The pillars of digital security

Philippe Doyle Gray

Photo: iStockphoto.com

INTRODUCTION

The informed debates about the ethics of lawyers using particular technology in the practice of law—like Dropbox, Evernote, iCloud, Facebook, Email, Smartphones, and iPads—have advocates at all parts of the spectrum, from 'always' to 'never.' But informed lawyers agree that there is room for debate only after fundamental safeguards are implemented.

This article synthesises disparate sources from around the world into a formulation that reflects a consensus amongst lawyers and computer scientists about those fundamental safeguards. These are called the pillars of digital security.

My formulation links:

1. key terms of the American Bar Association's model rules of professional conduct,
2. the way in which computing devices work, and
3. the way in which lawyers practice their profession.

This article will identify the sources from which the pillars derive, what those pillars entail, explain how to implement them in legal practice, and guide configuration of iOS devices in accordance with iOS 7.1.2 (for older devices) and iOS 8.1.1.

WHERE DO THE PILLARS OF DIGITAL SECURITY COME FROM?

Diligent lawyers have always asked the question: is it ethical to … ? This article has been prompted by the current crop of new lawyers—and some not so new—asking me: Is it ethical to use … Dropbox? Evernote? iCloud? Facebook? Email? Smartphones? iPads? One might as well ask whether it is ethical to use notepads and pens, lever-arch folders with printed inserts, or mobile telephones. I regularly walk from the Supreme Court of New South Wales down King Street to stop at the intersection with Elizabeth Street. So too do other lawyers. When it's raining we huddle under the awning of the Sydney University Law School, but in fine weather we gather around the traffic lights waiting for the signal that it's safe for pedestrians to cross. Usually I see paper files or lever-arch folders neatly stating the names of the clients concerned, and sometimes the nature of their confidential affairs. Often I can't help but overhear a colleague talking about his matter; a few times sensitive material was inadvertently broadcast to passers-by that happened to include me. Once I even overheard a colleague—speaking on his mobile phone—discuss settlement negotiations during a mediation that had adjourned over lunch: he quite openly discussed not only the parties' respective offers, but his own client's bottom line. The real security problems lie not in cloud computing, but in ourselves.[1]

It is not useful to ask the question: is it ethical to … ? Instead, the question that we should be asking is: how do I ethically use … Dropbox? Evernote? iCloud? Facebook? Email? Smartphones? iPads?

Blame the iPad

Between September 2010 and August 2012 the legal profession reached a tipping point. Before then, comparatively few people questioned lawyers' use of technology—including most lawyers. The extent to which one utilised information technology in the practise of law was a matter of personal preference and entirely optional. Information was usually stored in paper, sometimes in electronic form, typically on site, but always under conditions where it could be accessed and controlled by senior lawyers. But everything changed with the (re-)arrival of cloud computing and the contemporaneous explosion in popularity of Internet-enabled mobile computing devices, not least of which was the tablet computer whose time had come.

In 2009, while the Blackberry was the de rigeur smartphone of the twenty-first century lawyer, the iPhone became an accepted and acceptable alternative: of the top 200 American law firms based on revenue, five per cent supported attorneys with iPhones in 2008, but in 2009 that had jumped to 55 per cent.[2] And then on 3 April 2010 Apple Inc. starting selling iPads.[3] They were an instant hit with American lawyers.

In 2011, about one year after the first iPad went on sale, the American Bar Association surveyed lawyers and found that 15 per cent of respondents used a tablet for law-related tasks, and of that 15 per cent, 89 per cent used an iPad.[4] That same year, of the top 200 American law firms based on revenue, 96 per cent supported attorneys with iPhones and 99 per cent supported attorneys with iPads; in more than half of all law firms every fourth attorney used a tablet computer—and anecdotal evidence suggested that over 90 per cent were using iPads.[5]

In 2012, the American Bar Association found that 33 per cent of respondents used a tablet for law-related tasks, up from 15 per cent the previous year; of that 33 per cent, 91 per cent used an iPad.[6]

By mid-2012, one out of every three lawyers in America used an Apple iPad in the practice of law. Suddenly significant amounts of information—including client's confidential information—was in electronic form, accessed over the Internet, and—perhaps most worryingly—was controlled by third parties who (gasp) were not lawyers. It was time to examine technology's effect on the legal profession, and in particular confidentiality-related concerns that arose from lawyers' increasing transmission and storage of electronic information.[7]

New South Wales was the leader of the pack. By mid-2012, the Ethics Committee of the Law Society of NSW in conjunction with the Office of the Legal Services Commissioner had published guidelines for solicitors about social media,[8] outsourcing (off-shoring)[9] and cloud computing.[10] But the guidelines remained merely guides and have never been adopted by the law society as professional conduct rules.[11]

The American Bar Association quickly took the lead. By August 2012, the Americans had recognised that technology's effect on the legal profession had two critical components:

1. the confidentiality-related concerns recognised in 2010, but also
2. lawyers' competence.

That month the American Bar Association amended its model rules of professional conduct to reflect those two critical components and to provide guidance regarding lawyers' use of technology and confidentiality.[12]

Confidentiality-related concerns

Confidentiality-related concerns were the subject of former American Bar Association rule 1.6:

> (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
>
> (b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
>
> (1) to prevent reasonably certain death or substantial bodily harm.
>
> (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services.
>
> (3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services.
>
> (4) to secure legal advice about the lawyer's compliance with these Rules.
>
> (5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or
>
> (6) to comply with other law or a Court order.

There is no direct equivalent of American Bar Association rule 1.6, but the same subject matter is addressed by rules 108–116 of the *New South Wales Barristers' Rules* dated 6 January 2014, of which rule 108 is the most pertinent:

> 108. A barrister must not disclose (except as compelled by law) or use in any way confidential information obtained by the barrister in the course of practice concerning any person to whom the barrister owes some duty or obligation to keep such information confidential unless or until:
>
> (a) the information is later obtained by the barrister from another person who is not bound by the confidentiality owed by the barrister to the first person and who does not give the information confidentially to the barrister; or
>
> (b) the person has consented to the barrister disclosing or using the information generally or on specific terms.

The solicitors' rules in New South Wales are presently the *New South Wales Professional Conduct and Practice Rules* made by the Law Society on 19 September 2013 under section 703 of the *Legal Profession Act 2004*, which commenced on 1 January 2014. They are a combination of the *Australian Solicitors' Conduct Rules* as adopted by the Law Council of Australia on 18 June 2011 (Rules 1-43) and selected NSW Practice rules (Rules 44-60) which have been retained from the existing rules. Rule 9 is the most pertinent:

> **9 Confidentiality**
>
> 9.1 A solicitor must not disclose any information which is confidential to a client and acquired by the solicitor during the client's engagement to any person who is not:
>
> 9.1.1 a solicitor who is a partner, principal, director, or employee of the solicitor's law practice; or
>
> 9.1.2 a barrister or an employee of, or person otherwise engaged by, the solicitor's law practice or by an associated entity for the purposes of delivering or administering legal services in relation to the client,

EXCEPT as permitted in Rule 9.2.

> 9.2 A solicitor may disclose confidential client information if:
>
> 9.2.1 the client expressly or impliedly authorises disclosure.
>
> 9.2.2 the solicitor is permitted or is compelled by law to disclose;
>
> 9.2.3 the solicitor discloses the information in a confidential setting, for the sole purpose of obtaining advice in connection with the solicitor's legal or ethical obligations;
>
> 9.2.4 the solicitor discloses the information for the sole purpose of avoiding the probable commission of a serious criminal offence.
>
> 9.2.5 the solicitor discloses the information for the purpose of preventing imminent serious physical harm to the client or to another person; or
>
> 9.2.6 the information is disclosed to the insurer of the solicitor, law practice or associated entity.

The American Bar Association's August 2012 amendments added a paragraph at the end of American Bar Association rule 1.6 [emphasis added]:

> (c) A lawyer shall make *reasonable efforts* to prevent the *inadvertent* or *unauthorized disclosure* of, or unauthorized access to, information relating to the representation of a client.

Subsequent commentary has focussed on the words that have been emphasised. These form the basis of some of the pillars: (1) access to information, (2) disclosure of information, (3) inadvertence on the part of the lawyer, and (4) conduct unauthorized by the lawyer.

Lawyers' competence

Lawyers' competence was the subject of American Bar Association Rule 1.1:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

There is no direct equivalent of American Bar Association Rule 1.1, but the same subject matter is addressed by rule 5 of the New South Wales Barristers' Rules:

> 5. These Rules are made in the belief that:
>
> (a) barristers owe their paramount duty to the administration of justice;
>
> (b) barristers must maintain high standards of professional conduct;
>
> (c) barristers as specialist advocates in the administration of justice, must act honestly, fairly, skilfully and with competence and diligence;
>
> (d) …

The solicitors' rules provide:

> 4. Other fundamental ethical duties
>
> 4.1 A solicitor must also:
>
> 4.1.1 act in the best interests of a client in any matter in which the solicitor represents the client.
>
> 4.1.2 …
>
> 4.1.3 deliver legal services competently, diligently and as promptly as reasonably possible.
>
> 4.1.4 …

The *Solicitor's Manual* (formerly *Rileys Solicitor's Manual*) acknowledges the well-known proposition that part of the lawyer's duty to be competent in the service of his or her client (and to the court) is to maintain currency with developments in the law, procedure and professional rules.[13] But neither the commentary, nor the authorities commented upon, mention technology.

The same vice afflicts the *Code of Conduct 2011* published by the independent regulatory body of the Law Society of England and Wales, the Solicitors Regulation Authority—no mention of technology.[14]

American Bar Association Rule 1.1 includes eight paragraphs of explanatory commentary too long to set out in full[15] except for paragraph 8; the August 2012 amendments added words that appear in bold:

> **Maintaining competence**
>
> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Subsequent commentary and the balance of the pillars of digital security spring from these terms.

The Canadian Bar Association's 181 page *Code of Professional Conduct* contains a competency rule with a fleeting reference in its commentary to technology [sic]:[16]

> RULE
>
> 1. The lawyer owes the client a duty to be competent to perform any legal services undertaken on the client's behalf.
>
> …
>
> COMMENTARIES
>
> …
>
> 4. Competence involves more than an understanding of legal principles; it involves an adequate knowledge of the practice and procedures by which those principles can be effectively applied. To accomplish this, the lawyer should keep abreast of developments in all areas in which the lawyer practises. The lawyer should also develop and maintain a facility with advances in technology in areas in which the lawyer practises to maintain a level of competence that meets the standard reasonably expected of lawyers in similar practice circumstances.

I wonder if that should read ' … develop and maintain a *familiarity* with advances in technology …' Perhaps the circularity of reasoning made the draftsman dizzy.

In any event, there is no reason to suppose that American lawyers are more ethical than the rest of us.

WHAT ARE THE PILLARS OF DIGITAL SECURITY?

This article synthesises disparate sources from around the world into a formulation that reflects a consensus amongst lawyers and computer scientists about fundamental safeguards. These I have called the pillars of digital security.

My formulation of the pillars is based upon numerous discussions with many technologically-literate lawyers from Australia, Canada, Germany, Switzerland, the United Kingdom and the United States of America. It is also based upon many discussions with computer scientists (aka 'IT guys') from Australia, Canada and the United States, who service the legal profession in their respective jurisdictions. I have endeavoured to take into account a wide body of professional literature for the legal profession, some of it written by computer scientists and the balance by lawyers.

My formulation reflects a consensus amongst those people and that material, and promotes a common understanding between the fields of law and computer science in a way that links:

1. key terms of the model rules of professional conduct
2. the way in which computing devices work, and
3. the way in which lawyers practice their profession.

The first tranche of pillars concerns *access to* information:

> **Locks** ensure access to information when you have temporarily parted possession *deliberately*.
>
> **Location tracking** ensures access to information when you have temporarily parted possession *inadvertently*.

The second tranche concerns *use of* information:

> **User authentication** regulates the *authorised* disclosure of information
>
> **Encryption** prevents the *unauthorised* disclosure of information
>
> **Data deletion** prevents *unauthorised* and *inadvertent* disclosure of information
>
> **Backup** prevents inadvertent *destruction* of information, and
>
> **Pebkac** prevents the *ineffectual* disclosure of information.

LOCKS: HOW DO I FIND MY STUFF WHERE I LEFT IT?

Locks ensure access to information when you have temporarily parted possession deliberately. You need to find your computing devices where you left them.

Information and communications technology comes in two forms: devices and services. Devices are physical objects. Services are provided through physical objects. Devices include such things as laptop computers and mobile phones. Services include such things as Dropbox and Facebook.

Devices—being physical objects—are secured with physical locks as well as digital locks. Services are secured with digital locks only.

Physical locks

Physical locks ensure access to information when you have temporarily parted possession deliberately—you leave something behind with the intention of coming back to it later. Computing devices come in two forms: those that are easy to move around and those that are not. The former are known as mobile devices and the latter as desktop devices. Mobile devices come in two forms: those that you have already lost, and those that you are going to lose.

A mobile device that always sits on your desktop remains a mobile device. If your laptop always sits on your desk, then it probably should be secured with a Kensington lock. This is a small, metal-reinforced hole found on many mobile devices into which a lock-and-cable apparatus is inserted. The lock-and-cable apparatus works like a bicycle lock: you tether your mobile device to an immovable, or difficult-to-move, object, like a desk, chair or another piece of furniture. If one of your devices is regularly left unattended, and it is secured with a Kensington lock, then all of your devices in the same place should be secured with a Kensington lock. For example, an external hard drive that always sits on your desk beside your laptop should itself be secured with a Kensington lock. If you build a house with 10 doors and put locks on nine of them then it isn't safe.

The particular characteristics of your device and the particular characteristics of your environment dictate the nature and extent of any physical locks. Do you work alone in an office with a lock on the door, that you lock shut every time you leave the room? If so, then the lock on the door is sufficient to protect all your desktop and mobile devices in that room. Do you work in a café located inside a busy airport? If so, then perhaps the most secure place for your device will be in your jacket inside-pocket.

Physical and digital locks are related:

1. The bigger, heavier and more awkward-to-move your computing device, the less need for a physical lock. Conversely, the smaller, lighter and easier to carry your computing device, the greater need for a physical lock.
2. The better the physical lock, the less need for a good digital lock. Conversely the worse the physical lock, the greater the need for a good digital lock: smartphones don't usually come with Kensington locks.

You need to consciously assess the characteristics of your device and the characteristics of your environment to formulate a strategy so that your physical locks—in combination with your digital locks—adequately control access to your devices. When you are the subject of disciplinary action for breach of client confidentiality, or when your disgruntled client threatens to take work elsewhere, you need to give a clear and thorough explanation that starts with your security assessment. There is a world of difference between a thief breaking into your office in the middle of the night, and you forgetting to take your mobile phone with you when you get off the train.

Digital locks

Not to be confused with passwords (more on that below), a digital lock is a digital means by which access to information on a computing device is controlled. Digital locks include logins and parental controls. An important, related topic is software patches.

In the same way that you can physically attach a padlock to a gate—or not—digital locks can be activated—or not. And just as a purchase of a gate does not usually include an accompanying padlock, purchase of a computing device does not usually include a digital lock that has been activated. When you acquire a computing device, you should activate its digital lock. Precisely how you do this will vary from device to device.

Digital locks—like physical locks—can be left unlocked by accident. Digital locks—like physical locks—can be self-locking. If you assess that your computing device requires a digital lock, then it should have a digital lock that is both active and self-locking. Precisely how you do this will vary from device to device.

In iOS 7.1.2 and 8.1.1, to enable self-locking, you set the amount of time that should elapse before the device locks itself by going to:

> Settings > General > Auto-lock

Self-locking raises an important question: How much time should elapse before the device locks itself? The answer depends upon the particular characteristics of your device and the particular characteristics of your environment. But there are rules of thumb: (1) desktop devices should self-lock in 10 minutes, and (2) mobile devices should self-lock in three minutes. That is the amount of time that will elapse before your unattended (misplaced) device will secure itself. That may seem highly inconvenient, but remember that we are not measuring elapsed time per se, but elapsed time from when the device was last used. If you are continuously using your device then it should not lock by itself.

Sometimes you find yourself continuously using your computing device but in a way that your device cannot detect. For example, you might be watching a movie on your laptop. If your laptop locks itself every three minutes then you are not going to enjoy the movie. In that case, one option is to assess the particular characteristics of your device and the particular characteristics of your environment to determine if the amount of time that should elapse before the device locks itself can be extended—and if so then extend it. If you find yourself sitting on a long-haul flight then it is unlikely that doing this will put yourself at risk. But remember that after you have finished watching the movie you need to change the self-locking time back—and you might forget to do that. A second option—that avoids you forgetting—is to use software that temporarily extends the amount of time that should elapse before the device locks itself. An example (for Mac OS X) is Caffeine.[17]

Other times you might be using your device intermittently and the repeated unlocking is not practical. This happens to me in Court. My iPad is a mobile device so it is configured to self-lock after three minutes of inactivity, but it is easy to be making oral submissions and answering questions from the bench for more than three minutes; having to pause—if only for a few seconds—to unlock my iPad breaks the flow and impedes advocacy. So, when in court, I set my iPad to self-lock after 16 minutes (that's an odd time don't you think?). I change it back to three minutes when the court adjourns. Regrettably iOS has no equivalent to Caffeine.

Beware hidden dangers with self-locking times. *Sleeping* is a function that saves power, often by dimming the screen. Often sleeping can be configured automatically. Often automatically sleeping can be configured together with automatically self-locking. But the amount of time that will elapse before your unattended (misplaced) device will sleep is not necessarily the same as the time that will elapse before your device will secure itself. Beware that just because a device will sleep automatically that does not mean that it has locked automatically at the same time. The difference in time between when a device sleeps and locks is called the 'grace period'. The rule of thumb for mobile devices is that they should self-lock in three minutes. Depending on how your device is configured, that three minutes may represent the time elapsed when a device auto-sleeps plus the grace period.

On iOS devices this is a real danger, because auto-locking and auto-sleeping are configured using the same controls—but these are different controls than those used for the grace period. This is examined in the next section. And this explains my odd time to set my iPad to self-lock in court: after 16 minutes. The reason for that odd time is a product of the different configuration tools for auto-locking, auto-sleeping and the grace period; I can't quickly and conveniently set self-locking to 15 minutes.

Logins

A digital lock often takes the form of a login that resembles a password because the login is a series of characters typed on a keyboard. In that case, your login should be complex as distinct from simple.

The idea of a complex versus simple login is different to the idea of complex (complicated) or simple password. When we speak of a simple or complex login, we are speaking about a login that is numerical (all numbers) or alphanumeric (numbers and letters).

While laptops accommodate both simple and complex logins, smartphones and tablet computers usually default to simple logins only—they don't have separate keyboards. Remember that digital locks are usually not initially active. After you first make the digital lock active, then unless you do something more your login will be simple. You may need to change the security settings on your device to change the login from simple to complex. Precisely how you do this will vary from device to device.

In iOS 7.1.2 and 8.1.1, to enable a complex login—called a passcode—first disable simple logins before then enabling a login at all—not as you might expect the other way around, by first enabling a login and then choosing it to be complex:

> Settings > Passcode > Simple Passcode > Off
>
> Settings > Passcode > Turn Passcode On

While you are in this neck of the woods, notice the option at the bottom of the screen 'Erase Data'. This is addressed in the section below on data deletion.

Also while you here, make sure that the grace period is set so that the amount of time that elapses before the device locks itself is the total of the time configured for auto-lock (see above) plus the grace period; this avoids the hidden danger of a device that is asleep but unlocked (see above). The grace period controls are confusingly labelled require passcode and accessed by:

> Settings > Passcode > Require Passcode

Complex logins raise another important question: How complicated should I make my complex login? That hides an anterior question: Why not use simple logins instead? Simple logins are not secure. Simple logins on iOS devices comprise four digits, and for reasons discussed below in the section about user authentication, four digits are grossly inadequate. And the answer to the other question—how complicated should I make my complex login—is also considered in the section about user authentication.

Biometrics

Biometrics is a tempting alternative to logins-that-resemble-passwords. Simply have your device scan your fingerprint or your retina and hey presto, open sesame, just like in the movies when the villain impersonates the president of the United States and orders a nuclear strike on Austria in retaliation for Conchita Wurst winning Eurovision 2014. Apple has released the iPhone 5s and later models with a finger print scanner and you might be forgiven for thinking that this option has enhanced security because of its use of biometrics.

The Chaos Computer Club e. V. describe themselves as Europe's largest association of hackers, who for more than 30 years have provided information about technical and societal issues, such as surveillance, privacy, freedom of information, hacktivism, and data security.[18] On 20 September 2013, Apple released the iPhone 5s. The *very next day* the Chaos Computer Club's biometrics hacking team made a fingerprint of the phone user with basic household items like a digital camera, laser printer, and white glue that was good enough to create a fake finger that could unlock an iPhone 5s.[19]

It's not hard to imagine why this was so easy: you are not the president of the United States and you are not authorising a nuclear strike—you are a dude using a mass produced consumer device sending your vote by text message for Conchita Wurst on *Austria's Got Talent*. The quality of the equipment and the consequences of mistaken identity are not comparable.

Respected legal-profession security consultants and computer scientists John W Simek and Sharon Nelson of Sensei Enterprises have been reported[20] as saying:

> Despite rumors of their impending death, says Nelson, passwords probably won't die—but they may need a partner to survive. Two-factor authentication (something you know, plus something you have) is the future, says Simek. 'Biometrics are a temporary solution. I think tokens will be the second factor, along with passwords.'
>
> …
>
> 'Biometrics won't cut it,' adds Nelson. 'Despite the true believers, once the electronic representation of your fingerprint is compromised, you are toast. You can't go get a new finger.'

Parental controls

Parental controls are not just for parents. Parental controls are to be used anytime you hand over your computing device to someone else who will use it, without it being under your direct and immediate control: children, the infirm, witnesses under examination and intoxicated associates are all prime candidates. And even when it's a question of parents and children, it's not necessarily parents protecting children, but parents being protected from their children. In March 2013, the *Sydney Morning Herald* reported that five-year-old Danny Kitchen asked his parents for the password to the family iPad to download a free game, and in 10 to 15 minutes racked up a bill on his mother's credit card totalling $2,500.[21] His story is not unusual; there are many other news reports about children doing similar things.[22]

Smartphones and tablet computers—which store sensitive client information—are great distractions for children. Adults are inclined to hand over their devices to let children play with them—and children are inclined to incline adults to do so. Laptops and desktop computers fall into the same category. Once you place your computing device into a child's hands—or anyone else's hands for that matter— then you have lost control unless you engage parental controls.

What I hear you say: you don't store sensitive client information on your iPad? What about email? What would happen if little fingers forwarded an email to your opponent with the help of email-address auto-complete?

Sensitive information can also be embarrassing: what if somebody became bored playing angry birds and took a funny photograph of grandpa dressed in a Mexican hat, standing on a table, red-faced and holding a bottle of Tequila? And then emailed it.

Parental controls allow you to *partially* unlock your device. The user can access some information but not everything. This works differently on different devices. And it might be called something different than parental controls.

When handing over your device to a child (or anyone else), you can engage parental controls to limit the device to particular functions. Precisely how you do this will vary from device to device. Beware that some devices have one set of parental controls that limit a child *from* using a particular function, while the same device has a different set of parental controls that limit a child *to* using a particular function—and you may need to enable both.

In iOS 7.1.2 and 8.1.1, to limit your iPad to your nephew's favourite game but also prevent him from making in-app purchases depleting your credit card, then you need to limit your nephew to the game by enabling guided access while preventing him from making in-app purchases by enabling restrictions:

> Settings > General > Accessibility > Guided Access
>
> Settings > General > Restrictions

Software patches

The advertising brochure for the seminar at which an earlier draft of this article was presented stated:

> Bring along your iOS devices (updated to the latest version of iOS 7) and be guided by the speaker to configure your iDevice on the spot.

That was designed to push you to patch your iPhones and iPads. Every computing device runs on software. Software is written by humans who make mistakes. Software developers sometimes fix their mistakes, and then they usually release a *patch*. A patch is software code that is designed to replace the code on your computing device to fix the mistake. Installing that software on your computing device to fix a mistake is called patching.

Patching is very important because software mistakes include vulnerabilities. These vulnerabilities expose your computing device to malicious attack by hackers. Patching strengthens or eliminates the vulnerabilities and in turn this increases the digital security of your device.

Patching is free. If you are being asked to pay for new software, then this is not a patch but is likely to be an *upgrade*. An easy way to differentiate between patches and upgrades is the first digit of the version number of the software:

- moving from iOS 6 to iOS 7 or iOS 6.5 to iOS 7.1 is upgrading
- moving from iOS 6.1 to iOS 6.2 or iOS 7.1.1 to iOS 7.1.2 is patching

LOCATION TRACKING: WHAT IF IT'S NOT WHERE I LEFT IT?

If you left something in a place and it's not there when you return, then it has been misplaced. You need to find it again. That's when to use remote location-tracking. If you cannot regain possession of something that has been misplaced then it has been lost. This is addressed in the section below on data deletion.

Remote location-tracking allows you to use an Internet connection between your misplaced device and the relevant cloud service to locate and control your device. But there is an important caveat: your device needs to have its remote location-tracking functionality enabled in order for the relevant cloud service to locate and control your device. Like digital locks, when you acquire a computing device, you should activate its remote location-tracking functionality. Precisely how you do this will vary from device to device.

Beware that on some devices—and all iOS devices—you need to enable remote location-tracking *before you lose your device*. If you don't do so then there's nothing you can do later. Other devices are more forgiving. If your device uses the android operating system, and if you connected the device to your Google account, then you *may* be able to use Google's Android device manager[23] to remotely track your device after you lose it.

Another reason to enable remote location-tracking now is that you need to check that remote location-tracking is actually enabled. You need to test that it works. This will force you to familiarise yourself with the requisite procedures that vary from device to device and from cloud service to cloud service.

For Apple devices the relevant cloud service is Apple's iCloud,[24] and the remote location-tracking functionality is confusingly called Find my iPhone despite the fact that it finds not only iPhones, but iPads, laptops and desktops too. On iOS 7.1.2 and 8.1.1 devices to enable remote location-tracking functionality after an iCloud account is opened—go to:

> Settings > iCloud > Find My iPhone > On

Another hidden danger with iOS 7 needs special mention. Some news reports misleadingly suggest that starting with iOS 7, users do not need to enable remote location-tracking before losing the device as was the case with previous versions of iOS.[25] This is wrong and directly contrary to Apple's own information.[26] The confusion arises because Apple uses the same name - 'Find my iPhone' - to describe two different things: their cloud-based remote-tracking service, and their iOS app. You don't need the app to use the service—but you do need to activate the functionality on your device that links the device to the service.

USER AUTHENTICATION: MORE THAN PASSWORDS

User authentication regulates the authorised disclosure of information. It is a means by which a person (user) legitimately gains access to data (information). I have considered how this can be done by use of logins[27] and biometrics[28] and now we come to passwords, the most common method of user authentication. Passwords have three significant problems:

- too simple
- hard to remember
- re-used

What this leads to is that you use an insecure password over and over again. Your password is insecure, so it is easy to guess or to break. Why is it easy to break? Because if it is simple then it is likely to be used by other people too. A malicious hacker can perform a Google search on 'most common passwords' and try those first. Try it yourself if you don't believe me and see if you recognise your password.

A password six characters long would take two seconds *to break; a password 12 characters long would take* 48 thousand years *to break.*

Moreover, simple passwords can be broken very quickly. The Australian Government through its service Stay Smart Online has published an indication of the time taken for a computer system built in October 2013 to guess a password based on the number of characters making up the password (assuming a random password chosen from 95 different characters: uppercase, lowercase, numbers, symbols). A password six characters long would take *two seconds to break*; a password 12 characters long would take *48 thousand years* to break.[29] And remember that the six-character password is made up of six characters any one of which could be an uppercase letter, lowercase letter, number or symbol. Those four-digit, simple logins are grossly inadequate.[30] I acknowledge that four-digit logins on iOS devices are not the same thing as four-digit password logins to a cloud computing service—but a four-digit logins on iOS devices are simple not complex.

Philippe Doyle Gray, 'The pillars of digital security'

Furthermore, re-use of your password over and over again increases the danger exponentially. If you use the same password for on-line banking and for your customer loyalty program, then when your customer loyalty program details are obtained by malicious hackers—because your retailer or airline does not deploy as good security as your bank—then those hackers can immediately use those very same credentials to access your on-line bank account. If each password were unique then this could not happen. The solutions are simple:

- make them harder—much harder
- stop remembering them
- ensure they are unique

These solutions may be simple but many people think that they are also difficult to implement. Not so: user authentication is a technological problem and it has a technological solution: password managers.

Password managers are software that generate and record complex, complicated, unique and random passwords along with contextual information so that you never have to remember them. The three most-recommended password managers for lawyers are:

- 1Password by AgileBits[31]
- LastPass by LastPass Inc.[32]
- eWallet by iLium Software[33]

AgileBits[34] and LastPass Inc.[35] have produced excellent motion pictures less than two-minutes long explaining the three significant problems identified above and how each of their products implements solutions. Watch them.

Using password managers to generate passwords raises an important question: How complex and complicated should your passwords be? The answer depends upon the particular characteristics of your device and the particular characteristics of your environment. But there are guides from a number of sources.

The Australian Government through its service Stay Smart Online advises[36] that your passwords should not comprise words, but a random mixture of upper and lower case characters, number and symbols. While it conspicuously avoids suggesting a minimum length, examples given of acceptable passwords contain at least 13 characters.[37]

The Canadian lawyers' compulsory professional indemnity insurer LawPRO advises at least 12 characters long—and longer is even better—with at least one symbol character in a position other than the first and last, and containing at least one character from each of the following groups: (1) uppercase letters, (2) lowercase letters, (3) numerals, and (4) symbols.[38]

The American Bar Association has suggested a minimum length of 15 characters, including a variety of character types, including upper and lower case letters, numbers and special characters (like &, % or @) but warned that common character substitutions (e.g. replacing 'a' with '@' or 's' with '5') may not be enough to protect you: more sophisticated attacks will include these variations as well.[39]

The Hon Judge Herbert B Dixon Jnr of the Superior Court of the District of Columbia who is also the technology columnist for *The Judges' Journal* advises using a random combination of upper and lowercase letters, numbers, and symbols of at least 12 characters.[40]

The Australian Government through its service Stay Smart Online advises[36] that your passwords should not comprise words, but a random mixture of upper and lower case characters, number and symbols.

Sharon Nelson, forensic computer scientist of Sensei Enterprises has advised to make your password at least 14 characters, using upper and lower case, numbers and special characters.[41]

Microsoft Inc. requires all employees to use passwords at least eight characters long—longer is better—that include at least three of the following: uppercase and lowercase letters, numerals, punctuation marks, and symbols.[42]

Apple Inc. advises a long sequence of random characters that include a mix of upper and lowercase letters, numbers, punctuation marks, and (if the site or item supports it) characters typed while holding down the Option key … over eight characters long[43]

Google Inc. advises to (1) include punctuation marks and/or numbers, (2) mix capital and lowercase letters, (3) include similar looking substitutions, such as the number zero for the letter 'O' or '$' for the letter 'S' but does not recommend a length.[44]

I have edited these guidelines enabling you to configure software like 1Password, LastPass or eWallet. Reputable password managers generate passwords that are *unique* and *random* by default—there is nothing to configure. If you do not use a password manager to generate passwords then do not rely on these guidelines only.

The American Bar Association has explicitly linked insecure password use to a breach of the model rules of professional conduct.[45]

Two-factor authentication

Passwords can be stolen or circumvented. If they are unique, then only one source of data is exposed to the danger of unauthorised disclosure of information. But what comfort do you get by the words 'only one'? Is that the only one for which you will be sued in negligence or prosecuted for unethical conduct?

The solution is two-factor authentication, also known as two-factor verification, and two-step verification. When enabled this requires both a password and a time-sensitive code that is sent to a mobile telephone. A hacker may obtain your password, but while your phone is safe in your pocket so too is your data. This two-factor authentication is the same security measure deployed by banks and other financial institutions.

Two-factor authentication applies to services not devices. Precisely how you enable two-factor authentication on a service will vary from service to service, and it will also vary with the device that is your second factor—usually your smartphone.

First, start with your smartphone. There are two common ways that codes will be generated: (1) text message (SMS) sent to your phone, or (2) via an authenticator app installed on your phone. If you prefer an authenticator app then you will need to first install the app. What app should you use? This will vary from device to device.

On iOS 7 and iOS 8 devices, you have at least two choices: Google Authenticator[46] and OTP Auth.[47]

Second, go to your service's support page and search for two-factor authentication> and that will take you to a set of instructions. Links to instructions appear in the footnotes for:

- Google[48]
- Dropbox[49]
- iCloud[50]
- Facebook[51]

ENCRYPTION: HOW DO I SECURE MY STUFF WHEN IT'S MISPLACED?

Encryption prevents the unauthorised disclosure of information. It secures your data if your device is misplaced and potentially stolen, and it secures your data when accessing a service.

Devices

Encryption secures your data between the time when your device is lost (stolen) and the time you realise that it has been lost (stolen).

When we are talking about physical devices, by this stage your physical locks have been defeated, and the risk that you now face is that your digital locks will be circumvented—if your device has been stolen. You might not know if it has been misplaced or stolen until it's too late. By enabling a required login on your device—the digital lock—a thief can either break the lock or bypass the lock.

One way to break the lock is that a thief will try to guess your login. He might not have to guess if he already has your login—because you re-use your logins. Even if he has to guess, it might be easy to guess your login if it is simple instead of being complex. And he will start with the most common iPhone unlock codes; if he's just starting out in his life of crime and short of start-up funds then he can get a list by performing a Google search on 'most common iPhone unlock codes.' If you have a complex login then his alternative is to by-pass the lock.

By-passing your lock can take several forms. One spectacularly trivial example that affects some iOS devices is to use Siri—the 'intelligent' personal assistant and knowledge navigator which works as an application on iOS. Just ask her to by-pass the lock! Press down on the <Home> button on a locked iPhone and ask Siri to make a phone call, send a text, look through notes and send email. By simple manipulations of your questions you can access and extract contact information. In iOS 7.1.2 and 8.1.1, to eliminate that vulnerability ensure that Siri is deactivated while the device is locked:

> Settings > Passcode > Siri > Off

But the threat against which you need to guard yourself is not specific. The threat against which you need to guard yourself is that, somehow or another, a person will gain access to the hard disk on your mobile device. And when they do, in order to prevent the unauthorised disclosure of information on that disk, the data needs to be encrypted. Precisely how you do this will vary from device to device.

Philippe Doyle Gray, 'The pillars of digital security'

Photo: iStockphoto.com

In iOS 7.1.2 you can relax—Apple has made this easy. All you need to do is to Turn Passcode On as explained above and look for the words at the bottom of the screen that confirm encryption is enabled:

> Data protection is enabled.

Because encryption of external hard drives and other easily portable objects is so important, many commentators believe that failure to encrypt mobile devices is an unethical practice for lawyers.[52] Remember that there is risk when encrypting your smartphone's data if you then make a backup of that data that is not encrypted. If you build a house with 10 doors and put locks on nine of them …

Services

I have been talking about physical devices but there are also services to think about: see above. Encryption secures your data between the time when your service is compromised (hacked) and the time you realise that it is compromised (hacked). That of course depends upon the time—if ever—that your service provider itself becomes aware and then—if ever—informs you. In the case of money in the bank, paper bank statements might take 30 days to arrive …

Just as in the case of devices, a thief can either break the digital lock or by-pass the digital lock. Your concern here is breaking not by-passing (it's not your device). Even if the thief has to guess your login, it might be easy because of re-use or he may start with the most common login passwords by performing a Google search on 'most common login passwords.'

Devices and services

But there is another aspect to services. Services are provided through physical objects via the Internet. Some objects will be yours: your smartphone, your iPad. These objects are your devices.

Your devices can connect to the Internet via a cable or wire, and this is called a wired connection. A device can connect to the Internet via the electromagnetic spectrum (also used by radio and television), and this is called a wireless connection.

The most common wireless connection that you will encounter are wireless networks (aka wi-fi). Wi-fi poses a danger of unauthorised disclosure of information. Wi-fi networks can be encrypted but often they are not. More and more businesses offer complimentary wi-fi. If in doubt, treat these connections as not secure and not encrypted. And how certain can you be that the backpacking waiter serving you understands wireless network encryption? Remember: needing a password to access a wireless network (a login) is different to the wireless network being encrypted. Don't do your Internet banking over your favourite café's wireless network—but reading the news over coffee is perfectly fine.

Once your Wi-fi is secure, then the next issue is the website you are visiting. When surfing the world wide web you will encounter http and https—note the last letter. Https is an abbreviation for hypertext transfer protocol secure. It is a communications protocol for secure communication over a computer network. It encrypts the data flow between two devices connected over the Internet. Many popular websites offer Internet addresses—URLs—in both http and https options, both of which will take you to the same place. The differences will be almost invisible:

> http://www.google.com
>
> https://www.google.com

Https is secure but http is not. Use https every time that it is available—it won't be available on every website so you have to check your browser window every time. But you will forget to check your browser window every time, so change your web browser to something that supports software that will do this for you without you having to think about it. I recommend a web browser extension that works with several popular browsers called HTTPS Everywhere published by the Electronic Frontier Foundation.[53]

DATA DELETION: HOW DO I SECURE MY STUFF WHEN IT'S LOST?

If you cannot regain possession of something that has been misplaced then it has been lost. If it has been lost the risk you now face is that your digital locks will be circumvented. By then enabling a required login on your device—by activating the digital lock—a thief is then forced to either break the lock or by-pass the lock. This will take time. Use that time to delete the data. In this way, data deletion prevents unauthorised disclosure of information.

How do you delete data on a mobile computing device no longer in your possession? Sometimes you can't. You need to consciously assess the characteristics of your device and the characteristics of your environment to formulate a strategy so that you adequately control access to information on your devices. Don't put sensitive data on a USB memory stick that you toss into your briefcase or handbag. USB memory sticks are small, easy to lose and impossible to erase when they're gone.

But some mobile computing devices support data deletion even when they are no longer in your possession—either data is deleted automatically (say, after 10 failed attempts to enter a login) or you delete data remotely. Precisely how you do this will vary from device to device.

In iOS 7.1.2 and 8.1.1, to enable automatic data deletion, go to:

> Settings > Passcode > Erase Data

Danger! If you enable automatic data deletion then while this will work when your device is no longer in your possession, it will also work when it remains in your possession but you fail to enter your login 10 times—which might happen if you are prone to 'drunk dialling'. But those wonderful designers at Apple thought of this too. A person who picks up an iPhone with the passcode lock enabled has 10 chances to enter the correct code, but that doesn't mean that he can just try 10 different codes in a row. After six incorrect attempts, the person must wait one minute before trying again. If the seventh attempt is wrong, the person must wait five minutes before trying again. If the eighth attempt is wrong, the person must wait 15 minutes before trying again. If the ninth attempt is wrong, the person must wait 60 minutes before trying again. After 10 incorrect attempts, you have clearly continued drinking for a long time and Apple won't save you from yourself.[54]

In iOS 7.1.2 and 8.1.1, to enable remote data deletion, go to:

> Settings > iCloud > Account [and enter the details for your account]
>
> Press <Done>
>
> Settings > iCloud > Find My iPad > On[55]

Of course, you need an iCloud account before you do this because in the Apple universe remote data deletion is part of remote location-tracking.

Obsolescence

When equipment reaches the end of its lifespan you might be tempted to throw it away, donate it for recycling, or give it to a friend or relative. Once you part possession you no longer have control. If sensitive data remains then you risk inadvertent disclosure of information.

Before parting possession you need to delete the data so that it is no longer accessible. In this way, data deletion prevents inadvertent disclosure of information. Precisely how you do this will vary from device to device.

In iOS 7.1.2 and 8.1.1, to delete the data so that it is no longer accessible, go to:

> Settings > General > Reset > Erase All Content and Settings

You will asked for confirmation.

After giving confirmation, you will be asked for your login.

Watch and wait—the process can take from a few minutes to several hours depending upon the device,[56] so connect your device to a charger and leave it connected until the process is complete.

BACKUP: HOW DO I SECURE MY STUFF WHEN IT'S GONE?

Backup prevents inadvertent destruction of information.

It's not a question of if—it's a question of when—you will need to *restore* data. Consider these scenarios: (1) a hard drive fails; (2) data was deleted, either inadvertently or maliciously; (3) a virus corrupted a file; (4) a file was lost; or (5) a file was accidentally overwritten. Whatever backup system you use, it must be automated. If someone has to manually start, stop or otherwise monitor the backup, it isn't going to happen—and certainly not regularly.[57]

Appreciate the difference between a backup of data and the software to access that data. Provided that you back up your data and software, there is no need to back up your data and software together. It is often much easier to back up data alone. But beware of the format in which your data exists: while ubiquitous formats do not demand a backup of software because the software is likely to be ubiquitous too, obscure formats are another matter.

And of course you need to periodically check your backups to ensure that you have actually backed up.

The 3-2-1 Rule[58]

The purpose of a backup is to make sure that your digital data can survive any of the hazards that await. In principle, this is a straightforward process. Copy all of your files to some other device(s), keep the backup somewhere safe, and use it to restore the data in the event of a problem.

The simplest way to remember how to back up your data safely is to use the 3–2–1 rule (or the 1–2–3 rule!):

1 1 copy stored offsite

2 2 different media types

3 3 copies

Redundancy is not backup[59]

Redundancy is storing information in more than one place. Many offices have redundant systems that involve storing data within devices that have at least two internal drives. Redundancy alone is not backup; it is a fail-safe measure in the event of failure of the storage device's initial internal drive. This means that if one drive fails, another will immediately kick in and preserve any data contained within. It's just like when you double-bag your groceries—if one bag seems flimsy for what you've purchased, you might place the whole thing inside another bag so that if it breaks, there's a second layer of protection before your eggs crack all over the floor. However, redundancy alone does not preserve your data. It saves you in the event of a minor technological glitch, but not from physical disaster like fire or flood.

Ongoing self-education is essential to maintaining competence about the benefits and risks associated with relevant technology.

Backup, on the other hand, is the practice of keeping data in different places so that if something happens to one copy, you have additional copies. In theory, if you email yourself a document via Gmail, you're creating a backup. One exists on your hard-drive, and one exists on Google's servers. But that's not ideal for a general backup system, for reasons that should be obvious. The ideal way to back up what's important to you is to ensure that you have copies saved both on- and off-site, and *that* would be satisfied by storing both in the cloud and in physical locations.

PEBKAC: HOW DO I PROVE THAT I AM ETHICAL?

In February 2002, at a United States Department of Defense news briefing about the lack of evidence linking the government of Iraq with the supply of weapons of mass destruction to terrorist groups, United States Secretary of Defense Donald Rumsfeld was questioned and gave his famous reply [emphasis added]:[60]

> Question: Could I follow up, Mr. Secretary, on what you just said, please? In regard to Iraq weapons of mass destruction and terrorists, is there any evidence to indicate that Iraq has attempted to or is willing to supply terrorists with weapons of mass destruction? Because there are reports that there is no evidence of a direct link between Baghdad and some of these terrorist organizations.
>
> Rumsfeld: Reports that say that something hasn't happened are always interesting to me, **because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we**

> **don't know.** And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.
>
> And so people who have the omniscience that they can say with high certainty that something has not happened or is not being tried, have capabilities that are—what was the word you used, Pam, earlier?
>
> Question: Free associate? (laughs)
>
> Rumsfeld: Yeah. They can (chuckles) they can do things I can't do. (laughter).

The danger of unknown-unknowns applies to lawyers use of technology: lawyers are not computer scientists and it is not practical to require lawyers to possess the same knowledge as computer scientists. One day it may be trite to suggest that - to be ethical - lawyers must be competent in the use of technology in the practice of law. A degree of competence may reveal known-knowns and known-unknowns. But unknown-unknowns *always* lurk. And because they always lurk, ignorance may not be a good defence. In any event, the important question is: how do I maintain competence?

Ongoing self-education is essential to maintaining competence about the benefits and risks associated with relevant technology. And that does not always entail learning how to use technology, but whether it should be used at all. Technology is a tool, not a panacea. But self-education is not enough; you also need self-awareness.

Social engineering, in the context of information security, refers to the psychological manipulation of people into performing actions or divulging confidential information.[61] This is illustrated by my two favourite reports of social engineering.

In January 2013, Australian PC & Tech Authority magazine reported:[62]

> During the course of a 3-day security conference in London recently, a poster on the wall of the hall featured the logo of a well-known security vendor, the words 'Just scan to win an iPad' and a QR code. That poster had been created and stuck there by David [Maman of GreenSQL], but neither the organisers of the event, nor the security vendor whose logo was featured, bothered to ask what it was doing there or request that it be taken down. Some 445 people did scan the QR code and browsed the page that it linked to. At this point it's worth a reminder that this was a conference for IT security professionals. All they actually got when they scanned that QR code was a web page featuring a smiley face, but it could have been a piece of malware, or one of a multitude of poisoned URL attacks.

In November 2013, Reuters reported:[63]

> Former U.S. National Security Agency contractor Edward Snowden used login credentials and passwords provided unwittingly by colleagues at a spy base in Hawaii to access some of the classified material he leaked to the media … Snowden may have persuaded between 20 and 25 fellow workers at the NSA regional operations centre in Hawaii **to give him their logins and passwords by telling them they were needed for him to do his job as a computer systems administrator …** The revelation is the latest to indicate that inadequate security measures at the NSA played a significant role in the worst breach of classified data in the super-secret eavesdropping agency's 61-year history. [emphasis added]

Who would have thought that self-awareness was lacking at an IT security conference or the American National Security Agency? And this leads us to pebkac.

Imagine yourself explaining to a client why it was that your record of their confidential information found its way into the hands of a stranger.

Pebkac is a derogatory term for incompetent computer users. It is an acronym: Problem Exists Between Keyboard And Chair. Incompetence in both these cases was not incompetence in the use of technology per se, but nevertheless the problem existed between the keyboard and chair.

Doing what everyone else does is usually a safe strategy for lawyers. But not when other lawyers are incompetent—in that case the strategy needs to be adapted to the environment. And the environment may include pebkac.

Let's use email as an example. We end where we began—with the ethics of competence and confidentiality. Notepads and pens, lever-arch folders with printed inserts, or mobile telephones are all liable to communicate information by which you make an unauthorised or inadvertent disclosure of information.

Email is like mail in some respects but not in others. Email is more or less an electronic postcard: just like the postcard, where any postal worker handling the mail can read its contents, any server operator and programs from governments can read your email.[64]

That is not to say that lawyers should not use email. But instead it is to say that lawyers should not *always* use email. If you are acting for an employee in a dispute with his employer, sending a confidential email to your client's work email address may—and almost certainly will—allow the unauthorised disclosure of information to your opponent. If you are in the habit of always using email then you are not consciously thinking about what you are doing and you are at risk.

The follow-the-herd problem is recognised by the *Civil Liability Act 2002* (NSW) [emphasis added]:

> **5O Standard of care for professionals**
>
> (1) A person practising a profession (a professional) does not incur a liability in negligence arising from the provision of a professional service if it is established that **the professional acted in a manner that (at the time the service was provided) was widely accepted in Australia by peer professional opinion as competent professional practice.**
>
> (2) However, **peer professional opinion cannot be relied on for the purposes of this section if the Court considers that the opinion is irrational.**
>
> (3) The fact that there are differing peer professional opinions widely accepted in Australia concerning a matter does not prevent any one or more (or all) of those opinions being relied on for the purposes of this section.
>
> (4) Peer professional opinion does not have to be universally accepted to be considered widely accepted.

Is it irrational to suppose that American lawyers are more ethical than the rest of us?[65]

Different people have different concerns about security. Some people want to believe that information and communications technology is not secure. It is not inconceivable that some of those people are lawyers who reject technology. It is not inconceivable that some of those lawyers are judges. Nor is it inconceivable that some of those people are clients.

Fear, ignorance and apathy that are associated with the use of technology in professional legal practice are all good reasons to forget that security is relative. My home is secured by double-bolt deadlocks. This is a requirement of my insurance company. For the purposes of my contract of insurance, my home is secure. If I lock myself out of the house, I can go to my neighbour, and telephone a locksmith, who will charge me $300 to open my front door in about 30 seconds. If it is opened, does that mean my home is not secure? Hindsight reasoning coupled with fear, ignorance and apathy make a powerful combination. Clients who win can believe they had a good case; clients who lose can believe they had a bad lawyer.

Imagine yourself explaining to a client why it was that your record of their confidential information found its way into the hands of a stranger. Then imagine an angry client testifying against you before a disciplinary tribunal. And then add to that, the problem of pebkac. What are you going to say?

You need to give a clear and thorough explanation that starts with your security assessment. And you need to prove when, where and how you undertook that assessment. Don't forget that technology has both risks and benefits. Identify the benefits.

I strongly recommend that you use a password manager and implement two–factor authentication wherever possible. In the event of a data breach, the persuasive analogy the lends itself is of a thief breaking into a bank fault. The question for any adjudicator changes from 'could the lawyer have made his records more secure?' to 'is using a password manager and implementing two-factor authentication adequate?' This approach drives adjudicators to take into account all the relevant circumstances, to be able to assess expert evidence about those circumstances, and to carefully evaluate both the risks and the benefits of technology.

Lawyers love documents to tender. Make some. Start with this article.

Endnotes

1. Ernie Svenson, 'Security analysis for lawyers: poor, to fairly cloudy' 21 February 2013, available at http://ernietheattorney.net/security-analysis-for-lawyers-poor-to-fairly-cloudy/
2. Jeff Richardson, 'Over half of the most profitable law firms use iPhones' available at http://www.iphonejd.com/iphone_jd/2009/11/over-half-of-the-most-profitable-law-firms-use-iphones.html
3. Apple Inc. Press release, 'iPad Available in US on April 3' available at https://www.apple.com/pr/library/2010/03/05iPad-Available-in-US-on-April-3.html
4. Jeff Richardson, '2011 ABA Technology Survey suggests around 300,000 U.S. lawyers use an iPhone, around 130,000 use an iPad' available at http://www.iphonejd.com/iphone_jd/2011/07/aba-technology-survey-reveals-increase-in-smartphone-use.html
5. Jeff Richardson, 'AmLaw 2012 survey shows strong iPhone, iPad support at the most profitable law firms' available at http://www.iphonejd.com/iphone_jd/2012/11/amlaw-survey-2012.html
6. Jeff Richardson, '2012 ABA Tech Survey reveals surge in lawyer iPhone, iPad use' available at http://www.iphonejd.com/iphone_jd/2012/07/2012-aba-tech-survey-reveals-surge-in-lawyer-iphone-ipad-use.html
7. American Bar Association Commission on Ethics 20/20 Working Group on the Implications of New Technologies, 'Client Confidentiality and Lawyers' Use of Technology' issues paper, 20 September 2010, available at http://tinyurl.com/n35fef7 and also at http://www.americanbar.org/content/dam/aba/migrated/2011_build/ethics_2020/clientconfidentiality_issuespaper.pdf
8. Kenny and Gordon, 'Social Media Issues for Legal Practice', *Law Society Journal*, April 2012, Vol 50, No 4 at p.66-68 available at http://tinyurl.com/qfyxp87 and also at http://www.olsc.nsw.gov.au/agdbasev7wr/olsc/documents/pdf/lsj_social_media_april2012.pdf
9. Kenny and Gordon, 'Outsourcing Issues for Legal Practice', *Law Society Journal*, May 2012, Vol 50, No 4 at p72–73 available at http://tinyurl.com/lytnw8x and also at http://www.olsc.nsw.gov.au/agdbasev7wr/olsc/documents/pdf/lsj_outsourcing_may2012.pdf
10. Kenny and Gordon, 'Cloud Computing Issues for Legal Practices', *Law Society Journal*, June 2012, Vol 50 No 5 at p.78–79 available at http://tinyurl.com/o99cu3r and also at http://www.olsc.nsw.gov.au/agdbasev7wr/olsc/documents/pdf/cldcomputing_lsj_article_june_2012_kenny_gordon.pdf
11. 'Cloudy conditions at the NSW Law Society' *Justinian*, 22 January 2013 available at http://www.justinian.com.au/news/cloudy-conditions-at-the-nsw-law-society.html
12. American Bar Association House of Delegates Resolution Revised 105A as amended (Technology & Confidentiality), 6 August 2012, available at http://www.americanbar.org/groups/professional_responsibility/policy.html
13. G E Dal Pont, *The Solicitors Manual*, LexisNexis at [29,160] updated to service 54
14. SRA Code of Conduct 2011, available at http://www.sra.org.uk/solicitors/handbook/code/content.page
15. You can access all eight paragraphs at http://tinyurl.com/c8obv9h and also at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html
16. Code of Professional Conduct available at http://www.cba.org/cba/activities/code/
17. See https://itunes.apple.com/au/app/caffeine/id411246225?mt=12
18. http://www.ccc.de/en/home
19. 'Chaos Computer Club breaks Apple TouchID' available at http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid
20. Joan Feldman, 'Five Must-Know Password Protection Tips' 9 May 2014, available at http://www.attorneyatwork.com/five-password-protection-tips/
21. Camille Bautista, 'Five-year-old spends $2500 on apps in 10 minutes' Sydney Morning Herald, 5 March 2013 available at http://www.smh.com.au/digital-life/digital-life-news/fiveyearold-spends-2500-on-apps-in-10-minutes-20130304-2fhpm.html
22. See for example 'UK cop turns in his son after Apple refuses to refund App Store spending spree' available at http://www.tuaw.com/2013/03/25/uk-cop-turns-in-his-son-after-apple-refuses-to-refund-app-store/
23. https://www.google.com/android/devicemanager
24. https://www.icloud.com/#
25. For example, Marc Knoll, 'How to track your lost iPhone or iPad without a tracking app' 6 June 2014 available at http://trendblog.net/how-to-track-your-lost-iphone-or-ipad-without-tracking-app/
26. 'iCloud: Find My iPhone Activation Lock in iOS 7' http://support.apple.com/kb/ht5818
27. See Logins
28. See Biometrics
29. 'How strong is your password?' available at http://tinyurl.com/o6k7359 and also at http://www.staysmartonline.gov.au/alert_service/alerts/how_strong_is_your_password_sso_alert_priority_low#.U8HtVKg4RG9
30. See paragraph 55
31. https://agilebits.com/onepassword
32. https://lastpass.com/
33. http://www.iliumsoft.com/ewallet
34. http://youtu.be/yln4opypuO0
35. http://youtu.be/RM0fzHxMASQ
36. 'How strong is your password?' available at http://tinyurl.com/o6k7359 and also at http://www.staysmartonline.gov.au/alert_service/alerts/how_strong_is_your_password_sso_alert_priority_low#.U8HtVKg4RG9
37. 'Set and use strong passwords' available at http://tinyurl.com/ponqf6j and also at http://www.staysmartonline.gov.au/home_users/secure_your_computer/set_and_use_strong_passwords
38. Dan Pinnington, 'Keeping your passwords strong and secure' LAWPRO Magazine December 2013 available at http://www.practicepro.ca/LawPROmag/Keeping_Passwords_Secure.pdf
39. Your ABA, 'Security fundamentals: Passwords' April 2012, available at http://www.americanbar.org/content/newsletter/publications/youraba/201204article12.html
40. Judge Herbert B. Dixon, Jr., 'Worst Passwords of 2013: password & 123456', *The Judges Journal*, Vol. 53 No. 2, 2014 available at http://tinyurl.com/okobfa2 and also at http://www.americanbar.org/publications/judges_journal/2014/spring/worst_passwords_of_2013_password__123456.html
41. Joan Feldman, 'Five Must-Know Password Protection Tips' 9 May 2014, available at http://www.attorneyatwork.com/five-password-protection-tips/
42. 'Create strong passwords' available at https://www.microsoft.com/security/pc-security/password-checker.aspx
43. 'Choosing good passwords in Mac OS X' available at http://support.apple.com/kb/HT1506
44. 'How safe is your password?' available at https://accounts.google.com/PasswordHelp
45. 'How 'Ethical' is your Password?' February 2013, available at http://tinyurl.

com/ny3yxyd and also http://www.americanbar.org/groups/professional_responsibility/services/ethicsearch/ethicstipofthemonth.html

46. https://itunes.apple.com/au/app/google-authenticator/id388497605?mt=8
47. https://itunes.apple.com/au/app/otp-auth/id659877384?mt=8
48. https://www.google.com/intl/en/landing/2step/index.html
49. https://www.dropbox.com/help/363/en
50. http://support.apple.com/kb/ht5570
51. https://www.facebook.com/note.php?note_id=10150172618258920
52. Natalie Kelly, Daniel J. Siegel & John W. Simek, 'More Than a Locked Door' *Law Practice Magazine* Volume 40 Number 2 available at http://tinyurl.com/lcfhz9x and also at http://www.americanbar.org/publications/law_practice_magazine/2014/march-april/more-than-a-locked-door.html
53. https://www.eff.org/Https-everywhere
54. Jeff Richardson, 'A look at the iPhone passcode lock feature' 28 September 2009 available at http://www.iphonejd.com/iphone_jd/2009/09/iphone-passcode-lock.html
55. or Find My iPhone – this will vary from device to device
56. http://support.apple.com/kb/ht2110
57. Natalie Kelly, Daniel J. Siegel & John W. Simek, 'More Than a Locked Door' *Law Practice Magazine* Volume 40 Number 2, March-April 2014 available at http://tinyurl.com/lcfhz9x and also at http://www.americanbar.org/publications/law_practice_magazine/2014/march-april/more-than-a-locked-door.html
58. Peter Krogh, 'Backup Overview' 27 February 2012 available at http://www.dpbestflow.org/backup/backup-overview
59. Noble McIntyre, 'How to Secure Your Paperless Office' 30 October 2013 available at http://lawyerist.com/70726/secure-paperless-office/
60. 'DoD News Briefing - Secretary Rumsfeld and Gen. Myers' 12 February 2002, transcript prepared by The Federal News Service Inc., accessed 6 July 2014 and available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636
61. Wikipedia contributors, 'Social engineering (security),' Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=Social_engineering_(security)&oldid=615406453 (accessed July 12, 2014).
62. David Winder, 'Security pros get caught out by QR codes,' PC & Tech Authority, issue 182, January 2013
63. Mark Hosenball and Warren Strobel, 'Exclusive: Snowden persuaded other NSA workers to give up passwords – sources' 7 November 2013, available at http://www.reuters.com/article/2013/11/08/net-us-usa-security-snowden-idUSBRE9A703020131108
64. Wikipedia contributors, 'Electronic envelope,' Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=Electronic_envelope&oldid=583596044 (accessed July 12, 2014).
65. See paragraph 25

Verbatim

Mineralogy Pty Ltd v Sino Iron Pty Ltd (No 4) [2014] WASC 282 at [59]:

It is necessary to make one final concluding comment on the manner in which this litigation continues to be prosecuted and defended. My comment concerns the importance of civility in the conduct of litigation. Modern litigation is far removed from the procedure and practices that were subjects of daily discussion between those counsel and judges sitting on the Benches of the Inns of Court and at the bar messes in the 19th century. The need for civility, from all participants in the legal process, is often forgotten today. I have remarked more than once in the course of this litigation of the need for polite, respectful interchange. The reiteration in these reasons arises due to a comment in the course of correspondence which was included in the vast amount of affidavit material provided in these applications. In one letter between the solicitors, reference was made to an allegation of conduct by the opposing solicitors said to be 'incongruous with professional ethical obligations'.

I say nothing about the content of the allegation in this case, particularly in circumstances where neither the issue, nor the facts, nor all the correspondence, is before the Court. It suffices to say that as a general matter an allegation of breach of professional obligations should never be made without very careful consideration. One reason for this is that in some circumstances the making such an allegation could itself amount to a breach of ethical obligations. More commonly, though, such allegations can be destructive of the relationships of respect that should exist in litigation, including the respect between opposing solicitors, all of whom are officers of the court. Other legal representatives in the course of practice, whether opposed or not, should always be treated with respect, dignity, and occasionally admiration (even if the language of respect has today become merely a forensic label). This is never inconsistent with the vigorous, even forceful, prosecution of a client's interests.