are archived now.

Employees should require permission from the corporation to write a blog or provide comments on any subject that is related to the corporation. Blogging on items of personal interest (or Facebook or other social networking) should be done outside the office and not on company time.

**6. Make sure policies are unambiguous and clear, and specifically address “greynet” technologies.**

According to Wikipedia<sup>5</sup>:

“Within the context of corporate and organizational networks, a **greynet** is an elusive networked computer application that is downloaded and installed on end user systems without express permission from network administrators and often without awareness or cognition that it is deeply embedded in the organization’s network fabric. These applications may be of some marginal use to the user, but inevitably consume system and network resources.”

Employees need to know what is permissible, what is not, and how each type of communication is treated in the records scheme.

**7. Lock down workstations, and disable USB ports.**

Ban local storage, while you’re at it. The computer that was bought by the corporation should be controlled by the corporation. It isn’t a home computer.

Most people’s home computers are the Wild West, with anti-virus, anti-spam, anti-adware, anti-malware barely able to keep up, if they are running at all. The nasty bits come in uninvited along with the downloads of free software, free services and appealing little gadgets.

This free-for-all approach isn’t appropriate for corporations. Firstly, the unofficial privately subscribed instant messaging (IM) service such as MSN is a parallel communications network, creating problems for compliance. Secondly, the free services like BitTorrent, Kazaa and other file-sharing systems chew up bandwidth and open up the risk of violations of IP, or, equally bad, becoming a host for “botnets”<sup>6</sup>. Thirdly, there’s the resulting instability in the workstations from the attendant “helper” and spyware software. Finally, there’s the productivity issue of people writing their personal blogs on company time.

Lockdowns won’t entirely solve the problem, since IMs and other tools come with Windows or are browser based, so the network policies must be there to make it clear what is permissible.

**8. Address cultural issues.**

It’s easier to avoid bad habits than to try to change them after the fact.

---

<sup>5</sup> Wikipedia Greynet <http://en.wikipedia.org/wiki/Greynet>

<sup>6</sup> A botnet is a collection of compromised computers under the remote command and control of a criminal “botherder.” From an FBI press release dated June 13, 2007, titled Over 1 Million Potential Victims of Botnet Cyber Crime at <http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm>

## 9. Develop a cordial relationship with IT.

One of the interesting consequences of e-discovery is that it throws together people who, throughout their careers, have actively avoided one another – lawyers and engineers. There is ample opportunity to misunderstand what the other side is saying, and missed messages can result in costly errors.

*Illustration ii:* A well-established company in the communication sector has recently acquired an innovative start-up. Unlike other areas examined during a merger, there is “no general or widely accepted approach that one could use for initial due diligence of IT”.<sup>7</sup> However, the hardware and software systems were sound, the infrastructure was well-documented, the equipment under warranty, and the software licensed, so the team believed there was no source of concern. What became clear during the course of litigation related to the merger was that the innovative start-up permitted their design team to use collaboration technologies (downloaded from the internet) that gave each user a local, editable version of the workspace, which employees used to work from their home computers. This additional source of evidence only came to light in the middle of discovery.

If the IT team had known what might be a risk and been on the lookout for greynets and Web 2.0 technologies, and had the lawyers understood the implications of relaxed information management policies, both might have been in a better position to plan for the preservation, collection and review of the information for relevance rather than having to react.

It’s amazing what comes out in casual conversation.

*Illustration iii:* When Corporate Counsel received her BlackBerry, she started using the pin-to-pin communications with other company officers as a means to stay on top of issues. Curious about what happens to the messages and wanting to retain them for reference, she asked how she could search and retrieve them later and learned that IT had not been asked to set up a log of the messages.

## 10. Consider the trend to have RM report to Legal rather than admin.

In a study funded by the National Historic Publications and Records Commissions (NHPRC) Electronic Records Research Fellows Grant in 2005-2006, nearly half (47%) the participants

---

<sup>7</sup> Initial Due Diligence of Information Technology as Risk Identification before Capital Investment in Finance Industry, M.Sc.Bo-stjan Delak, 2008 submission as a proposal for a PhD thesis, University of Ljubljana, Slovenia, <http://www.doc.ic.ac.uk/~pjm/caisedc2008/delak.pdf>, URL retrieved January 21, 2009

reported ultimately to the legal department, and only 13 percent report to administrative services.<sup>8</sup>

© Peg Duncan 2009

---

<sup>8</sup> Where Records Management Should Report: A Study and Comparison of Industry and Government, Carol E.B. Choksy, published by ARMA International in 2008  
<http://www.arma.org/pdf/journal/rmreporting.pdf>

## References

1. NARA: Guidance and Resources for Integrating Records Management and Electronic Information Systems, <http://www.archives.gov/records-mgmt/handbook/integrating-records-mgmt.html>
2. R U Ready for IM, Jesse Wilkins, May/June 2007 edition of The Information Management Journal  
[http://findarticles.com/p/articles/mi\\_qa3937/is\\_200705/ai\\_n19433430](http://findarticles.com/p/articles/mi_qa3937/is_200705/ai_n19433430)
3. Uncovering the Malware Economy, a panel presented at the Federal Trade Commission's Spam Summit in July, 2007  
<http://www.ftc.gov/bcp/workshops/spamsummit/presentations/Malware-Economy.pdf>  
URL retrieved January 22, 2009
4. Social Networks and Government, describing potential uses for government information and services, November 19, 2008  
[http://www.usa.gov/webcontent/technology/social\\_networks.shtml](http://www.usa.gov/webcontent/technology/social_networks.shtml)
5. Blogs – Guide to Managing U.S. Government Websites  
<http://www.usa.gov/webcontent/technology/blogs.shtml>
6. NASA Blog: Linda Cureton: Consumerism and the Irrelevant CIO, posted on November 29, 2008 at <http://blogs.nasa.gov/cm/blog/Goddard%20CIO%20Blog>
7. NARA's ERM Initiative Guidance Products, available on  
<http://www.archives.gov/records-mgmt/initiatives/erm-products.html>
8. Government and Social Media, presented by Bev Godwin at the March 2008 Social Media for Communicators Conference  
[http://www.usa.gov/webcontent/documents/Government\\_and\\_Social\\_Media.pdf](http://www.usa.gov/webcontent/documents/Government_and_Social_Media.pdf)
9. White Paper On Data Retention Of Voice Mail For Regulated And Unregulated Industries In The U.S. And E.U., December 7, 2006, prepared for Microsoft by Covington and Burling LLP, available at  
<http://www.microsoft.com/exchange/evaluation/unifiedmessaging/dataretentionwp.mspx>

*The views expressed in this article are those of the author and do not necessarily reflect the views of the Canadian Department of Justice or the Government of Canada.*