ETHICAL CONSIDERATIONS IN THE USE OF TECHNOLOGY IN THE PRACTICE OF LAW[1]

I INTRODUCTION

1. Attorneys tend to be very conservative and generally are slow to change ingrained practices and procedures. However we live in a very dynamic interactive, interoperable, always on world where all professions are being called on to modernise to better serve the needs of society in general and clients in particular.

2. In the late 20th century having a fax machine, PBX system, desk top computer, photocopier, laptop and PDA were hallmarks of a technologically savvy lawyer and law practice. In the 21st century having a Scanner, law practice website with downloadable information, Facebook Page and Blog, Twitter handle, and Smartphone are signs of a technologically savvy lawyer and law practice.

3. Lawyers who are slow to adopt new technologies are sometimes perceived as dinosaurs on the brink of extinction. Indeed the argument has been made that the failure of an attorney to use technology can create ethical issues because the lawyer by avoiding technology may not be acting in the best interest of the client[2].

> "Many attorneys consider modern technology bothersome, even intimidating. As a result, some have managed to keep technology at bay. Lawyers will find that road increasingly difficult to follow—particularly if they want to stay competitive. In fact, doing so could

---

[1] Prepared by Nicole Foga, Attorney-at Law, Chairman Telecommunications Broadcasting Technology Committee, April 2013

[2] An Attorney Shall Act in the Best interest of His Client - Canon IV of the Legal Profession (Canons of Professional Ethics) Rules, 1978

> create ethical issues for you and your firm. You have an obligation to provide effective representation to your clients at a reasonable cost. If technology allows you to work more efficiently and at a lower cost, but you decide not to use it, you have arguably breached an ethical duty to your client. How can you justify spending five hours researching a memorandum of points and authorities using books when you could do the same research in 20 minutes online? Certainly, your clients would not care if you only billed for the 20 minutes, but that strategy will likely make it difficult to continue to pay your bills. If you make it your practice to charge for the five hours, your clients will likely care and, moreover, so might your state bar. Your clients will likely also care if you did not find a recent decision that could have helped their case available online but not yet available to you in the advance sheets for use in a physical library."[3]

4. It is undeniable that the use of Information and Communication Technologies (ICTs) can increase an attorney's competitive edge, maximize efficiencies in practice management and improve the quality of legal service delivery. Why wait until your client is in Jamaica to update them on their legal matters and receive instructions when documents can be exchanged and instructions obtained over the Internet. Indeed, in today's networked world lawyers are often retained by clients without ever physically meeting them. Why waste valuable time at the Office of the Registrar of Companies when some due diligence can be conducted online? Why go to the National Land Agency (NLA) to obtain a copy of a Title when the Title can be downloaded from the NLA website? Why purchase magazines, journals and books that need to be shipped to Jamaica and cleared through Customs when digital copies are accessible online.

5. It is important to recognize that notwithstanding the forgoing benefits of ICTs, digital solutions are often twin edge swords. If we strip away the

---

[3] http://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/road_warrior_technology_mobile_lawyer_all_us.html **(Date accessed April 10, 2013)**

tantalizing speed and efficiency of technology we are forced to grapple with trust and confidentiality issues spawned by the relative anonymity of the Internet, the ease of access to files and ability to store and reproduce perfect copies of digital files.

6. While all users of the Internet are faced with these issues, Attorneys need to be particularly aware of them in light of the Canons of the Profession and the new emerging ethical issues brought into play by ICTs.

7. Today, Attorneys routinely store sensitive client information in digital format on computers at the office and at home, on smartphones and other personal mobile devices, communicate with clients via e-mail and maintain an online presence through websites and social media. What steps are taken to ensure that the information is secure? Are sensitive files encrypted and/or password protected? When is the attorney/client relationship established via e-mail communication? Can merely responding to an online query create a lawyer client relationship or amount to an inference that the legal advice is not restricted to the jurisdiction in which the attorney is licensed to practice? These are some of the social and ethical issues attorneys embracing technology must consider.

8. The following Canons require special consideration and analysis when Attorneys utilize ICTs:

> ***Canon I - An Attorney Shall assist in Maintaining the Dignity and Integrity of the Legal Profession and Shall Avoid even the Appearance of Professional Impropriety.***
>
> ***Canon II - An Attorney Shall not indulge in or assist in any Unauthorised, Improper or Unprofessional practice.***
>
> ***Canon IV - An Attorney shall Act in the Best Interest of His Client and Represent Him Honestly, Competently and Zealously within the bounds of the law. He shall preserve the Confidence of his Client and avoid conflicts of interest.***

Canon VI - an Attorney has a duty to maintain a Proper Professional Attitude towards His Fellow Attorneys

9. The Internet facilitates a feeling of community and encourages instantaneous commentary whether through blogs, twitter or responses to online articles or features. Attorneys need to be circumspect in their e-mail communications and what they post on the Internet, always being mindful of who has access to the e-mails and postings. Comments in an e-mail and online postings intended to be casual private social commentary and not meant to be construed as being delivered in a professional capacity can still have the unintended consequence, if it is available in the public domain, of breaching Canons I, II and VI.

10. It is a common practice for persons to be copied on e-mails and for e-mails to be forwarded. It is not unusual for an e-mail to be distributed with long e-mail trails. Attorneys need to be vigilant that e-mails exchanged between attorney and client are not inadvertently forwarded or copied to opposing counsel. Exercise extreme caution in using the "reply all" function of e-mail programs.

11. It is also common practice when a number of attorneys are working on a particular contract to share files and use tracked changes when editing documents. It is important that confidential material noted as comments are properly removed for the document before being shared with opposing counsel. Metadata[4] in word documents can provide confidential information if not properly removed. [5]

---

[4] Metadata is data about data. It is the descriptive information about a file that is embedded in the file and which it is relatively easy to reveal. It reveals such information as: Time and date of creation of file; Creator or author of the data; Location on a computer network where the data were created.

[5] For more information on the ethical issues related to Metada see *The Ethical (and Practical) Pitfalls of Metadata By Michael Commins, Paralegal.* http://www.mlslawyers.com/metadata.htm

12. Attorneys who are Road Warriors i.e. Attorneys who carry their office with them whether by carrying client files and other confidential information on their Smartphones, USB drives, Ipad, Blackberry Playbook and who use blue tooth technology and are always looking to connect to wireless networks, run the risk, if the devices are lost or stolen or their communication intercepted, of breaching Canon IV. Failure to put in security procedures to prevent unauthorized access to confidential client material could amount to professional negligence which would be exacerbated by the absence of any reasonable back up system.[6]

II SOCIAL MEDIA PITFALLS

13. Social Media is defined by Wikipedia (free online encyclopaedia used by millions worldwide) as:

> "The means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks. Andreas Kaplan and Michael Haenlein define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content. Furthermore, social media depend on mobile and web-based technologies to create highly interactive platforms through which individuals and communities share, co-create , discuss, and modify user-generated content. It introduces substantial and pervasive changes to communication between organizations, communities and individuals. Social media differentiates from traditional/industrial media in many aspects such as quality, reach, frequency, usability, immediacy and permanence. There are many effects that stem from internet usage. According to Nielsen, internet users continue to spend more time with social media sites than any

---

[6] See : Best Free File Encryption Utility http://www.techsupportalert.com/best-free-file-encryption-utility.htm ; or 5 Best Free USB Encryption Software by Kripa May 12, 2010; or http://www.ilovefreesoftware.com/12/featured/5-best-free-usb-encryption-software.html ; or Five Best File Encryption Tools. http://lifehacker.com/5677725/five-best-file-encryption-tools (All sites Accessed April 10, 2013)

> other type of site. At the same time, the total time spent on social media in the U.S. across PC and mobile devices increased by 37 percent to 121 billion minutes in July 2012 compared to 88 billion minutes in July 2011." [7]

14. The International Telecommunications Union considers social media to be transformational in how individuals and businesses will operate on the internet.

> "Historically, it used to be enough to have an online presence on the Internet for the one-way broadcasting and dissemination of information. Today, social networks such as Facebook and Twitter are driving new forms of social interaction, dialogue, exchange and collaboration. Social networking sites (referred to more broadly as social media) enable users to swap ideas, to post updates and comments, or to participate in activities and events, while sharing their wider interests. From general chit-chat to propagating breaking news, from scheduling a date to following election results or coordinating disaster response, from gentle humour to serious research, social networks are now used for a host of different reasons by various user communities.
>
> Social networking services are not just bringing Internet users into fast-flowing online conversations – social media are helping people to follow breaking news, keep up with friends or colleagues, contribute to online debates or learn from others. They are transforming online user behaviour in terms of users' initial entry point, search, browsing and purchasing behaviour. Some experts suggest that social media will become the Internet's new search function – predicting that people will spend less time navigating the Internet independently and instead search for information or make decisions based on "word-of-mouth" recommendations from their friends, the so-called "friend-casting". In the process, social media are changing users' expectations of privacy, acceptable online behaviour and etiquette – fast."[8]

15. Social Media Sites can be divided into 6 substantive categories:

---

[7] http://en.wikipedia.org/wiki/Social_media (date accessed April 10, 2013)

[8] http://www.itu.int/net/itunews/issues/2010/06/35.aspx (Accessed April 10, 2013)

"**Social Networks** - Services that allow you to connect with other people of similar interests and background. Usually they consist of a profile, various ways to interact with other users, ability to setup groups, etc. ***The most popular are Facebook and LinkedIn.***

Bookmarking Sites - Services that allow you to save, organize and manage links to various websites and resources around the internet. Most allow you to "tag" your links to make them easy to search and share. ***The most popular are Delicious and StumbleUpon.***

Social News - Services that allow people to post various news items or links to outside articles and then allows it's users to"vote" on the items. The voting is the core social aspect as the items that get the most votes are displayed the most prominently. The community decides which news items get seen by more people. ***The most popular are Digg and Reddit.***

Media Sharing - Services that allow you to upload and share various media such as pictures and video. Most services have additional social features such as profiles, commenting, etc. ***The most popular are YouTube and Flickr.***

Microblogging - Services that focus on short updates that are pushed out to anyone subscribed to receive the updates. ***The most popular is Twitter.***

Blog Comments and Forums - Online forums allow members to hold conversations by posting messages. Blog comments are similar except they are attached to blogs and usually the discussion centers around the topic of the blog post. ***There are MANY popular blogs and forums."***[9]

16. Social media sites should be used by attorneys with extreme caution giving full consideration to the Canons of the profession. Attorneys should avoid:

(i) Discussing cases online without client's consent

(ii) Criticising clients, attorneys or judges online

(iii) Tweeting or blogging about matters that are sub-judice

---

[9] http://outthinkgroup.com/tips/the-6-types-of-social-media (date accessed April 10, 2013)

(iv) Obtaining information on opposing parties by 'friending' on Facebook

(v) Being 'friends' of judges on Facebook who they appear or may appear before.

III SCAMS TARGETTING ATTORNEYS

Cheque Fraud – Client Solicitation online

17. An unsolicited e-mail comes from a potential "client" that seeks the representation of the attorney in a debt recovery or divorce settlement matter. The "client" requires legal representation and has carefully selected the attorney as being trustworthy. A written fee agreement may be signed and in some instances a substantial advance fee may even be agreed.

18. The matter appears simple and straight forward: collect a cheque from the debtor who has suddenly agreed to pay up to avoid litigation, deposit the cheque in the attorneys trust account, deduct professional fees and then wire the money to the "client".

19. The cheque looks legitimate, may appear to be drawn on a large, well known bank, and may contain little or no clues as to its fraudulent nature. Shortly after the cheque is deposited the targeted attorney will receive a phone call, text message or email from the "client" shortly expressing urgency in having the proceeds wired to the "client". The attorney persuades the bank to speed up the clearance process and the money is wired to the "client's" foreign bank account. Sometime after the bank named on the purported cashier's check will dishonour and return it as a counterfeit/fraudulent item. The "client" cannot be found. The attorney's bank proceeds to debit the attorney's account for the entire amount of the dishonoured check.

20. An emerging variation of this involves the criminals orchestrating the contact with the targeted attorney through an existing and legitimate client of the firm.

Example of E-Mail Solicitations to be wary of:

Example I

Subject: URGENT collection matter

Dear Counsel,

I received your contact information from a business associate. I am currently searching for a reputable attorney that can assist our company with an urgent matter, and all future matters we may need assistance with.

To briefly explain the situation, one of our customer/supplier's are currently behind in payment. We have given plenty of time and opportunity for them to settle the invoice, but to no avail. I'm hoping, with your credentials, you are able to assist me.

Kindly email me at : marylee@hvsteelco.com

Sincerely, Mrs. MARY LEE
Hunan Valin Steel Co., Ltd
Main Tower of Valin Garden, No. 222,
Xiangfu West Road, Tianxin District,
Changsha, Hunan, China 410004
Email: marylee@hvsteelco.com

Basic Internet Search revealed that: Hunan Valin Steel Co., Ltd. (SZSE: 000932) is based in Changsha, Hunan, primarily engaged in the smelting, manufacture and sale of iron and steel products, as well as nonferrous metal products.
But note its website address is http://www.valin.cn/2009en/

HVsteel Co is completely different. An internet search revealed the following:

H V Steel Co has no known officers.
Filings: Domestic For-Profit Corporation (TX - Inactive)
Source: Texas Secretary of State last refreshed 3/13/2013

If we look at the ***who is*** record for the domain name hvsteel.co we find:
Domain Name..... hvsteelco.com
Creation Date..... 2012-09-27
Registration Date.... 2012-09-27
Expiry Date..... 2013-09-27
Tracking Number..... 1748050167_DOMAIN_COM-VRSN

Organisation Name.... MARY LEE
Organisation Address. PO Box 61359
Organisation Address. Sunnyvale
Organisation Address. 94088
Organisation Address. CA
Organisation Address. US

Example II [10]

From: Steven Larsen <stevenl@ite.net>
Date: Wed, Jun 1, 2011 at 3:41 PM
Subject: I need a commercial litigation lawyer
To:

I need a commercial litigation lawyer to handle a collection matter, I will also need a referral if this is not your line of practice. Thank you as I look forward to your response soonest.

Sincerely,
Larsen.
– –

From: Steven Larsen <stevl1990@hotmail.com>
Date: Thu, Jun 9, 2011 at 4:24 PM
Subject: RE: I need a commercial litigation lawyer
To: ahall@twincitiesfirm.com

Thanks for your reply. I represent Steven Lawson Tex Co Ltd based in United Kingdom. We got your contact information from the online Lawyers Directory as a result of our search for reliable firm to provide legal services as requested.

We request your representation to counsel us in litigation and enable us collect a debt owed to us in the amount of $900,000.00USD by a delinquent seller in your jurisdiction. We are of the opinion that once our presence is established in your state via a legal representative, our seller will have no option but comply with payment request and accompanied with legal action and litigation will push for the accounts to be paid to effectively.

We believe that a normal scenario will require a phone call or demand letter from you to our seller if your services is retained and litigation should be applied as a last resort.

We understand the concept of running a conflict check that is why we are providing our delinquent seller located in your state for your conflict check and to enable you present to us your retainer agreement for your services.

Falconer's Cleaners & Laundry,
1229 E Lake Street
Minneapolis, MN 55407-1620

We will like to have a telephone conference with you on this issue as to let you know further details of this transaction.

---

[10] http://minnesotaattorney.com/scams-targeting-attorneys/ (Date accessed April 9, 2013)

We happened to have place an order of Machinery Equipment worth $1,800,000.00, and they demanded we pay 50 percent of the funds before delivering our products. Payment to the seller was made in January of 2011 and our calculation shows that delivery is above three Months late, for the regular purchase agreement requires seller to effect goods not later than 60 days upon payment or legal action may be enforced if delivery delay exceeds 90 days.

It will be very helpful if we receive your retainer agreement for review. This will enable our board decide on the conditions of the retainer in our next board meeting. Also once we have reviewed your agreement I will forward you supporting documents i.e., proof of payment, sales invoice, wire transfer slip. This will enable your firm start working on this case. I will also call you to follow up on this matter once your firm has agreed to take on this case.

We thank you for your business as we look forward to your prompt response.

Sincerely,
Steven Larsen.
President
Larsen Fabrics Limited
19-23 Grosvenor Hill,
London W1K 3QD
Tel:+447045706686
Fax:+448447747720

Example III[11]

From: Kevin Brady <kevin.brady28@yahoo.co.uk>

Date: Thu, Oct 21, 2010 at 3:23 PM

Subject: CASE DETAILS

To: Aaron Hall <ahall@twincitiesfirm.com>

Dear counsel,

Thank you for your earnest response. Let me start by introducing the company I represent. Channel Electronics and Security Limited are acknowledged security and electrical experts throughout United Kingdom, it's authorized to cooperate with foreign individuals and partners for a comprehensive range of security solutions for domestic and commercial premises in the European regions and other parts of the world. We export and Import some of our products in North America and Europe.

We request your representation to counsel us in litigation and enable us collect a debt owed to us by a delinquent seller. We do appreciate your time in reviewing our request and we will do everything possible to insure a smooth and hitch free business relationship. We are ready to work with you to achieve our goal as the importance of your services cannot be over emphasized.

---

[11] Ibid

We are of the opinion that once our presence is established in your state via a legal representative our seller will have no option but comply with payment request and accompanied with legal action and litigation will push for the accounts to be paid attention to effectively.

We believe that a normal scenario will require a phone call or demand letter from you to our seller if your services is retained. Although we believed that litigation should be applied as a last resort as we intend to preserve the relationship we have with our seller. Though we do hope not to resort to litigation unless all other options are exhausted but we will like the comfort of knowing that the option is available and letting our seller know that litigation may be enforced if the option becomes necessary.

We understand the concept of running a conflict check that is why we are providing our delinquent seller located in your state for your conflict check and to enable you present to us your retainer agreement for your services.

Allied Electronics Inc,

6120 EARLE BROWN DR

BROOKLYN CENTER , MN 55430.

This particular seller owes approx. $950,720.00 and the delivery is overdue as our regular purchase agreement requires seller to effect goods not later than 60 days upon payment or legal action may be enforced if delivery delay exceeds 90 days. We happened to have placed an order of enclosures, racks and cabinet materials worth $1,901,440.00, and they demanded we pay 50 percent of the funds before delivering our products. Payment for this seller was made in 10th February of 2010 and our calculation shows that delivery is a Months late.

It will be very helpful if we receive your standard retainer agreement. This will enable our board decide on the conditions of the retainer in our next board meeting. Also once we have reviewed your agreement I will forward you supporting documents i.e., proof of payment, sales invoice, so your firm can start working on this case. It's not my company policy to give out documents when we have not agreed on retaining your firm.

We thank you for your business as we look forward to your prompt response.

Sincerely,

Mr Kevin Brady
Business Executive
Channel Electronics and Security Ltd
23 Avon Riverside Est, Victoria Road
Avonmouth Bristol BS11 9DB
Land Tel-+44 7526305058
Mobile-+4470457526952,+447045733570
Fax-+441173376725
kevinb@ceasltd.co.uk
kevin.brady28@yahoo.co.uk
www.ceasltd.co.uk

Avoiding Online Scams

22. Tips to avoid these types of schemes[12]:

1. Carefully scrutinize unsolicited email/phone calls from individuals or entities with whom you have no prior dealings requesting your services, particularly if the email/phone calls originate from a foreign country.

2. Take steps to independently verify:

    a. the identify of the "client" .

    b. the information provided by your "client" including the accuracy and genuineness of the information contained in the solicitation including phone number and addresses.

3. The presence of numerous typos and/or variations of well known business is often a hint that the solicitation is not bona fide.

4. Be suspicious of a solicitation that offers a relatively large fee or commission for little or no work or that appears outside of your usual practice areas.

5. Don't jump the gun. Wait until the confirmation is obtained from the bank that the monies deposited have been cleared in accordance with bank policy

---

[12] https://www.mtb.com/customerservice/securitycenter/Pages/attorney-check-scams.aspx (date accessed April 9, 2013)

6. Educate your staff to be on the lookout for these types of schemes.

7. Periodically review enforcement websites for information on current fraud schemes contact the TBTC Committee for assistance.

8. If you have doubts concerning the validity of a cheque you received, contact the institution on which the cheque is drawn to request confirmation.

9. When undertaking representation of an existing client, be on the lookout for any seemingly unusual facts or circumstances, including those described herein, existing between your client and their purported client.

IV CLOUD COMPUTING - PITFALLS

23. Cloud computing is being advertised in Jamaica as substantially cutting costs to businesses and all three telecom providers offer or have stated they intend to offer cloud based services. Sole practitioners and small firms may be giving active consideration to using cloud computing services to cut costs but there are significant ethical challenges that must be addressed.

24. The National Institute of Standards and Technology (NIST), which falls under the US Department of Commerce defines Cloud Computing as:

> " a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of

five essential characteristics, three service models, and four deployment models."[13]

25. There are five essential characteristics to Cloud Computing.

" ***On-demand self-service.*** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service."[14]

---

[13] Page 2, **The NIST Definition of Cloud Computing:** Recommendations of the National Institute of Standards and Technology Peter Mell and Timothy Grance **Special Publication 800-145, September 2011.**

[14] Ibid

26. There are three services models related to Cloud Computing: *Software as a Service (SaaS); Platform as a Service (PaaS). Infrastructure as a Service (IaaS)*. This paper will only focus on SaaS:

> "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings".[15]

27. The use by lawyers of SaaS has already been the subject of an ethics opinion in the USA. The Committee on Ethics and Practice Guidelines of THE IOWA STATE BAR ASSOCIATION wrote the President of the Association on September 9, 2011 in response to a request to "address whether a lawyer or law firm may utilize what is known as "software as a service" commonly referred to as "SaaS".

28. The Committee in its Opinion Stated the following:

> "Because SaaS involves storing client information on computer servers that are not owned and operated by the lawyer or law firm, lawyers have questioned whether SaaS can be used in light of Iowa Rule of Professional Conduct 32:1.6 Comment [17] 2
>
> *Rule 32:1.6 [Comment 17] states:*
> *[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the*

---

[15] Ibid.

lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

We believe the Rule establishes a reasonable and flexible approach to guide a lawyer's use of ever-changing technology. It recognizes that the degree of protection to be afforded client information varies with the client, matter and information involved. But it places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly.

Access to stored data and data protection should be taken into consideration when performing due diligence. Whatever form of SaaS is used, the lawyer must ensure that there is unfettered access to the data when it is needed. Likewise the lawyer must be able to determine the nature and degree of protection that will be afforded the data while residing elsewhere.

It is beyond the Committee's ability to conduct a detailed information technology analysis regarding accessibility and data protection used by the presently available SaaS services. Even if we had that ability our analysis would soon be outdated. Instead we prefer to give basic guidance regarding the implementation of the standard described in Comment 17.

We suggest that lawyers intending to use SaaS, or other information technology services that store the lawyer's work product and client information on servers that are not owned by the lawyer, should ask the following questions:

1. *Access:* Will I have unrestricted access to the stored data? Have I stored the data elsewhere so that if access to my data is denied I can acquire the data via another source?

2. *Legal Issues:* Have I performed "due diligence" regarding the company that will be storing my data? Are they a solid company with a good operating record and is their service recommended

by others in the field? What country and state are they located and do business in? Does their end user's licensing agreement (EULA) contain legal restrictions regarding their responsibility or liability, choice of law or forum, or limitation on damages? Likewise does their EULA grant them proprietary or user rights over my data?

3. Financial Obligation:
What is the cost of the service, how is it paid and what happens in the event of non-payment? In the event of a financial default will I lose access to the data, does it become the property of the SaaS company or is the data destroyed?

4. Termination:
How do I terminate the relationship with the SaaS company? What type of notice does the EULA require. How do I retrieve my data and does the SaaS company retain copies?

V. CONCLUSION

29. There are no easy answers to the ethical issues raised by the use of ICTs and we cannot turn back the digital hands of time. Our society and indeed the whole world is moving in the direction of transformation into dynamic Knowledge Based interconnected societies. While the tools used to practice law are changing and will continue to change as our society modernises the ethical and social responsibilities and duties of attorneys grounded in centuries of tradition are immune to technological alterations.

END OF PART ONE

ADRESSING ETHICAL CONSIDERATIONS RELATED TO ICTS

– OPINIONS FROM OTHER JURISDICTIONS

UNITED STATES OF AMERICA

I THE IOWA STATE BAR ASSOCIATION - Committee on Ethics and Practice Guidelines

Data Protection
Lawyers intending to use SaaS should also perform due diligence regarding the degree of protection that will be afforded the data:

1. Password Protection and Public Access:
Are passwords required to access the program that contains my data? Who has access to the passwords? Will the public have access to my data? If I allow non-clients access to a portion of the data will they have access to other data that I want protected?

2. Data Encryption:
Recognizing that some data will require a higher degree of protection than

Lawyer's Use of Information Technology Due Diligence Services
The Committee recognizes that performing due diligence regarding information technology can be complex and requires specialized knowledge and skill. This due diligence must be performed by individuals who possess both the requisite technology expertise and as well as an understanding of the Iowa Rules of Professional Conduct. The Committee believes that a lawyer may discharge the duties created by Comment 17 by relying on the due diligence services of independent companies, bar associations or other similar organizations or through its own qualified employees.

II ALABAMA

ETHICS OPINION 2010-02 Retention, Storage, Ownership, Production and Destruction

What are the ethical considerations relating to electronic files?
The practice of law today often requires legal documents and many other components of a client's file to be converted to, created, transmitted, stored, and reproduced electronically. Moving from "the paper chase" to "the paperless office" presents practical concerns. Converting existing paper files to electronic

format is usually accomplished by "scanning" the paper file, which converts it to a format that can be stored, transmitted, and reproduced electronically.

When paper files are converted to electronic format, destruction of the paper file is not without limits or conditions. Even after Category 1 documents are scanned and converted to electronic format, the lawyer cannot destroy the paper Category 1 document. After scanning and conversion, Category 2 and 3 documents may be destroyed, but the best practice is to follow the procedure used for ordinary paper documents.

Like documents that are converted, documents that are originally created and maintained electronically must be secured and reasonable measures must be in place to protect the confidentiality, security and integrity of the document. The lawyer must ensure that the process is at least as secure as that required for traditional paper files. The lawyer must have reasonable measures in place to protect the integrity and security of the electronic file. This requires the lawyer to ensure that only authorized individuals have access to the electronic files. The lawyer should also take reasonable steps to ensure that the files are secure from outside intrusion. Such steps may include the installation of firewalls and intrusion detection software. Although not required for traditional paper files, a lawyer must "back up" all electronically stored files onto another computer or media that can be accessed to restore data in case the lawyer's computer crashes, the file is corrupted, or his office is damaged or destroyed.

A lawyer may also choose to store or "back-up" client files via a third-party provider or internet-based server, provided that the lawyer exercises reasonable care in doing so. These third-party or internet-based servers may include what is commonly referred to as "cloud computing." According to a recent ABA Journal article on the subject, "cloud computing" is a "sophisticated form of remote electronic data storage on the internet. Unlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored 'in the cloud' is kept on large servers located elsewhere and maintained by a vendor." Richard Acello, *Get Your Head in the Cloud*, ABA Journal, April 2010, at 28-29.

The obvious advantage to "cloud computing" is the lawyer's increased access to client data. As long as there is an internet connection available, the lawyer would have the capability of accessing client data whether he was out of the office, out of the state, or even out of the country. In addition, "cloud computing" may also allow clients greater access to their own files over the internet. However, there are also confidentiality issues that arise with the use of "cloud computing." Client confidences and secrets are no longer under the direct control of the lawyer or his law firm; rather, client data is now in the hands of a third-party that is free to access the data and move it from location to location. Additionally, there is always the possibility that a third party could illegally gain access to the server and confidential client data through the internet.

However, such confidentiality concerns have not deterred other states from approving the use of third-party vendors for the storage of client information. In Formal Opinion No. 33, the Nevada State Bar stated that:

> *"[A]n attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney's direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services. If, for example, the attorney does not reasonably believe that the confidentiality will be preserved, or if the third party declines to agree to keep the information confidential, then the attorney violates SCR 156 by transmitting the data to the third party. But if the third party can be reasonably relied upon to maintain the confidentiality and agrees to do so, then the transmission is permitted by the rules even without client consent."*

In approving on-line file storage, the Arizona State Bar noted in Formal Opinion 09-04 that:

> "[T]echnology advances may make certain protective measures obsolete over time. Therefore, the Committee does not suggest that the protective measures at issue in Ethics Op. 05-04 or in this opinion necessarily satisfy ER 1.6's requirements indefinitely. Instead, whether a particular system provides reasonable protective measures must be "informed by the technology reasonably available at the time to secure data against unintentional disclosure." N.J. Ethics Op. 701. As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."

In their opinions, the Bars of Arizona and Nevada recognize that just as with traditional storage and retention of client files, a lawyer cannot guarantee that client confidentiality will never be breached, whether by an employee or some other third-party. Rather, both Arizona and Nevada adopt the approach that a lawyer only has a duty of reasonable care in selecting and entrusting the storage of confidential client data to a third-party vendor. The Disciplinary Commission agrees and has determined that a lawyer may use "cloud computing" or third-party providers to store client data provided that the attorney exercises reasonable care in doing so.

The duty of reasonable care requires the lawyer to become knowledgeable about how the provider will handle the storage and security of the data being

stored and to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider. If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider.

In whatever format the lawyer chooses to store client documents, the format must allow the lawyer to reproduce the documents in their original paper format. If a lawyer electronically stores a client's file and the client later requests a copy of the file, the lawyer must abide by the client's decision in whether to produce the file in its electronic format, such as on a compact disc or in its original paper format.

When a lawyer discards laptops, computers, or other electronic devices, he must take adequate reasonable measures to ensure that client files and/or confidential information have been erased from those items. Failure to do so could result in the disclosure of confidential information to a subsequent user. If such disclosure occurs, the lawyer could be subject to disciplinary action for a violation of Rule 1.6 of the Alabama Rules of Professional Conduct.

III STATE BAR OF WISCONSIN

Technology: 25 Tips to Prevent Law Firm Data Breaches[16]

1. Have a strong password – at least twelve characters. No matter how strong an eight character password is, it can now be cracked in about two hours. A strong twelve-character password takes roughly seventeen years to crack. Use a passphrase you can remember e.g. password: "LoveTBTC 2013!"

2. Don't use the same password everywhere.

3. Change your passwords regularly. This will foil anyone who has gotten your password.

4. Do not have a file named "passwords" on your computer. And do not have your password on a sticky note under your keyboard or in your top right drawer (the two places we find them most often.)

---

[16] Sharon D. Nelson & John W. Simek http://www.wisbar.org/NewsPublications/Pages/General-Article.aspx?ArticleID=10212 (date accessed April 11, 2013)

5. Change the defaults. It doesn't matter if you are configuring a wireless router or installing a server operating system. In all cases, make sure you change any default values. The default user ID and passwords are well known for any software or hardware installation. Apple isn't immune either, since there are default values for their products as well.

6. Your laptop should be protected with whole disk encryption – no exceptions. Stolen and lost laptops are one of the leading causes of data breaches. Many of the newer laptops have built-in whole disk encryption. Make sure you enable the encryption or your data won't be protected. Also, encryption may be used in conjunction with biometric access. As an example, laptops require a fingerprint swipe at power on. Failure at that point leaves the computer hard drive fully encrypted.

7. Change your password frequently and don't use the same password for every website.

8. Backup media is also a huge source of data leaks – it too should be encrypted. If you use an online backup service (which means you're storing your data in the cloud), make sure the data is encrypted in both transit and storage – and that employees of the backup vendor have no access to decrypt keys.

9. Thumb drives, which are easy to lose, should be encrypted – and you may want to log activity on USB ports. It is common for employees to lift data via a thumb drive – without logging, you cannot prove exactly what they copied.

10. Keep your server in a locked rack in a locked closet or room – physical security is essential.

11. Most smartphones write some amount of data to the phone – even opening a client document may write it to the phone whether or not you save it. The iPhone is particularly data rich. Make sure you have a PIN for your phone – this is a fundamental protection. Don't use "swiping" to protect your phone – thieves can discern the swipe the vast majority of time due to the oils from your fingers. Also make sure that you can wipe the data remotely if you lose your phone.

12. Solos and small firms should use a single integrated product to deal with spam, viruses and malware. For solos and small firms, it is recommend using Kaspersky Internet Security 2012, which contains firewall, anti-virus, anti-spyware, anti-spam and much more. For larger firms, Trend Micro is recommended.

13. Wireless networks should be set up with the proper security. First and foremost, encryption should be enabled on the wireless device. Whether using Wired Equivalent Privacy (WEP) 128-bit or WPA encryption, make sure that all communications are secure. WEP is a weaker layer and can be cracked. The only wireless encryption standards that have not been cracked (yet) are WPA with the AES (Advanced Encryption Standard) or WPA2.

14. Make sure all critical patches are applied. This may be the job of your IT provider but too often, this is not done so ASK.

15. If software has gone out of support, its security may be in jeopardy – upgrade to a supported version to ensure that it is secure.

16. Control access – control who has access to your electronic systems.

17. If you terminate an employee, make sure you cut all possible access (including remote access) to your network immediately and kill their ID. Do not let the former employee have access to a computer to download personal files without a trusted escort.

18. Using cloud providers for software applications is fine **provided** that you made reasonable inquiry into their security. Read the terms of service carefully and check your state for an ethics opinion on this subject.

19. Be wary of social media applications which are now being invaded by cybercriminals. Giving another application access to your credentials for Facebook, as an example, could result in your account being hijacked.

20. Consider whether you need cyberinsurance to protect against the possible consequences of a breach. Most insurance policies do not cover the cost of investigating a breach, taking remedial steps, or notifying those who are affected.

21. Firms are encouraged to have a social media and an incident response policy. Let your employees know how to use social media as safely as possible – and if an incident happens, it is helpful to have a plan of action in place.

22. Dispose of anything that holds data, including a digital copier, securely. For computers, you can use a free product like DBAN to securely wipe the data.

23. Make sure all computers require screen saver passwords and that it gets invoked within a reasonable period of inactivity.

24. Use wireless hot spots with great care. Do not enter any credit card information or login credentials prior to seeing the https: in the URL and for remote access, use a VPN or other encrypted connection.

25. Do not give your user ID and password to anybody. This includes your secretary and even the IT support personnel.

IV AMERICAN BAR ASSOCIATION (ABA) ETHICS COMMITTEE[17]

Confidentiality and Privilege

The ABA Ethics Committee has opined that it is not reasonable to require that a mode of communication, such as e-mail, be avoided simply because interception is technologically possible, especially when unauthorized interception of the information is a violation of law.

Nonetheless lawyers may be required to keep abreast of technological advances in security as well as technological advances being developed by hackers who are seeking to steal secrets.

Social networking presents many new ways for lawyers to reveal information sometimes inadvertently.

Lapses in confidentiality can occur on a firm's website and client intake forms, in e-mails and attachments, blogs, bulletin boards, chat rooms etc.

Simply making a list of contracts public on a networking site, could disclose a confidential relationship.

The lawyers confidentiality protection duty extends to persons providing service to the client at the lawyers direction.

Means of Communication

Lawyers may need to discuss means of communication with their clients. Where for example a client uses an employee's computer system to communicate with a lawyer, claims of privilege may be lost because the employee may lack privacy rights in the system.

Creation of Unintended Attorney – Client Relationship

Websites inviting potential clients to communicate with lawyers should disclaim the existence of an attorney – client relationship except with an express agreement from the lawyer and caution prospective clients not to send a lawyer confidential information, without confirmation of an agreement to undertake representation.

---

[17] Ethics of Lawyer Social Networking – Steven C. Barnett Albany Law Review 73 Alb. L. Rev. 113 (2009)

To avoid creating implied attorney client relationship, lawyers must refrain from giving fact specific legal advice in social interactions. Some jurisdictions have crafted ethics rules specifically governing advice provided over the internet.

Thus lawyers should limit themselves to providing legal information generally on websites.

Unauthorized Practice of Law

ABA Rule 8.5 provides that a lawyer not admitted in a particular jurisdiction is subject to disciplinary authority in that jurisdiction, "if the lawyer provides or offers to provide any legal services in that jurisdiction".

Although courts in the United States have not found that operating a Website alone constitute the practice of law, some courts have held that maintaining an online presence can contribute to liability.

In California, a court held that although not physically present an out-of-state lawyer's use of telephone, fax, computer, or other modern technological means could constitute unauthorized practice of law, although the court declined to rule that a lawyer's virtual presence in California automatically amounted to practicing law.

The constant addition of social networking tools to the array of communication methods that lawyers use everyday has made it necessary for concerted thinking about the adaptation of legal ethics rules to this dynamic world where interactions between attorneys, clients and communities of social network users can become quite complicated.

Blogging and the Social Media

Lawyers should be circumspect in their participation in online public discussions. Online public discussions should be conducted with the same respect for the administration of justice required of public statements that lawyers may make in other forums and media.

CANADA

Professional Conduct and Social Media[18]

Participation in online forums can pose concerns for client confidentiality (e.g. disclosing a judgment on twitter), unintended formation of client relationship (giving advice on facebook about a specific situation without including a disclaimer); and conflicts of interest. Participation in online discussions can take the form of postings and comments to blogs, law blogs, wikis, chat rooms, Internet forums, list serves, social media, and other electronic forums and media. A lawyer's communications in online public forums are public statements that should be in conformity with the Rules/Code of Professional Conduct in the jurisdiction in which he/she practices.

In particular, lawyers who communicate in online forums should ensure that they make clear when they are writing in their professional capacity and offering legal services. In those instances, they should provide contact information, and be certain they are able to identify the person with whom they are communicating.

General best practice tips:-

- Keep personal and professional interests separate. Facebook is better suited for personal, family and friend connections.
- Proof read before you post.
- Do not give legal advice on public forums.
- Frequently monitor and update your posts as posts in one forum are usually replicated in others through trackbacks and reposts or references.
- Use the built in privacy capabilities of social networking sites, and consider limiting the access of users you are connected with.
- Remember that what you put out there is **permanent**. Everything written on the web can be traced back to its author so never write anything you wouldn't say out loud to all parties involved (whether personal or professional).
- Do not post or link to any materials that are defamatory, harassing or indecent.
- Develop a policy for employees (even if you are a solo practitioner).

---

[18] Information to Supplement the Code of Professional Conduct : Guidelines for Practising Ethically with New Information Technologies - Ethics and Professional Issues Committee Canadian Bar Association , September 2008

SCOTLAND

LAW SOCIETY OF SCOTLAND[19]

Ethical Considerations and Professionalism

The use of social media is subject to the same ethical and professional standards as all other conduct of a member of the legal profession. Individual solicitors must ensure they abide by the professional practice rules and maintain professional relationships with clients and other members of the profession.7

Social media is often designed to encourage informal communication and sharing of personal views and opinions. The nature of social media also often leads to a blurring of the distinction between public and private. Although building personal relationships and creating a personal dimension to a profile may be a good thing, care is needed to ensure that appropriate standards are met, even in a more informal environment.

Defamation may be committed through comments made online, including through social media. Tone can be much harder to convey through text based communications, and what was meant as a joke may be treated more seriously.8 Anonymity cannot be guaranteed, even when posting under a username, and members of the profession should always assume that comments may be traced back to them, and exercise appropriate discretion.

Issues around confidentiality should be carefully considered. Information made available by you to a small group in private can then be republished to a wider audience. Likewise, individuals should take care when forwarding or 're-tweeting' information to understand in what context that information was sent to them, and whether it was intended for re-publication. Once information is committed to social media a large degree of control is lost.

Professional duties such as acting in the best interest of a client remain key issues when using social media, especially given the potentially large audience who may be able to see the information posted. Other areas where members of the legal profession have specific duties include the duty to maintain respectful and courteous relationships with the courts and with other members of the profession.

The Law Society of Scotland Practice Rules 2011 covers many areas that may be relevant to online activity including:

- Advertising and approaching represented persons (rule B3)

---

[19] http://www.lawscot.org.uk/socialmediaguidance (Accessed April 10, 2013)

- Confidentiality of client matters (rule B1.6)
- Relations with courts (B1.13)
- Relations between regulated persons (B1.14)

Friends and Followers

One of the key characteristics of most social media sites is the ability to link to other users, for example by becoming a 'friend' or 'follower'. The links between different users are often publicly visible.

The impact of suggesting a relationship or interest though creating links through social media should be carefully considered. Issues such as conflict of interest may arise, with the possibility that a perception of conflict may be created even if the individual does not consider a conflict to exist. This may happen, for example, if a client notices that his or her solicitor is 'friends' with a solicitor acting for the opposing party to a case or with a judge or tribunal members involved in a case.

Creating a link with clients through accepting them as friends on a social media site should be approached with caution. Members of the legal profession should take care to consider the nature of their activity on that site - including whether it is a business or personal account - and how the client might view the solicitor's online activities and relationships, visible through the site.

Some social media platforms will show content from friends and contacts within your own 'stream' - consideration should be given to how this external content could be perceived by employers and clients, and consideration given to settings to ensure all linked information within your pages is appropriate.

Linking to other members of the legal profession should likewise be treated with common sense, and care should be taken to avoid inappropriate online communication, such as discussing a case or posting any other confidential information, and any potential or perceived conflict of interest. It is worth remembering that even 'direct messaging' (private communication between two individuals) is not necessarily secure. It should also be noted that the internet allows information to be linked together, and that issues have arisen for professionals from that. For example, a passing comment about a 'difficult client' on Twitter might be linked with the time of the tweet, and information from a public court hearing to specifically identify the client in question (as happened recently in an English disciplinary case).

Security

Most social media sites will have a range of customisable privacy settings. Members of the legal profession who use these sites should take care to familiarise themselves with these settings and to ensure that they are adjusted to provide the security and audience desired.

By being aware of who is able to see the information posted on a site, individuals can tailor their content to achieve their goals for that site. For example, a purely private profile may be best restricted with the highest privacy settings, while a business profile might benefit from being publicly discoverable and accessible. Different settings may also be used to create different views for various categories of contacts, for example by having stricter privacy settings for photographs in comparison to notes or comments.

Confidentiality will always be a key issue for all communications, particularly online. Information posted online is extremely difficult to remove, and may be accessible for a considerable period even after deleted. Great care should be taken to avoid posting any confidential or sensitive information through social media.

Many social media sites are designed to encourage people to create a profile containing considerable amounts of personal information. Care should always be taken when sharing personal information that may become publicly available. Consideration should be given to the desirability and potential consequences of making information such as current employer, office and private contact details visible so as to minimise risks such as social engineering and identity theft. Employers should also be aware of the potential for false or unauthorised profiles to be set up, which may purport to be related to the firm through use of profile information or other links.

In addition to different privacy and profile controls, each platform will have its own set of terms and conditions. Whilst these are often lengthy and complicated where social media is being used in a professional setting it is important to ensure that those using social media have read and understood the key terms and conditions of each site being used, in particular around privacy and data ownership. These terms may also contain, for example, certain conditions relating to promotion of services and interactions with other members of a site. They may also provide for rights of ownership or reuse of information and content by the owners of platform.

Personal and physical security should also be considered. Revealing a significant amount of personal information may allow clients to identify a home address and to make contact with you there, and posting information on holiday plans, if a sole principal, could indicate when an office was being left unattended for a week.

Social Media and the Law

As social media becomes an increasingly important part of everyday life, its impact on and interaction with the law is becoming clear.

As a means of communication, social media is obviously relevant in a number of different areas, including defamation.

In family law an increasing number of issues are arising in relation to contact with parents or siblings where this has been prohibited by the court but contact is maintained through social media and this has later become known. Depending on how active or passive the contact has been this can create serious issues. Solicitors may need to deal with the consequences of these actions with their clients, and it may be there is increasingly a need to proactively explain to clients the difficulties they may face if they use social media in such as way.

In relation to criminal matters the police now regularly use social media to look for comments about an offence that has been committed or to check a version of events provided by someone who has been questioned. Solicitors may need to be proactive in assessing the implications of social media in a case. There are also issues linked to stalking and higher profile issues around racist, sectarian or threatening statements.

Issues are also now frequently arising in relation to employment law, particularly in situations relating to recruitment, misconduct and dismissal. 9 Solicitors involved in drafting wills are now also increasingly having to consider the digital legacy left by an individual - be that encouraging them to leave passwords and user names with their will to allow sites that some relatives may find upsetting after death to be taken down, through to advising on ownership of things such as collections of family photographs held on social media accounts.

Another example of the internet creating a new context for legal issues is advertising. In particular, the Institute of Advertising has warned that activities such as posting positive comments or reviews, or planting viral marketing advertisements, without making it clear that the individual is acting on behalf of a business, could breach the consumer protection laws.10 Similarly the Advertising Standards Authority (ASA) and Financial Services Authority (FSA) will seek to apply their own standards and regulations to social media if applicable. Firms should consider the implications of individuals using social media for business purposes, and whether activity on personal accounts may amount to advertising or paid for content.

The law is still developing, and much remains to be seen about how the increasing use of social media will impact different areas. In the meantime, the legal profession should be aware of the potential for social media to affect a situation. For example, could a client's behaviour through social media lead to a breach of a court order restricting communication or contact? Could a client's online activity be used as evidence through statements made and locations indicated on social media sites?

Social media is also affecting law in other ways, for example in elements of bail conditions, and with the question of blogging live from courts becoming increasingly relevant.

In short, in every aspect of law and practice solicitors should increasingly be asking what new implications are bought by social media and our increasingly digital lifestyle.

Social Media in the Courts

Social media played a significant role in the English riots in August 2011. In Scotland, individuals accused of encouraging rioting through Facebook were released on bail with a condition that they did not access the internet. Live blogging from courts, including Twitter, was first allowed in a Scottish court during Tommy Sheridan's sentencing hearing in January 2011.12 'Text based communications' are generally permitted in the Supreme Court, subject to certain exceptions, for example where reporting restrictions are in place. Courts in other jurisdictions, including England, have allowed documents to be served on individuals through Facebook and Twitter where other methods were unsuccessful.

END OF PAPER