



2009 Corporate Counsel Seminar Series
Session 3

Managing Litigation and Employment Issues in Electronic Communications

Wednesday, September 23, 2009

Email Etiquette



1. Be concise
2. Limit CC's/Reply-to All
3. Ask/answer questions clearly
4. Limit use of URGENT/IMPORTANT and all capital text
5. Breaking the chain

Email Etiquette



6. Use specific subject lines
7. Use proper spelling, grammar and punctuation
8. Avoid angry responses, criticism, sarcasm
9. Don't use fancy formatting or signatures, or attach vCards to every email
10. Recognize email's limitations



Arthur Hamilton

Managing Litigation and Employment
Issues in Electronic Communications

Litigation Issues

Wednesday, September 23, 2009

Complex Obligations of E-Discovery



- The concept that electronically stored information is discoverable is not new
- But the sheer volume of electronically stored information now adds a significant degree of complexity to documentary discovery
- And the nature and characteristics of electronically stored information require close attention to details such as the retention of this information

Complex Obligations of E-Discovery



- Complexity also results from the fact that electronically stored information can be stored in multiple locations:
 - On-site and off-site servers owned/operated by the client
 - Service providers or shared servers
 - Individual users' drives (magnetic disks)
 - Back-up tapes or other storage devices
 - Text message/PINs on Blackberry units or cells
 - Personal computers used by employees
 - Electronic calendar/task lists etc.
 - Optical disks (CDs or DVDs)
 - Flash memory (such as "thumb" or "flash" drives)

Complex Obligations of E-Discovery



- To try to make sense of this, the *Sedona Canada Principles Addressing Electronic Discovery* have emerged
- Under these principles, in any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account:
 - i. The nature and scope of the litigation, including the importance and complexity of the issues, interests and accounts at stake;
 - ii. The relevance of the available electronically stored information;
 - iii. Its importance to the Court's adjudication in the given case; and
 - iv. The costs, burden and delay that may be imposed on the parties to deal with electronically stored information.

Complex Obligations of E-Discovery



- The principles are engaged as soon as litigation is reasonably anticipated – at that time, parties must consider their obligation to take reasonable and good faith steps to preserve potentially relevant electronically stored information.
- Parties should not be required, absent agreement or Court order, to search for or collect deleted or residual electronically stored information.
- The reasonable costs of preserving, collecting and reviewing electronically stored information will generally be borne by the party producing it.

E-Discovery Best Practices



- Always be in position to identify all relevant sources and volume of electronically stored information
- Maintain a list of all IT personnel and custodians of the information
- Maintain retention and/or litigation hold policies for electronically stored information
- Understand the systems being run, so that any automatic or default deletion practices can be managed (things such as 30 day over-writes on back up tapes, etc.)
- Train personnel to recognize and properly react to litigation hold notices from opponents
- Develop a protocol of who at the client, if anyone, should collect and retain the electronically stored information

E-Discovery Best Practices



- Apart from best practices for dealing with electronically stored information that exists, there are best practices related generally to the use of electronic forms of communication and information retention, which, when not followed, can lead to difficulties in the prosecution or defence of proceedings:
 1. E-mail nightmares
 - Casual language (or worse)
 - Consciousness of thought or reactive emails which can be commended more for their speed than their accuracy
 - Personal, gratuitous attacks
 - Ambiguous/sarcastic messages which are open to interpretation

E-Discovery Best Practices



2. PINs

- Supposedly private communications, but these text messages still go through a server somewhere, and are retrievable (either from the device itself or the service provider's server)
- PINs which must be produced can actually make a situation much worse
 - Because it was to be private, people tend to let their guard down ever more
 - The author is highlighting her or his intent to keep something confidential, even where no court would recognize a confidentiality protection
- PINs are sometimes accompanied by a regular email message telling the recipient to check for a PIN, which highlights that mode of messaging for the opponent

E-Discovery Best Practices



3. The “Grumpy” User

- Personnel who try to by-pass systems put in place for all employees
- Personnel who delete material without reviewing it, to keep their in-box clear
- Personnel who use unprofessional language in electronic communication
- Personnel who don't adhere to retention, hold or storage policies for electronically stored information

In some instances, best practices require a cultural shift in the way electronically stored information is utilized and handled.

Protecting Privilege



- With electronically stored information the principles for maintaining privilege are the same, but the opportunity for error is much greater
 - Volume of documents is greater
 - Differentiation of documents is less obvious
 - Attachments to e-mails may not be properly identified/protected
 - E-mail chains can contain both privileged and non-privileged material
- There is no substitute for a very careful review of all documents being considered for production.

Protecting Privilege



- When producing electronically stored information, ensure the production is accompanied by a reservation of rights to retrieve any document which contains privileged information, but which was inadvertently produced
- When using key words to run search parameters, be over inclusive when selecting terms to capture communications of a privileged nature
- Beware to look for privileged information, not just the indentifies of those you would expect to be engaging in privileged communications



John McGowan

Managing Litigation and Employment
Issues in Electronic Communications

Employment Issues

Wednesday, September 23, 2009

E-mail and Internet Use Policies



- Key Features:
 - Company computers are company property.
 - Company e-mail should be used only for company purposes.
 - Either no, or incidental, personal use of company computers during work.
 - Personal e-mails should not go out from the company server or be identifiable as company documents.
 - THE COMPANY RETAINS THE RIGHT TO MONITOR COMPUTER USE, INCLUDING E-MAIL AND INTERNET USE.
 - NO EXPECTATION OF PRIVACY IN ANY ELECTRONIC COMMUNICATIONS OR RESPECTING WEBSITES VISITED.

E-mail and Internet Use Policies



- Key Features:
 - All computer use and communications must be consistent with other company policies including without limitation harassment.
 - Company reserves the right to block access to certain sites including social networking sites (Facebook).
 - No installation of games or any other software, whether or not employment related, without approval of I.T. department.
 - Supervisor must have knowledge of all passwords employees are using, and must be updated when those passwords are changed.
 - Other issues may be addressed, but these are the core issues.

E-mail and Internet Use Policies



- Recent Developments in At-Work Internet Use:
 - *Leduc v. Roman*
 - This case involved a motion to require the plaintiff to disclose components of his Facebook webpage that were not otherwise accessible to the public.
 - Arose out of a car accident. Issue was plaintiff's ability to enjoy the same quality of life he had prior to the accident.
 - Court found that the Facebook profile page were "documents" and discoverable in that they "might have some relevance to demonstrating the plaintiff's physical and social activities, enjoyment of life and psychological well being".

E-mail and Internet Use Policies



- Recent Developments in At-Work Internet Use:
 - *Leduc v. Roman*
 - Court inferred from the social networking purpose of Facebook that it was likely that relevant information would be there, and that a defendant's requesting information about the contents of the private components of the webpage were not a fishing expedition.
 - Leave was granted to cross-examine the plaintiff on his supplementary affidavit of documents about the nature of content posted on the Facebook profile.

E-mail and Internet Use Policies



- *Horizon v. Bonnen*
 - To my knowledge, the first example of somebody being sued for defamation based on a Twitter post (posted in reply to a friend visiting her):

“You should just come anyway. Who said sleeping in a moldy apartment was bad for you? Horizon Realty thinks it’s okay.”
 - Lawsuit launched by Horizon for \$50,000 for defamation and breach of business reputation.
 - Simple example of a short communication leading to litigation, and potentially involving employers where the comment is associated with occupational function, or relates to the employer itself.

E-mail and Internet Use Policies



- What if Your Company is the Subject of a Hate Blog or Webposting?
 - *Cohen v. Google, Inc. and Blogger.com* provides a recent example:
 - A well publicized case involving a model in New York who was described as a “skank” in an anonymous bloggers page.
 - Google was ordered to disclose the identity of the blogger.
 - A copy of decision is enclosed in the materials.
 - Blogger was last reported to be suing Google for \$15,000,000 for having revealed her identity pursuant to the Court Order. Stay tuned.



www.casselsbrock.com