Lawyers In "The Cloud"

A Cautionary Tale

Garry J. Wise, B.A. LL.B., Barrister and Solicitor
Wise Law Office, Toronto - (416) 972-1800

Presented at: Security for Lawyers in a Wired World - October 16, 2009
Law Society of Upper Canada Teleseminar

****

Prologue: Nothing Lasts Forever

With the July 26, 2009 shutdown of *Yahoo's GeoCities* now imminent, we are once again reminded that on the Internet, nothing is necessarily forever.

A mighty innovator in digital days gone by, *GeoCities* housed many of the Internet's earliest law firm websites and legal resource directories. *GeoCities* was the Web's fifth leading destination in mid-1997, hosting more than one million free websites by the end of that year. Acquired by Yahoo! for $3.57 billion in 1999, it continued to boast 177 million visitors annually as recently as 2008.

GeoCities died a slow death, brought inevitably on by superior, innovative alternatives in the digital marketplace and its own, ultimate obsolescence. A precursor to *Blogger* and other modern, free self-hosting services, it succumbed to a failure of vision rather than resources, and ultimately was left far behind.

Now, it shall be no more.

Even as *Yahoo*! was laying *GeoCities* to rest, the City of Los Angeles was ushering in a new era, as it gave serious consideration to a controversial, multi-million dollar initiative to utilize *Google's* online applications for the City's email, word-processing, data storage, police records and other, sensitive municipal functions.

Notwithstanding the sound economics of the plan, the L.A. proposal has received a frosty reception in web security circles. As *Associated Press* reported on July 17, 2009 in *Concerns raised as L.A. looks at Google Apps:*

> At issue is the security of computerized records on everything from police investigations to potholes as the nation's second-largest city considers dumping its in-house computer network for Google e-mail and office programs that are accessed over the Internet.
>
> Paul Weber, president of the Los Angeles Police Protective League, complained Thursday that the union had scant information on the plan or what it would mean for the safety of sensitive records, such as narcotics or gang investigations.
>
> His worries came just one day after the online-messaging service Twitter acknowledged hackers were able to access confidential information stored with Google, which has been promoting greater use of "cloud computing" — storing data online rather than on individual computers under a company's or government agency's direct control. The shift toward doing more over the Web could make it much easier for hackers to gain access to corporate or government files. No longer would someone need to try to break through layers of security firewalls. As various personal and work accounts become increasingly linked together, all one needs is a single password to access documents just like a regular employee.

The *GeoCities* closure may fall well short as a cautionary tale, just as L.A.'s debate may or may not prove to be a harbinger of things to come. Nonetheless, for lawyers assessing the security of *Google Docs,* online data storage and other software as a service (Saas) technologies offered exclusively on the Web, there is a clear message to be taken from these two, parallel developments.

Progress and change remain inevitable online. The darlings of yesteryear (and this year) are likely to lose considerable luster with the passage of time. One day, they may also be gone.

The *GeoCities* shutdown demonstrates graphically that users have virtually no control over the eventual fate of the services they utilize – or the data they create within those services. In fact, many *GeoCities* users are currently scrambling to complete a last-minute salvage operation, even if it is for posterity alone.

If nothing lasts necessarily forever online, then, it is well worth a moment to consider the degree to which *"nothing"* in that context may also include *our data*.

With this reality in the back of our minds, let us look at *the Cloud*.

Practicing Law in *The Cloud*

So what is this *Cloud*, and why are so many professionals asking about it? What are its advantages? What should we be concerned about? Should we go there, and if we do, how must we protect ourselves?

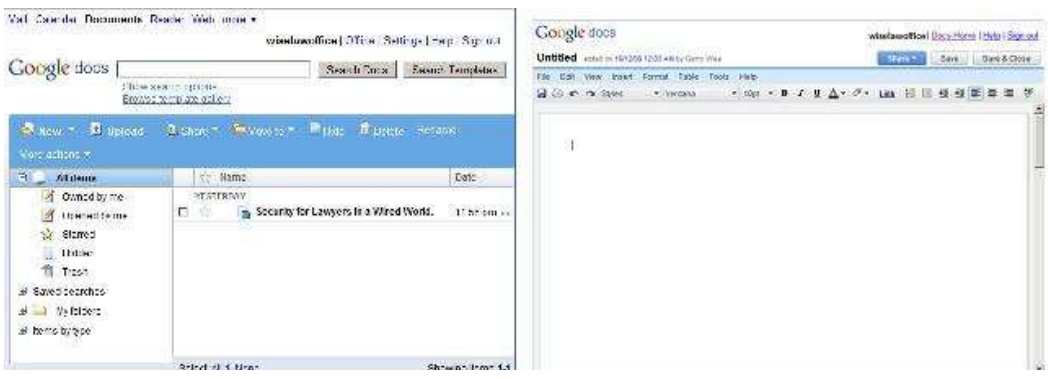
In this paper, we will canvas the emerging world of "*Cloud* computing," with a particular emphasis on recent events that shed considerable light on whether *the Cloud* delivers an adequately stable and secure environment for the legal professional. Upon review, it seems *the Cloud* is not quite ready for prime time.

Dennis Kennedy provides a good working definition of this next generation of online offerings in *Working in the Cloud,* an August 2009 article in the *American Bar Association Journal:*

> In popular terms, the cloud refers to two related things. First, the websites and services that allow you to use the Internet as a platform to run programs and store data. Second, the system of worldwide data centers owned by Amazon.com, Google and others on which these Internet services run.
>
> The term *cloud* is used because in this system, which includes things like virtual servers, it actually becomes a little difficult to point to exactly where all your data is being stored or managed. It's definitely not in your firm's server room. You also do not install the software you use on your own computer. It's accessible on a website through your browser.

Most typical law office functions can now be handled exclusively online in *the Cloud* with SaaS (software as a service) providers that enable worldwide access from any web browser and feature enhanced, collaborative functions. By way of examples, comprehensive word processing and spreadsheet functions are available with Google Docs. Web-based email providers include Yahoo Mail, Gmail, and Hotmail, to name but a few. Law office accounting functions can be performed online with *E-conomic, Kashflow and Xero* (allegedly coming soon to Google Apps).

Figure 1 – Google Docs



Similarly, legal research has long since abandoned the library for the laptop.

Comprehensive case management software is offered with packages like *Houdini* that purport to centralize and simplify various professional functions, enable tagging and indexing documents, and provide a password-protected client interface. These services aspire to replace our typical cache of expensive, cumbersome software packages like Microsoft Office and PC Law and various localized case management suites.

These online offerings will likely have considerable success - they are tempting, indeed.

They allow for the reduction or elimination of hardware and software costs. They provide the convenience of access from the web, as opposed to local PC or firm server access. They offer unlimited data storage, facilitate easy collaboration and help maintain document version control. Software patches and updates are managed centrally by providers, with little or no action by the user required. Centralized backup and data storage redundancy reduces the risk of data loss.

Perhaps most critically, these services offer genuine, functional advantages.

For the legal profession, and commercial enterprises generally, however, there is one overarching concern about these services that causes us to tread very cautiously:

Are they safe?

How Secure is Professional Life in *the Cloud*?

There may always be security, reliability and stability issues associated with the commercial implementation of any new, digital technologies.

Life in *the Cloud* is hardly unique in this regard. Just as the last generation of innovations – personal computing, email, word processing, the web and digital communications – posed a bevy of never-before contemplated security concerns for lawyers, this next generation of online services will pose its own.

Many of the key security concerns in *the Cloud* can be described quite succinctly:

1. Security breaches that could lead to unauthorized access to a user's account and interference with the sensitive information contained therein.

2. Hacker and other attacks that create "denial of service" downtimes and interfere with account and information access;

3. Malicious spyware, keylogger programmes, hacker attacks and old-fashioned user carelessness, all of which could lead to passwords breaches and unauthorized access;

4. Software company closures and bankruptcies that may permanently shut down vital services without adequate notice to allow data preservation;

5. Law enforcement outside Canada may require disclosure of your account - in jurisdictions that offer no protection for solicitor-client privileged information this is especially problematic.

Practitioners should indeed be concerned about these many, exotic security risks posed by *the Cloud* . They are generally beyond our physical control and technological grasp and in some regards, are extremely difficult to guard against.

Having said that, and without minimizing these next- generation concerns, a good general rule to follow is that *security begins at home*

Security Starts at Home – *Safe Data* Basics

Inside or outside *the Cloud*, a firm's *security hygiene* will always be the best predictor of the ultimate safety of its data – in a nutshell, a firm's data will only be as secure as its users' passwords and its own security policies and awareness.

The risks of a data loss or a security breach at a distant *SaaS* server are likely quite remote in comparison to the nightmares that can arise from carelessness or oversight in our own offices.

Simply put, before indulging in any esoteric review of new-fangled security concerns, it is important to note that a few *safe-data basics* will go a long way to ensuring your information is safe, protected and always accessible as required, whether you enter *the Cloud* or not:

- Conduct daily backups
- Password-protect your computer, software and critical documentation
- Refresh or update passwords regularly
- Keep second or redundant copies of all email folders and digital client documentation
- Replace or upgrade computers and software that have proven unreliable
- Run anti-virus software daily and update your software regularly;
- Use anti-spyware software and conduct regular spyware scans
- Use firewalls to prevent intrusions by hackers
- For Windows users, use automated Windows Updates to install operating system updates and security patches
- Be mindful of data security concerns when hiring and when staff departs.
- Consider adopting "need to know basis" data access policies and employ data-access hierarchies within your firm
- Vigilantly guard your Blackberry and laptop;
- Backup your mobile devices and secondary computers;
- Don't leave confidential information on your desk overnight or when you have meetings in your office.
- Exit all software and documents when you leave your office – don't leave sensitive information on your screen when you aren't in front of your computer.

Even for those that have adopted all such safe-data measures, however, *the Cloud,* throws a few, serious new twists into any law firm's security overview. Because you do not have physical control of your data in *the Cloud*, your firm's data security online is often beyond your control. It will be determined by the diligence of third party service providers.

By any reading of recent history, there is genuine cause for concern in this regard. We will survey the key risks below.

Data Breaches

A 2008 study by the Enterprise Strategy Group found a shockingly high prevalence of data breaches among the North American companies it sampled:

> In a November 2008 survey of 179 North American-based security professionals, 56 percent claimed that their organization had suffered a data breach within the past 12 months. In further analysis, 61 percent of organizations with 1,000 to 5,000 employees suffered a data breach in that time frame. It's easy to assume that these smaller firms are more at risk since they are likely to have fewer security technologies in place and smaller

security staffs. Perhaps this is true, but even bigger companies are suffering data breaches--49 percent of organizations with 5,000 employees or more endured at least one data breach of their own.

The online encyclopedia *Wikipedia* has nicely catalogued some of the more notorious security breaches of recent years. While these breaches extend beyond *the Cloud*, they are illustrative of the vulnerabilities of the digital environment, generally.

Cumulatively, the evidence suggests that the online environment has yet to achieve any level of reliable security that would justify a generalized degree of user comfort:

Figure 2 – Major Data Breaches 2005-2009 (Excerpted from Wikipedia)

2009

- In January 2009 Heartland Payment Systems announced that it had been "the victim of a security breach within its processing system", possibly part of a "global cyber fraud operation" The intrusion has been called the largest criminal breach of card data ever, with estimates of up to 100 million cards from more than 650 financial services companies compromised.

2008

- In January 2008, GE Money, a division of General Electric, discloses that a magnetic tape containing 150,000 social security numbers and in-store credit card information from 650,000 retail customers is known to be missing from an Iron Mountain Incorporated storage facility. J.C. Penney is among 230 retailers affected.[1]
- Horizon Blue Cross and Blue Shield of New Jersey, January, 300,000 members
- Lifeblood, February, 321,000 blood donors
- British National Party membership list leak,

2007

- The 2007 loss of Ohio and Connecticut state data by Accenture
- TJ Maxx, data for 45 million credit and debit accounts
- 2007 UK child benefit data scandal
- CGI Group, August, 283,000 retirees from New York City
- The Gap, September, 800,000 job applicants
- Memorial Blood Center, December, 268,000 blood donors
- Davidson County Election Commission, December, 337,000 voters

2006

- AOL search data scandal (sometimes referred to as a "Data *Valdez*"[8],[9],[10] due to its size)
- Department of Veterans Affairs, May, 28,600,000 veterans, reserves, and active duty military personnel
- Ernst & Young, May, 234,000 customers of Hotels.com (after a similar loss of data on 38,000 employees of Ernst & Young clients in February)
- Boeing, December, 382,000 employees (after similar losses of data on 3,600 employees in April and 161,000 employees in November, 2005)

2005

- Ameriprise Financial, stolen laptop, December 24, 260,000 customer records

This record speaks for itself. Simply stated, the frequency of massive security breaches in the current digital environment justifies serious pause as to the wisdom of entrusting online systems with any sensitive or privileged professional information.

System Downtimes and Inaccessible Data

System downtimes and interrupted data access are a frequent nuisance in *the Cloud*. They are caused at times by innocent human error. They also result from targeted attacks with malicious intent.

For users, the results are indistinguishable. Their data becomes unavailable.

Richard Raysman and Peter Brown canvassed hackers and cybercrime in a July 2009 article in the *New York Law Journal*, *Are Web Applications a Security Concern*?

> Over the Fourth of July holiday weekend, a wave of cyber-assaults, or "denial of service" attacks, believed to have originated in North Korea, targeted a number of U.S. and South Korean government agency and commercial Web sites, causing some to suffer temporary outages. …
>
> In addition, several high-profile computer hackers have recently been indicted or face prison time as a result of their unlawful activities. For example, a hacker named "Max Vision," who stole almost 2 million credit card numbers from financial institutions, merchants and other hackers, recently pleaded guilty to federal wire fraud charges and is awaiting sentencing. In another matter, a 19-year-old blind hacker was sentenced to 135 months in prison for unauthorized access to telecommunication company information, among other crimes. Also, in ongoing proceedings, an accused British hacker, who allegedly accessed data on NASA computers, is seeking judicial review of a prior order permitting his extradition to the United States, arguing he should not be held criminally responsible because he is a sufferer of Asperger's syndrome. Facing similar concerns to operators of government networks, private companies with external Web sites can be susceptible to attackers looking to commit defacement or infiltrate computer networks to steal sensitive information. The increased corporate reliance on complex applications and technologies contribute to the potential for security vulnerabilities and an increased need for computer security. A growing concern, legitimate Web sites continue to be targeted by hackers, with a reported 30,000 pages affected every day by malware attacks. Successful attacks can compromise confidential resources or consumer data and harm an organization's image. Further, an improperly configured Web server can be attacked directly to obtain unauthorized access to an organization's internal resources. "

Other headlines over recent months, excerpted below, have focused on widespread service outages affecting the leading applications of Microsoft and Google:

- *Expert provides more proof hackers hijacked Hotmail accounts* - Computer World, October 12, 2009 – "It's almost certain that hackers obtained the Hotmail passwords that leaked to the Internet through a botnet-based attack, a researcher said today as she provided more proof that Microsoft's explanation was probably off-base…Microsoft acknowledged that "several thousand" Windows Live Hotmail usernames and passwords had been acquired by criminals, and that it believed the list was the result of a massive phishing attack. Google later said the same thing after another list surfaced with Gmail account details"

- *Gmail outage deprives millions of e-mail- Today's Top Trends, September 1, 2009* - "On September 1, 2009 - Gmail, Google's popular free e-mail service, was inaccessible to many of its 36 million users Tuesday afternoon, causing widespread chatter on Twitter and other social networks. The cause of the outage, which Google said lasted an hour and 45 minutes, was not apparent."

- *Widespread Google Outages Rattle Users - Digital Media - CNET News*, May 14, 2009 – "Many people found Google's search site was extremely slow or inaccessible Thursday, and other reports pointed to troubles with other properties including YouTube, Gmail, Google Analytics, Google Maps... UPDATED: Widespread outages involving several Google services--including search, Google Docs, and Gmail--were caused by an upgrade gone awry inside of Google, according to engineers."

- Google Outage Lesson*: Don't Get Stuck in a Cloud - PC World*, May 15, 2009 – "Google has apologized for yesterday's service outage that left 14 percent of its user base without Google's wide variety of online services for a few hours."

- *Twitter hack raises 'cloud computing' questions – CNN.com*, July 16, 2009 – "The recent hacking of a Twitter employee's personal *Gmail* account is raising questions about the security of storing personal information and business data on the Internet."

The Courts and Service Providers May Close Your Account Without Notice

As if security breaches and denial of service attacks were not adequate cause for concern, consider the September 26, 2009 decision of California's Northern District Court in *Rocky Mountain Bank -v- Google, Inc.*

In this case, the Court ordered *Google* to close a non-party's *Gmail* account after the Plaintiff bank accidentally forwarded an email containing names, addresses, social security numbers and loan information of more than 1,300 customers to the wrong *Gmail* address. The bank did not receive a response from the recipient after notifying of the error. *Google* advised the bank that account-holder information would be revealed only if a Court ordered such disclosure. On the hearing of the matter, the court ordered disclosure of the recipient's name, but *also required Google, to shut down the recipient's email account*. Subsequently, the bank and Google apparently asked the Court to order reactivation of the account.

- See: *Google Ordered to Close Email Account - Slaw*, September 26, 2009

Another recent occurrence at Facebook demonstrates the arbitrary authority to suspend or terminate service retained by online service providers.

A Toronto model had her Facebook account suspended for posting suggestive photographs. More interestingly, a supportive journalist also found his account unilaterally suspended. Facebook justified the journalist's account suspension, indicating, "the company had received reports that the journalist's account was fake." No notice was given to either individual prior to the suspension of the accounts. Both users' accounts were subsequently reinstated after the suspensions received international attention.

- See: *Model challenges Facebook over lingerie pics - CTV.ca* – September 26, 2009 -

Keyloggers and Spyware

Computer World recently reported on a 2008 keylogging incident at an Ohio hospital that would send chills down the spine of any IT administrator:

> A 38-year-old Avon Lake, Ohio, man is set to plead guilty to federal charges after spyware he allegedly meant to install on the computer of a woman he'd had a relationship with ended up infecting computers at Akron Children's Hospital.
>
> In late February 2008, Scott Graham …allegedly sent the spyware to the woman's Yahoo e-mail address, hoping that it would give him a way to monitor what she was doing on her PC. But instead, she opened the spyware on a computer in the hospital's pediatric cardiac surgery department, creating a regulatory nightmare for the hospital.

> Between March 19 and March 28 the spyware sent more than 1,000 screen captures to Graham via e-mail. They included details of medical procedures, diagnostic notes and other confidential information relating to 62 hospital patients. He was also able to obtain e-mail and financial records of four other hospital employees as well, the plea agreement states.
>
> …Eric Howes, director of research services with antivirus company Sunbelt Software… faulted the hospital's IT staff for allowing someone to download spyware from Yahoo mail and install it on their systems. "That points to a security failing at that hospital, but then they aren't that different from 99% of companies out there," he said.

- See: *Misdirected spyware infects Ohio hospital,* *Computer World* - September 17, 2009

Computer World also reports that mobile devices are increasingly vulnerable to this form of infection:

> A security researcher showed ways to spy on a Blackberry user during a presentation Wednesday, including listening to phone conversations, stealing contact lists, reading text messages, taking and viewing photos and figuring out the handset's location via GPS.
>
> A small piece of software able to conceal itself by not appearing on the Blackberry's application menu, nor taking up much memory space nor using much processing power, can allow a hacker to do all kinds of things.
>
> …Spyware on a Blackberry could intercept a phone call and let the hacker listen in, or even let the hacker listen to a meeting the victim is sitting in on. By silently answering the victim's phone, then turning on the speakerphone, the spyware could allow the hacker to overhear the meeting. It could also forward incoming and outgoing text messages to the hacker, and even enable the hacker to write messages from the victim's Blackberry, or run up the victim's phone bill by making international calls.
>
> The hacker could also program the spyware to have the handset's camera take pictures every 10 seconds, for example, to see find out the victim's location.

- See: *Careless downloading makes Blackberry users spy targets* – *Computer World*, October 7, 2009

Social Media and Web 2.0

Social media sites such as *Facebook* and *Twitter* are among the internet's fastest growing services. Not surprisingly, they are having their fair share of security glitches, and increasingly, are among the favoured targets of cybercriminals, whistle-blowers and mischief-makers alike.

Confidential data may, by definition be incompatible with social media, but our clients increasingly use sites like *Facebook* and *LinkedIn* to communicate with us for professional purposes.

Social media poses enormous document retention issues for professionals. It is difficult to save text messages, chat dialogues and video communications sent via these sites.

They are prone to impersonation, provide a wealth of useful material for identity thieves, have circulated their fair share of viruses and Trojans – and they are here to stay. As professionals increasingly utilize social media for marketing and communications purposes, our clients will take the initiative to expand the use of social media functions in their dealings with us. Thus it is important to be aware of their security issues.

The following recent reports, excerpted below, will illustrate a few of the security challenges of Web 2.0

- *Facebook security breach gives users admin privs on corporate pages* - *Gadgetell.com,* March 29, 2009 – "A Facebook user discovered that a security glitch gave him administrative control over several corporate pages, including those of Microsoft, American Airlines, and Southwest Airlines. The glitch gave him complete control over the pages."

- *In Our Inbox: Hundreds Of Confidential Twitter Documents* - *Techcrunch,* July 14, 2009 – "Here's a dilemma: The guy ("Hacker Croll") who claims to have accessed hundreds of confidential corporate and personal documents of Twitter and Twitter employees, is releasing those documents publicly and sent them to us earlier today. The zip file contained 310 documents, ranging from executive meeting notes, partner agreements and financial projections to the meal preferences, calendars and phone logs of various Twitter employees."

- Social Networks Leaking Users Data To Tracking Sites- WebProNews- August 24, 2009 – "…social networking sites able to transmit unique identifier to third parties allowing a users specific web browsing habits to be tracked and traced back to the user. 'Tracking sites don't have the ability to know if, for example, a site about cancer was visited out of curiosity, or because the user actually has cancer,' said Wills. 'Profiling is worrisome on its own, but inaccurate profiling could potentially lead to issues with employment, health care coverage, or other areas of our personal lives.'"

Other Recent Security Headlines

- *Man charged with infecting 3,000 computers – MSNBC.com,* August 13, 2009 – "A 20-year-old Australian man has been charged with infecting more than 3,000 computers around the world with a virus designed to capture banking and credit card data, police said Thursday."

- *The Biggest Security Hole on the Web? – WebProNews,* August 13, 2009 – "Two weeks ago, Adobe released a critical patch for Flash Player and Acrobat Reader. According to online security company Trusteer, about 80% of users are still vulnerable, and perhaps more startling, the company views this as being possibly the biggest security hole on the Internet today… "

***The Cloud* - E-Discovery Challenges and LSUC and LawPro Compliance**

Several authors have commented on the difficulties of maintaining, compiling and accessing remotely-housed *Cloud* data for disclosure in e-discovery processes. A recurring issue is that *Cloud* and Web 2.0 computing is not adequately optimized to export user data for offline uses.

A recent article by Craig Bell discussed the many complexities encountered in attempting to comply with a court order requiring that he gather and produce contents of litigants' webmail folders. He placed particular emphasis on the difficulties encountered in downloading and copying email subfolders, noting the need to create elaborate "work-arounds" to comply with the Order.

- See: *Yahoo! Let My E-Mail Go!* - *Law.com - Newswire*, Sept 24, 2009

The discussion may be equally applicable to the challenges faced by lawyers who use online services in ensuring that complete copies of all file contents, including metadata, are maintained. This raises professional compliance concerns that must be addressed if *the Cloud* is to become a destination of choice for the legal profession.

Homeland Security and US Domestic Surveillance

While an analysis of American domestic surveillance it is well beyond the ambit of this paper (and the expertise of the writer), it is well worth a brief footnote.

The specific policies and practices of the U.S. Government with respect to domestic surveillance, data mining, data collection and data retention are quite properly classified. As a consequence, there is considerable mystery as to the scope and nature of such surveillance.

Suffice to say that lawyers in *the Cloud* should be aware of the existence of such programmes and carefully consider their implications with respect to data housed at servers in nations where such policies may be in place.

Conclusion:

The litany of security concerns, mishaps and challenges documented in this paper must militate against any overly-enthusiastic embrace of *the Cloud* by the legal profession – at least for now.

Practitioners, however, should resist any false sense of security arising from the limited protections represented by their current in-house, local systems and software.

In or out of *the Cloud*, personal security habits are the greatest predictor of information safety.

In spite of the significant threats discussed in this paper, *the Cloud* also offers added layers of protection for data, through redundant storage, automated security patches and upgrades, and overall reliability of access.

Such discussions aside, however, the bottom line, however, is that *the Cloud's* time is – or will soon be - upon us.

If the legal profession's history of tentative, but eventual adaptation of new technologies is any guide, we will slowly incorporate *the Cloud* into our practices. As the *Cloud's* popular appeal increases and its track-record on security stabilizes, our clients will increasingly embrace these services and demand that we do so as well.

Even if nothing does last forever online, this next generation of services and tools has arrived.

Software as a service and *the Cloud* will increasingly tempt our profession with increased efficiencies, convenience and functionality. It is the *trend to watch* in our profession's digital future, now just ahead.

And it will continue to be so - until the next 'breakthrough,' that is.

- Garry J. Wise, Toronto
- October 12, 2009

Suite 310 20 Holly Street Toronto, Ontario, Canada M4S 3B1 $ Telephone: (416)972-1800 Facsimile: (416)972-1065
Email: gwise@wiselaw.net Visit our website: www.wiselaw.net