# Social Media and the Implications for E-Discovery

It's 8 o'clock. Do you know where your employees are?

It seems to make no sense to ask such a question, does it. After all what employees do on their own time has always been considered none of an employer's business and to ask may seem to border on invasion of privacy.
The question we need to consider though is "Are the times changing so much that we *should* wonder what goes on outside the office walls?"
In a world of instant distributed access, hitting the 'send', 'post' or 'publish' button can be added to the old Chinese saying "Four things come not back: the spoken word, the spent arrow, the past life, and the neglected opportunity."
The prevalent use of social media as a form of global grapevine has revolutionised the way we communicate, collaborate, and form popular opinion. The use of social media by employees has also impacted on the way that companies need to view the extent of the data that needs to be preserved in the event of a litigation hold.
The ubiquitous nature of social media gives rise to several issues that every Legal Department should be cognizant of.
A major one would be to recognise the true extent of the data to be captured in order to be litigation ready. Most responsible companies these days already have some system which mines the data from emails, file shares, document management systems and other repositories which store the myriads of documents and communications which pass between employees. But recently the courts have had to consider the completeness of disclosure in e-discovery situations. Turns out that there is much more to be disclosed than soft copies of documents. And this is where the legal department needs to get up to speed on the full impact of social media upon the e-discovery process.

Courts are being called upon to consider for the first time, whether statements, commentary and postings made by employees on social networks such as Facebook and Twitter, are discoverable. Statements made in instant messages (IM's), group discussion boards, forums, and conceivably skype and the new google chat, are open for legal debate in the courts. And 'data' extends to that kept by employees on mobile devices such as blackberries, iphones, ipads, laptops and the new generation of tablets currently hitting the markets. Data is also to be found in "the cloud", whether it lies on hosted servers or in the public cloud.

The kinds of social media platforms and the devices that enable their use are changing at such a rapid pace that e-discovery rules lag behind in their application. The courts are therefore being called upon to rule on matters on which there is no solid guidance. Judge Stephen Robinson, now a partner with the firm of Skadden, Arps in a recent webinar produced by the New York Law Journal made the point that not all judges are familiar with the technology systems that support social media. Courts assume that documents (and by extension, data), are collected, retained and easy to find. So it is in counsel's interest to set the scene depicting "information at large" in social media, and explain the technology and the terms to the Court.

It is clear is that the rules of litigation have changed irrevocably and we are sailing in uncharted waters. It is for this reason that advice coming from commentators is about the prudence of instituting a social media policy. The first step is to understand your data universe. A survey of social media use last year showed that about 50 % of companies have some sort of presence on social media sites, whether on LinkedIn, MySpace, Twitter, Digg, YouTube, Facebook ,blogs etc. Not as many as 50% have a social media policy though. Many companies today adopt the conservative approach to the use of new media and social media, under the misapprehension that proscribing the use of the internet during work hours somehow makes employees produce more work.The efficacy of such policy is another debate for another time. Suffice it to say that in a world of mobile personal connectedness, there is far more information from and about your company floating around the internet than you are even aware. Witness photos and real time "video in maps" from sources such as Bing Maps and Google maps which stitch photos from individual contributors, including photos on Flickr to give us a bird's eye view of office buildings and more in town. Not to mention blogs,micro blogs,wikis ("law-wiki" is a recent one rating law firms and lawyers), Twitter, instant messaging and chats, and the list expands rapidly.
Information is written about your company in the social media sphere, whether you like it or not. Even a recommendation from a supervisor on LinkedIn can resurface as evidence in a wrongful dismissal suit.
So it is in your interest to 'get with it', see what is being said about you, and join the discussions. Keep up to date with the happenings in social media.Place yourself on wikipedia and law-wiki before someone does it for you. In other words, do the damage prevention before you have to do damage control.
Some commentators have observed that one can safely assume that nothing that gets uploaded on to the internet is ever really destroyed or gone forever. Deleting an item may move it out of sight, but the content may have migrated and been spread to another place on the web through a third party. And this may not be malicious at all. A friend could share data (whether it' s photos or writings), innocently enough. A sent and deleted email could already have been forwarded by the recipient to a third party. Search engine spiders or bots trolling the web periodically, have already indexed the web page on which the posting was made. (And scarily, a criminal record though expunged from the records, may still be found in an archived paper or magazine online).

So this is a sample of the data universe in which e-discovery has to take place in today's digital world. The current uncontrolled reach of relevant information gives rise to issues of possession, custody and control of data during e-discovery. Both General counsel and External counsel need to be aware that information exists in places beyond the reach of the data management systems and the custodians thereof. Counsel needs to be aware of what exists too, because what he requests of opposing counsel is what he will be expected to produce for his own client.

When employees post statements (say for example, on Facebook) that may be of relevance in a potentially litigious matter, the question that often arises is, within whose possession, custody and control are those statements. The issue of compellability of such evidence rests upon the relevance of the data, and how much of a burden is its retrieval. Privacy concerns are also factored in.The issues of whether or not Facebook can be compelled to produce defamatory

statements made by employees, who have made those statements under their page ‘privacy’ setttings are matters that are currently making the court circuit. It is a nascent area of law and it would be interesting to see where this is all going to lead.

A social media policy is arguably the best protection in a charge of incomplete discovery of documents in an action. Given the dearth of legal procedural rules to guide social media discovery, a company’s best offence is said to be a written policy.It is more defensible to refuse to give up data when you can show that you did everything to follow your policy.This gives the court some reference for making a ruling.

Here are some factors I have pulled together, which should be addressed when drawing up a social media policy for your employees. These include:

- Educate employees, management, C-Suite and the leadership about general benefits and the risks and repercussions of the use of social media
- Identify an officer to monitor the social media environment for the latest development in new media and your company’s name in it (e.g. new wikis, new features in web applications -eg geographical mapping where your company might show up without your knowledge, new search features etc)
- Data-map the social media sites that employees are using to guide the defensibility of non-disclosed data
- Map where the data resides so it can be tracked quickly in the event of a litigation hold
- Where data is in the private cloud in the form of wikis and blogs and such, determine a time period for retention and disposal
- Identify the departments that should be involved in the ‘custodianship’ of social media data (is it IT, Legal, HR, and/or practice group?), as part of a litigation readiness program
- The policy itself should be short, simple and concise. The more detailed you make it, the more you open the door to an employee thinking that what is not specifically prohibited, is permissible.
- Educate employees about what constitutes defamatory material-what is not acceptable
- Proscribe the divulgement of trade secrets, confidential and sensitive information
- Be clear on what kinds of documents/statements made by employees, are privileged and not
- Document best practices and update policy regularly, in light of the changing face of social media