March 12, 2012

Author: Mary P. Kirwan, B.L.

Protecting Client Confidentiality in the Digital Age

Who cares?

The Bar Council cares. Client confidentiality is integral to the relationship between barrister and client.

Code of Conduct (relevant extracts: not all inclusive)

Barristers have a duty ‘not to engage in conduct’ which ‘may bring the barristers’ profession into disrepute’... or conduct ‘prejudicial to the administration of justice’... a barrister must ‘promote and protect fearlessly’... ‘their client’s best interests’... barristers have a duty to ensure their practice is ‘properly and efficiently administered’...

3.3(a): Confidentiality provision: Confidentiality is ‘a primary and fundamental right and duty of the barrister’... 3.3(f): In so far as it may be necessary to keep copy pleadings, advices or other documents, barrister have a duty to ensure the security and confidentiality of such documents. Any matter stored in electronic form should enjoy an appropriate level of encryption’.

6.2: A barrister may not make any public comment upon any case in which the barrister has been briefed or instructed or upon any of the parties involved in the case’... may not ‘cause or permit to be published... any particulars of any matters on which they have been, or are currently, engaged as barristers’.

6.13: The papers in any Brief or instructions delivered to a barrister are the property of the client... no right without consent to lend them or otherwise reveal their contents to any person...

Trust

The rationale for protecting client confidentiality is not, however, just about obeying rules and avoiding disciplinary action (a wise choice in itself): Trust, currently in short supply, underpins all

1 Copyright Mary P Kirwan 2012

Mary P. Kirwan is a qualified lawyer in Ireland, Canada and Australia. She worked as a commercial litigator and wiretap/money laundering prosecutor in Canada, where she lived for many years. She also wrote a column on data security for the Globe and Mail for several years and worked for several leading IT/data security firms, in a number of capacities, including legal, marketing and PR/media outreach. She has a MBS degree from the Michael Smurfit Graduate School of Business at UCD in Dublin (Specialty: Management Information Systems) and holds the CISSP (Certified Information Security Systems Professional) credential.

2 DISCLAIMER: This paper is for general informational purposes only. It is not intended as legal advice- or as an endorsement of any software vendor. It should not be relied upon as such. Nor is it intended to present a solution to any individual security concern. In case of doubt, or where you believe you may have a serious security issue, contact a reputable local dealer or service provider for advice and assistance. Unless you are very confident you know what you are doing, do not attempt to resolve it yourself.

1

2
relationships- and none more so than the relationship between advocate and client. You will lose it if you treat client confidentiality in a cavalier fashion, inadvertently or otherwise.

The client has a reasonable expectation that a barrister will protect his or her best interests. One does not do so by exposing sensitive information to third parties who may exploit it. If you are a devil, and you expose your masters’ client data, he or she will be unhappy with you: Carelessness and indiscretion inevitably casts one in a poor light.

**Legal privilege**

There may be legal consequences if client data is lost or exposed. There is potential for loss of legal privilege for otherwise protected information; the discovery process may be impacted negatively. You may be sued, and your professional indemnity insurance may not provide coverage.

As a practical matter, exposing sensitive information to the four winds, where it might end up in the hands of the media, or an unscrupulous adversary, may do damage that simply cannot be undone.

**Data privacy laws:** There is an increased emphasis at the EU Commission level to force data controllers and processors to report data breaches to both the data privacy commissioners and the impacted party: These trends will continue. Although barristers and solicitors are not always within scope, the law in evolving.

**Spilling the beans**

Hiding a breach of client confidentiality may be an alluring prospect to avoid personal embarrassment- in the hope it will simply ‘go away’. However, ‘staying mum’ is an undesirable although widespread practice.

Doing so may in itself constitute a breach of the Code of Conduct. In addition, silence potentially deprives a client of an opportunity to mitigate his or her losses.

**How do breaches of client confidentiality arise in the digital age?**

**Targeted attacks**

If you work on very high-value and sensitive litigation, there is a chance you will be targeted by wily, tech-savvy adversaries, who may identify you as a weak link in the security chain. In most cases, however, such people will not ‘beat themselves bloody at the firewall’- and take heroic measures to crack your military grade security- they will simply seek the easiest way in. There is always one.

Sophisticated attackers will usually prevail if you are in their sights: you must exercise reasonable caution to protect client confidentiality, but you are not expected to become the ‘Girl/Guy with the Dragon Tattoo’. Trying to bite off more than you can chew is inadvisable.

What is reasonable will depend on the circumstances, the sensitivity of the data in question and any reasonable steps taken to protect it. In most cases, following the basic steps outlined in this memo will stand you in good stead. Pleading ignorance (“I know nothing about computers”) will not.

**Carelessness**

Most of the time, data is exposed through sheer carelessness and stupidity. Common sense is an under-rated commodity.
1. **Leaving a laptop/tablet, flash drive or mobile phone in a taxi cab/nightclub** after a night on the town is invariably bad. **Consequences:** Often bad. In a criminal case, people may be killed; surveillance operations exposed and lengthy, expensive police investigations undermined.

   **Mitigation:** Software exists to encrypt files/whole drives and to remotely lock down a device when lost or stolen: It is more common at the enterprise level, but individual devices can be protected. If you encrypt data, you must protect the decryption key/process- if you can’t recover data, because you lost the key, you may be in worse shape than if you did nothing at all. **If you are computer illiterate,** don’t attempt to encrypt data without professional help.

2. **Throwing out sensitive physical data/files in the garbage** where ‘dumpster divers’ or the merely curious, homeless people, or the media can find it is also a bad idea. **Mitigation:** Shred anything remotely sensitive: Do it in the Law Library where professionals (hopefully) oversee the process. Using a cheap shredder at home may not suffice: Shredded data can be easily reconstituted unless industry standards are followed.

   **If you buy a new computer, don’t dump the old one in landfill** or give it to a charity shop without erasing the hard drive: Get help if you can’t do it yourself: Hitting ‘delete’ in MS Word does not delete files. Many security software programs now include a ‘hard’ delete programme that will do the job properly. If your data is worth a lot, or you seem like a high value target, attackers may put more effort into restoring deleted data. Data on drives that have been in a fire or ran over by a truck, can, quite often be reconstituted by professionals.

   As a general premise, the amount of effort an attacker will apply to steal data or reconstitute it will be proportionate to its value. What constitutes value may vary- politically motivated attackers may view, for instance, the public embarrassment of a government/corporation as a ‘high value’ activity. It is not always about money. Terrorists have other motivations.

3. **Talking loudly in public and general shouting one’s mouth off.** I could have made a fortune over the years from insider trading tips gleaned in airport lounges, planes, trains and restaurants/bars. I have read entire PowerPoint presentations on planes, disclosing highly sensitive data. **Mitigation:** Be silent as the grave. Discretion is the better part of valour. If you must type in public, 3M sells a privacy screen that ensures no-one but the person in front of the screen can read it.

   If you must boast about your cases, your genius trial work, how you devastated X on cross examination, how your client is an idiot and/or guilty and doomed to lose, talk to your cat or an inanimate object.

---

1 **Blackberry security:** If you do not know what you are about, you can easily ‘freeze’ your device and lose all the data.  

http://www.blackberry.com/newsletters/connection/personal/i410/checklist.shtml


http://docs.blackberry.com/en/smartphone_users/deliverables/11298/Turn_on_encryption_777804_11.jsp
4. **Social networking:** Under no circumstances should you ‘chat’, post or otherwise expose a client confidence/data on Facebook, Twitter, LinkedIn, or other social networking/internet site, or opine on a case publicly: You may be sued for libel as well as guilty of serious professional misconduct. In the UK, jurors who discussed cases on Facebook caused cases to be dismissed and/or retried. Indiscretion is also ‘cached’ in cyberspace forever: Yours may be a perpetual black mark against you.

5. **Do not misuse the property of a solicitor/client:** If you are granted access to a solicitors’ computer, don’t misplace the trust placed in you to use such access for the sole purpose of completing the work at hand: Do not tweet, post to Facebook or any internet site as any comment made by you may be traced back to the client computer: Any indiscreet comments made by you may be attributed to the (innocent) client.

6. **Do not ‘port’ your data to an insecure home computer** that your kids/spouse/neighbours use. If kids access a home PC, they can cripple, inadvertently or otherwise, all your security by, inter alia, downloading music, files, games, screensavers that are loaded with malware that overwhelms your system.

7. **Don’t leave a laptop/device filled with client data out in plain view at home** or in a hotel room where it can be stolen if you are burgled. Put it in the safe or make some effort to secure it/encrypt data. Have the data backed up, so you know what was possibly exposed, and so you can reconstitute it.

8. **Exercise great care when using public Wi-Fi or Wi-Fi in airport lounges/hotel rooms.** In most cases, this data, if not encrypted, is viewable ‘in the clear’. See below for more information.

**General principles**

The internet mirrors the real world: It is full of con artists, fraudsters, stalkers, paedophiles, deviants, and sundry cyber-criminals. Never assume that because you are ‘online’ you are somehow in a more benign environment than you would be in a strange city you don’t know very well.

Cybercriminals see you as an easy mark, and their techniques to trick you into lowering your defences are constantly evolving. If at first they don’t succeed, they will try, try again.

Cybercriminals can steal millions with the click of a mouse, from any country in the world, with little or no over-head. They also co-operate with one another; they share skills-sets and expertise. They have online communities where they train the young and uninitiated. They sell their wares (e.g. stolen credit card numbers, and personal data like social security numbers, mother’s maiden name and sensitive personal data that can help them steal someone’s identity) on websites that operate like eBay for criminals.

**Scams**

The Wide Wide Web (the ‘www’ bit) can stand for ‘Wild, Wild West’ if you don’t have your wits about you. Get rich scams (‘you have won the lotto’) and begging emails (Nigerian letter scams) are all geared to exploiting our gullibility, our desire for good news, and/or our susceptibility to hard luck stories.
If you want to give to charity, donate to a reputable charity. If you buy lotto tickets, you know how to find out if you have won: They won’t send you a pop-up on your PC telling you won 25 million in the Euro millions.

Think before you click. Treat your personal data, like credit card numbers and banking passwords the same way you guard and protect the nice earrings or diamond ring you inherited. Sensitive personal data has value to someone- and, in a worst case scenario, it can be used to impersonate you and even steal your (or your client’s) identity.

The scams used to try to defraud you are not static. The bad guys follow trends; they are very devious. In some respects, they have a fine understanding of human nature. They routinely exploit certain human weaknesses that seem constant through time and space, such as our desire to get something for nothing. We are taught that ‘there is no such thing as a free lunch’- yet hope dies eternal. This warning is doubly true in cyberspace.

Be careful of ‘free’ offers and pop-ups telling you that you must click a link to get free anti-virus software, a great ‘work from home’ job opportunity or training, a cute new screensaver, free music or lyrics, cheap medication, and so on.

Most legitimate businesses won’t spam you like that, and many of these offers are a front for attackers that want to infect your computer to spy and/or steal from you.

‘I just surf so I am fine’

Dangerous websites

Wrong. Even ‘surfing’ on Google can be dangerous. Don’t just wander onto any website in the same way you wouldn’t wander all over Dublin willy-nilly. Bad neighbourhoods exist on the net too and they can be hard to spot.

Worst site offenders include online chemists/pharmacies (never buy from them or you will be spammed for ever). Other offenders are gaming sites, celebrity sites, screensaver pop ups, music and lyric downloads, pirated music sites and porn sites.

Fake AV

Fake antivirus software, sometimes called “scareware,” is a big problem- it is malicious software designed to steal your money and information by tricking you into thinking that it is legitimate security software.

Cybercriminals mostly distribute scareware via Internet ads and popups and through poisoned search results, with the aim of making money—lots of money. One criminal group managed to make $100 million through fake antivirus scams.

Certain search terms are also more dangerous than others, as they may take you to one of the thousands of fake sites out there that are full of spyware and viruses that can infect your computer.

Privacy

As well as the security risks associated with surfing, don’t forget the privacy risks. Most commercial websites leave ‘cookies’ on your computer so they can identify you when your return- to offer and sell you stuff in a targeted manner.
In addition, although they claim they ‘do no harm’, search engines like Google store vast quantities of data. When you research a sensitive topic online, never assume you have anonymity. It is not the same as looking up a book at the local library (unless someone is looking over your shoulder) or in the privacy of your home. Just be aware that many of the people who run these giant companies are on record saying that there is” no such thing as online privacy”. Govern yourself accordingly.

The same suggestion is even more relevant on social networking sites. Whatever you type, whatever you say is out there in cyberspace, potentially to haunt you forever. Kids (and adults) – and lawyers-forget this, as they bully, defame or belittle other kids or companies (or clients) online, believing in a life without consequences. Potential employers/clients check you out on social networking sites too, to get your measure.

In addition, the defamation laws (e.g. libel and slander) apply to what you write and say online as in the real world. So, don’t Facebook, tweet or YouTube your way into the High Court- as a defendant.

Running amok

People- even lawyers- frequently lose the run of themselves online (e.g. on Facebook) doing/saying, posting things they would never do in the real world- and generally giving out way too much information.

Fraudsters have used information from Facebook users describing holidays (photos of ‘me on the beach in Ibiza’) as an opportunity to burgle their home. Photographs posted on Facebook may contain GPS indicators that criminals can use to track the location on the photograph.

A picture of a child at a school or playground might enable a paedophile pinpoint the child’s location. Cybercriminals and deviants can collate bits of information about you from public sources that enable them target you in a very specific way. Trial strategy conceivably might be revealed in this manner.

The most dangerous search terms

They change over time, but broadly speaking, ‘sex, drugs and rock n’ roll’ are constant themes.

The most dangerous search terms often revolve around beautiful women. At present, according to security companies, fans searching for “Heidi Klum” (a model) and other ‘hot’ female celebrities are at a higher risk of running into online threats designed to steal personal information.

Clicking on these sites and downloading files like photos, videos or screensavers exposes you to the danger of inadvertently downloading viruses and spyware. Spyware is malicious software that provides attackers with a way to spy on you (like a key under the mat), for instance, by logging your key strokes as you type, and/or watching you (or your kids) over your web camera.

Both these links provide an overview on the topic of dangerous search terms.


Attackers who gain access to your computer want to ‘own’ it. At best, they will steal your internet connection and use your bandwidth’. They might use your fast internet connection to launch attacks on other computers and/or they may store illegally obtained software (or worse) on it.
Your computer may become part of their ‘army’. If they can gain access to enough computers, they can create a vast network (often called a ‘botnet’) of infected computers (called ‘zombies’) to attack other computers and networks, even other governments (it’s like accumulating ammunition or weaponry for waging war: The more firepower, the better).

Email

You can get into trouble with email too. Security aside, it is best to assume your email may end up in the public domain- so be careful what you write. As stated at the outset, this admonition is even more pertinent for lawyers/barristers. Cached emails with damaging contents can reappear with horrible consequences on discovery, as Bill Gates knows to his cost.

Beware ‘phishing’ emails that seem to come from someone legitimate, asking you to go to a website (that will look real) and do something- they often purport to come from trusted sources like your bank, the government/tax office, health providers, and so on.

Don’t fall for it. Call the real thing to check if in doubt or drop into your physical branch. Remember email addresses (the ‘From’ part) can be easily faked, and it is nearly impossible to stop. Companies like banks will not (should not) contact you like this, so just don’t buy it.

Don’t click on an email from someone you don’t know, however enticing the subject heading. Don’t open attachments you don’t expect or recognize- they are huge carriers of infection.

Don’t give out your email address to every Tom Dick and Harry who wants it. If you do, the best case scenario is that you will be inundated with spam.

Throwing out stuff

As well as professional data, don’t put credit card, utility bills or anything with sensitive data on it into the green or ANY bin as garbage. Crooks may go through garbage to find this information about you.

Sharing and trusting

Don’t share PINs or passwords with anyone, even your spouse and kids. American Andy Grove (ex CEO of Intel- big computer company) once said: “Only the paranoid survive”. He had a point and this is especially true today with so much information in digital form. Older folk get robbed every day by trusted caregivers and relatives with PIN access to bank cards.

Another reason not to share this data is that if you do, and your credit/Laser card is used to rob you, the bank can hold you responsible (for ‘negligent’ behaviour) and legally refuse to reimburse you.

What can you do to protect yourself in the digital world?

Besides using common sense, you must ensure you have anti-virus and security software installed and kept up to date. If you don’t, you are a sitting duck. Even worse, no-one will have much sympathy for you, with so many tools now available for free.

For instance:

This link is to a free anti-virus scan from a reputable provider. However, you need an anti-virus programme that is ‘on’ all the time- a periodic scan is insufficient to protect yourself.

http://home.mcafee.com/store/free-services

This link has many free resources. A programme like SafeSite Advisor is useful as it helps to warn you about unsafe sites. McAfee keeps track of bad, infected sites and rates them accordingly. The big security companies have an edge over smaller providers as they have global resources that enable them pinpoint rogue websites and track the latest scams and security trends.

**Free Anti Virus from Microsoft (for Windows)**


Many reputable PC magazines and related websites periodically review anti-virus software. This link provides one example: It contains an overview of various well-rated free anti-virus products.

http://www.pcmag.com/article2/0,2817,2388652,00.asp

This link reviews a variety of anti-virus products, free and paid subscriptions. It is a bit technical and ‘geeky,’ but it may be useful nonetheless:

http://www.pcmag.com/article2/0,2817,2372364,00.asp

The link below is a review of various security suites (software that includes anti-virus/spyware protection as well as a firewall and other more comprehensive security features). It is highly advisable to have a firewall installed as well as anti-virus protection as it prevents intruders from breaking in to your computer. It is like having your own private security guard. You need both to protect your PC and your identity. Most security products are now easy to install (that was not always the case) and fairly user-friendly, and they no longer slow your PC down to a snail pace.

http://www.pcmag.com/article2/0,2817,2369749,00.asp

Dell ships computers now with optional McAfee SecurityCentre software – A 15 month subscription is free with many laptops. These offers change from time to time.

Lenovo (a Chinese company that bought IBMs excellent ThinkPad computer business) offers a 15 month subscription of Symantec Norton AntiVirus 2012 for 30.75 Euro, or the full security suite-Norton Internet Security 2012 for 33.21 Euro.

**Strong passwords**

It is important to pick strong passwords. It is best to use 8 characters or more, including a combination of numbers, letters and other symbols.

These articles give you helpful hints:


In addition, if you use online email services like Gmail, ensure you use the HTTPS version: Sign in to Gmail and go to Mail settings and set the "Browser Connection" option to "Always use HTTPS." I understand this may be the default setting now (i.e. they do it for you), but check to be sure.

In general when you can, ensure that website addresses you enter credit card details into, or access over public Wi-Fi hotspots have ‘https’ at the beginning- the ‘s’ part means they use encryption so that your data is scrambled as it flies through cyberspace.

**Wi-Fi hotspots** (e.g. at airports, coffee shops) and internet access in hotel rooms


This article has a useful overview of the topic.

Public Wi-Fi hotspots all have one thing in common—they are open networks that are vulnerable to eavesdroppers. It is relatively easy, with cheap, readily available software and an antenna, to eavesdrop on these open networks and basically see all the data that flies over them. It is sometimes called ‘war-driving’.

It is best to turn off your laptop or notebook’s Wi-Fi capability when you’re not using it and to turn off ‘file sharing’ so you are not sprouting leaks unnecessarily. You can find out how to do this by accessing ‘Help’ in Windows.

Public Wi-Fi access is often free, but the trade off can be costly. You should assume that whatever you type or do online can be seen by others.

“Who cares”, says you? I am just surfing, reading or sending email. You should care, because even if you don’t log into your online banking site (never do so from public Wi-Fi hotspots as the bad guys then have your password), you expose your email passwords. Even if you are just reading email, do you really want a stranger to see what you send and receive?

If you don’t have up to date security software installed, the eavesdropper may also be able to access your computer and infect it with a virus or spyware.

There are also criminals who will ‘spoof’ a legitimate Wi-Fi hotspot, and replace the log-in details and wireless signal with their own, so you are re-directed to their site instead, where you are guaranteed they are up to no good.

If you have basic knowledge of how a wireless set-up works, you should manually search and connect to a reputable provider – and see the network name— e.g. Cafe Java, rather than allowing your computer to automatically search for the nearest open connection (with some meaningless name). This basic step will give you some confidence that you are at least connecting to the coffee shops’ hotspot, rather than to Joe Evil Hacker.

In general, it is a good idea to review your banking records regularly to spot any anomalies that might suggest your PC has been hacked.

**Internet access: Routers: High-speed phone and cable connections**

If you have a fast intent connection provided by the phone or cable TV company, they will give you a box called a ‘router’ to facilitate the service. These boxes have proven to be, on occasion, a weak link
in the security chain as they ship with default passwords known to hackers, or simply with security settings that are easily broken.

In most cases, you can upgrade the security on the router, but, in my experience, they don’t make it easy for you to do so. Ask the installer to make the settings as strong as possible, and, if he can’t or won’t do so, call tech support after the fact and have them walk you through the process. Make sure first though that the call is free- and you are not paying an exorbitant rate per minute.

**Recent scams**

Microsoft surveyed 7,000 computer users in the U.K., Ireland, U.S. and Canada. The survey showed that across all four countries, 15% of people had received a call from scammers. In Ireland this rose to 26%. Of those who received a call, 22%, or 3% of the total survey sample, were deceived into following the scammers’ instructions, which ranged from permitting remote access to their computer and downloading software code provided by the criminals to providing credit card information and making a purchase.

The vast majority (79%) of people deceived in this way suffered some sort of financial loss. Seventeen percent said they had money taken from their accounts, 19 percent reported compromised passwords and 17% were victims of identity fraud. More than half (53%) said they suffered subsequent computer problems.

The average cost of repairing damage caused to computers by the scammers was more than £1,000.

**The following is Microsoft’s advice:**

- Be suspicious of unsolicited calls related to a security problem, even if they claim to represent a respected company.
- Never provide personal information, such as credit card or bank details, to an unsolicited caller.
- Do not go to a website, type anything into a computer, install software or follow any other instruction from someone who calls out of the blue.
- Take the caller’s information down and pass it to the authorities

(My comment: Ask them for their name, address and phone number. Tell them your nephew has ‘a big job as a Guard at Garda HQ and you want to run it by him).

- Use up-to-date versions of Windows and application software.
- Make sure security updates are installed regularly.
- Use a strong password and change it regularly (Me: Don’t share it or use the same one for everything).
- Make sure the firewall is turned on and that antivirus software is installed and up to date.
- (Me: if you buy a security product now from a reputable company, all of this is part of the package. The security companies constantly send you ‘updates’- they are basically tracking new infections as they emerge and sending you the antidote. It is a game of cat and mouse that never ends. If a virus takes hold before they find the ‘cure’, they often call that a virus ‘in the wild’).

**Microsoft advises anyone who thinks they may already have been a victim of a phone scam to do the following:**

- Change their computer’s password, change the password on their main email account and change the password for any financial accounts, especially bank and credit cards.
• Scan their computer with the Microsoft Safety Scanner (Me: Or your own anti-virus software) to find out if they have malware (bad stuff) installed on their computer. (Me: you need to check for viruses first before changing anything: if they have infected you and are logging your keystrokes, a new password won’t help as they will steal that too)

• Contact their bank and credit card companies. Me: Check your bank statements at the branch: don’t use the online banking service until you know your computer is ‘clean’.

Conclusion

Whatever grandiose statements you read about X, Y, Z system or software being un-hackable, don’t believe a word. Remember what they said about the Titanic. Unlike the Titanic, most software programmes were build (‘coded’) full of holes and flaws that hackers routinely exploit: The ship was leaky from the start.

The fact remains that almost anything can be ‘hacked’ if someone cares enough to try – and has a reasonable level of technical competency- and patience to burn.

With that uplifting thought in mind, a barrister in possession of client data must demonstrate that they have exercised reasonable care to protect it, proportionate to its value- no more, and no less. It is wise, in my view, to keep on top of trends in the space, and most of all, to keep your wits about you.

If you lack expertise- get help. Don’t try to be a hero.

..........................................................