Surviving as data driven lawyers in the Fourth Industrial Revolution

Peter Leonard[1]

This paper addresses two ways in which lawyers' interface with data, specifically:

- lawyers managing and protecting confidential information, in particular, sensitive information about clients;
- lawyers obtaining data as evidence from third parties.

Parts of this paper discuss:

- 1st challenge: how we run legal businesses
- 2nd challenge: where and how lawyers collect evidence
- The regulatory context – 'legal ethical obligations' and legal sector specific regulation
- Preservation of evidence
- Inadvertent disclosure
- illegally obtained evidence
- May illegally obtained evidence be admitted in legal proceedings?
- Cyber threats to law firms and where they come from
- Disclosure by lawyers of confidential information and exposure of third parties
- How bad can it get for a law firm? The Panama Papers and the Paradise Papers
- How to avoid being a statistic

This paper does not address how lawyers should deal with problems that clients may experience with collection, handling and management of data, and in particular, dealing with notifiable data breaches. Numerous published papers address the new Australian notifiable data breach scheme, including excellent materials available from the Australian Privacy Commissioner.[2]

Data suffuses the business of law. And as data has proliferated, so has the complexity of regulating human relations and the possibilities of establishing causation and inferring correlations.

Previous industrial revolutions liberated humankind from animal power, made mass production possible and brought digital capabilities to billions of people. The Fourth Industrial Revolution[3] is, however, fundamentally different. It is characterized by a range of new technologies that are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human.[4]

---

[1] Peter Leonard is a data, content and technology business consultant and lawyer advising data-driven business and government agencies. Peter is principal of Data Synergies and a Professor of Practice at UNSW Business School (Information Systems and Business and Taxation Law). Peter chairs the IoTAA's Data Access, Use and Privacy work stream, the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of corporate and advisory boards, including of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin, now a large Australian law firm. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant.

[2] Available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

[3] The First Industrial Revolution used water and steam power to mechanise production. The Second used electric power to create mass production. The Third used electronics and information technology to automate production. We are living through the Third, and the concurrent birth, of the Fourth Industrial Revolution.

[4] Klaus Schwab, The Fourth Industrial Revolution, by Klaus Schwab www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab; see also Michele Wucker, How to have a good Fourth Industrial Revolution www.weforum.org/agenda/2018/06/how-to-have-a-good-fourth-industrial-revolution-62ea95e5-16ce-4850-b6f6-f8a88b5690ed/

The Fourth Industrial Revolution brings new technologies that are changing where and how many of us work, what we buy and how we buy it, what we learn and what we delegate to our devices, and how we connect with each other.

1st challenge: how we run legal businesses

The challenge of our digital age to how we run legal businesses can be simply stated:

- Law firms are complex businesses that are operated by humans.
- Humans make mistakes.
- Law firms are a target rich environment for cyberattack.
- Law is a trust business. Trust is hard won and easily lost.
- Data driven processes amplify ability to effect good and to do, or suffer, the bad. Data driven processes enable things that go wrong at a scale and with a velocity that was previously unimaginable.
- The more complex the business, the greater the need for systemised and reliable operational and technical process controls and safeguards, to (1) reduce the risk of things going wrong, (2) detect at early stage when things wrong, and (3) minimise the impact of things that go wrong.
- Many law firms are excellent at lawyering (*what they do*), while also being somewhere between average to rubbish (1) at understanding and systemising their business processes (*how they do what they do*), and (2) in development and implementation of organisational and operational controls and safeguards (that ensure that the law firm *reliably and verifiably does it that way*).
- Outsourcing of digital processes is increasingly a necessary aspect of efficiently managing a modern legal practice. Outsourcing often reduces technological business risk: the outsourcer usually can better manage information security risks that are inherent to their business process and enabling technologies than many in-house technology teams managing similar capabilities delivered over in-house systems. But creation and management of each point of connection to an external service introduces vulnerabilities which must be understood and managed by the law firm. Each point of human connection to external systems is a point of risk and vulnerability to internal failure and to external exfiltration. That risk is often exacerbated by human factors: initial unfamiliarity with new forms of risks, and poor change management on introduction of new processes.
- Digital mishaps attract extensive adverse media coverage. Bad data stories are easy to report but hard to report accurately.
- Data breaches make good headlines, but the technical details are often deathly dull.
- Adverse media commentary usually obscures any distinction between mistakes of a business itself, mishaps of contractors to that business, and malevolent acts of third parties that exploit vulnerabilities of a business.
- Mud is attached to, and sticks, to the most prominent brand that is implicated in any media story.

2nd challenge: where and how lawyers collect evidence

Some of the above observations are now unremarkable, even commonplace. But when we look outwards, at what we do in the course of lawyering, we discover that there are less understood, emerging issues:

- The practice of law is (of course) fact and evidence based.
- We are experiencing an explosion in the availability, quality, range and capabilities for cross-correlation of sources of evidence.
- Digital forensics is today dominated by mobile forensics: one expert suggests that mobile forensics account for over 80 percent of the total digital forensic that global investigators are performing.[5] A single smartphone contains contacts, memos, call records, text messages, instant messages, pictures, videos, and GPS data of a person. But not always readily available: smartphones have strengthened in security over the years to include data encryption and biometric authentication. People also change their phones, on average, every two years and there are constant updates to apps and operating systems.
- As we move to an 'online merge offline world'[6] where sensor hear and see most everything we do, whether online or offline, in the home, at work, in transit or in public, these sources of evidence will be mined through subpoena and other lawful process, or unlawful collection. We are still in early stages of widespread take-up of internet of things (IoT) devices and services, but already we have a myriad of rich evidentiary sources including wearables; smart speakers; building and home automation, surveillance and detection devices; personal wellness devices and other health care trackers and monitors; smart city systems; and toll tags and embedded sensors in vehicles.
- The rise of self-help gathering of digital evidence by potential litigants is little discussed, but problematic and pervasive. Some of what they collect is illegally obtained.
- Australian judges often exercise discretion to admit illegally obtained evidence, particularly in family court proceedings.
- Relevant evidence is often obtained using subpoena issued at the request of a lawyer, over-the-counter by a registrar and without active judicial consideration. Australian lawyers drafting legal process are the key gatekeepers as to how and when subpoena are issued and other legal process used.
- Lawyers have incentives to vigorously assert their clients' rights. The most significant constraint upon a lawyer exaggerating or misrepresenting the client's rights is the lawyer's professional responsibilities.
- Professional responsibilities of lawyers are well articulated as principles, but not well explained as to their application to constrain what lawyers should do and say in relation to issue of subpoena and other legal process. This is a problem, particularly lack of understanding of professional responsibilities of lawyers in relation to new sources of digital evidence.
- Subpoena and other legal process for production of digital evidence are often served on third party service providers and other intermediaries that have no significant incentive to

[5] Cho Mu-Hyun, Explosion in digital evidence coming thanks to IoT and 5G: Hancom GMD January 1, 2019, www.zdnet.com/article/explosion-in-digital-evidence-coming-thanks-to-iot-and-5g-hancom-gmd/

[6] This phrase is taken from Kai-Fu Lee, AI Super-powers: China, Silicon Valley and the New World Order, a book which is essential reading for anyone interested in how artificial intelligence is now disrupting society and business.

resist legal process for production of evidence. Without that incentive, the risk of over-production is substantial.

- The risk of over-production of potentially probative digital data in response to legal process is partially ameliorated in our current, online world (being the Third Industrial Revolution) by the commitment of many major telecommunications service providers and Silicon Valley businesses to transparency as to their responses to legal process, and their willingness to commit legal resources towards ensuring due legal process. Many of these businesses call out and resist overly intrusive (or simply bad) legal process.
- As we move into an online-merge-offline world we increasingly find sources of evidence that are controlled by intermediaries that do not have any commitment to transparency and due process, or the money or access to legal skills required to actively resist requirements to produce.
- Australian legislatures have demonstrated willingness to remove the protection of transparency and knowledge of an affected individual to a third party responding to overly intrusive (or simply bad) legal process.[7]
- In the absence of transparency, or other protections such as human rights laws protecting the affected individual, there is significant risk of abuse of process. In many other jurisdictions, human rights protection operates as an important constraint upon mandatory collection of digital evidence.[8] That is not the case in Australia.
- There are a few examples in Australia of statutory override of mandatory court process: in particular, in relation to My Health Records[9] and access to data collected by telecommunications service providers for the sole purpose of complying with the mandatory data retention scheme. These examples are rare and were only made following public outcry and extensive media interest.[10]
- Another limiting approach would be for prosecuting authorities to voluntarily forebear from some more intrusive collections of evidence. The writer is not aware of any relevant Australian example. For a U.S. example, see the U.S. Department of Justice's guideline *Seeking Enterprise Customer Data Held by Cloud Service Providers*.[11]

[7] By way of one example, the Telecommunications Act 1997 (Cth), as amended in December 2018 to include subsection 317ZF(1), creates offences where (among others) a provider, an employee, a contracted service provider of a provider or an employee of a contracted service provider of a provider, discloses assessment notice information or technical capability notice information, or information obtained in accordance with a notice, to affected individuals, among many other people.

[8] For a succinct summary of the US position, see Wiley Rein, Internet Of Things Cos. Must Prepare For Law Enforcement, August 2018, available at https://www.wileyrein.com/newsroom-articles-Internet-Of-Things-Cos-Must-Prepare-For-Law-Enforcement.html.

[9] Following extensive criticism as to lack of controls, The Australian Parliament passed the My Health Records Amendment (Strengthening Privacy) Act 2018 (as assented to on 10 December 2018) which amended the Health Records Act 2012 to: remove the ability of the My Health Record System Operator to disclose health information in My Health Records to law enforcement and government agencies without an order by a judicial officer or the healthcare recipient's consent.

[10] The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2014 amended the Telecommunications Act 1997 to require certain telecommunications and internet service providers to retain prescribed information or documents (metadata) for a period of two years for the purposes of access by national security authorities, criminal law-enforcement agencies and enforcement agencies. After amendments, the Act prohibited civil litigants from being able to access metadata that is retained by a service provider solely for the purpose of complying with the proposed Scheme: see Bills Digest no. 89 2014–15 as available at www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1415a/15bd089.

[11] U.S. Department of Justice (Computer Crime and Intellectual Property Section, Criminal Division), Seeking Enterprise Customer Data Held by Cloud Service Providers, December 2017, available at www.justice.gov/criminal-ccips/file/1017511/download.

Regulatory context – 'legal ethical obligations' and legal sector specific regulation

> "The phrase 'legal ethics'... is an oxymoron to the extent that 'legal' implies mandatory laws, whereas 'ethics' for many connotes discretionary rules. In this latter sense, some use the term 'ethics' to distinguish rules that are professionally binding on a lawyer (ethical rules) from rules that are legally binding (legal rules). But such a practice conveys the incorrect impression that the ethical and legal rules are mutually exclusive, and that legal rules are more important than ethical rules."[12]

The Australian Solicitors' Conduct Rules were developed by the Law Council of Australia and promulgated in June 2011 as a common set of professional obligations and ethical principles for Australian solicitors when dealing with their clients, the courts, their fellow legal practitioners, regulators and other persons. The Rules[13] have been adopted in South Australia, Queensland, Victoria, New South Wales (as the Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015)[14] and the Australian Capital Territory.

The corresponding (but quite different) instrument for barristers in NSW is the is the Legal Profession Uniform Conduct (Barristers) Rules 2015[15], broadly based on the Australian Bar Association's Model Rules.[16]

A number of relevant provisions from the relevant Australian Solicitors' Conduct Rules are extracted in the annexure to this paper.

The Rules are a not legislative rules in the traditional sense: they might be called 'legal ethical obligations'.[17] The Rules are non-exhaustive codification of ethical principles to be observed that provides guidance to a legal practitioner on how that ethical principle applies in particular circumstances.

In 2018 the Law Council's Professional Ethics Committee undertook consultations as to possible revisions of the Rules, taking into account submissions in response to a detailed Discussion Paper[18] released in February 2018. That review has not yet resulted in revised Rules.

The Law Council has also released a version of the Australian Solicitors' Conduct Rules with an accompanying commentary. The Commentary[19], the Discussion Paper and guidance material from the State Law Societies are the principal secondary sources relating to the Rules.

In NSW and Victoria, the Rules operate under section 6 of the Legal Profession Uniform Law, which defines "professional obligations" as including:

---

[12] G Dal Pont, Lawyers' Professional Responsibility (4th ed, 2010), page 4.

[13] Available at www.lawcouncil.asn.au/files/web-pdf/Aus_Solicitors_Conduct_Rules.pdf; also www.lawsociety.com.au/practising-law-in-NSW/rules-and-legislation/rules.

[14] Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015 (NSW), available at www.legislation.nsw.gov.au/#/view/regulation/2015/244.

[15] Available at www.legislation.nsw.gov.au/inforce/5a7fbed4-700d-45da-84dc-b6f6b0fb2870/2015-243.pdf

[16] See further www.nswbar.asn.au/coming-to-the-bar/uniform-law

[17] A characterisation suggested by the authors of the Australian Law Reform Commission's Discussion Paper, Discovery In Federal Courts (2010, ALRC CP 2), in Chapter 2: Ensuring Professional Integrity: Ethical Obligations and Discovery. Available at www.alrc.gov.au/publications/discovery-federal-courts-alrc-cp-2

[18] www.lawcouncil.asn.au/docs/4dde1ab8-4606-e811-93fb-005056be13b5/2018%20Feb%20%2001%20ASCR%20Consultation%20Discussion%20Paper.pdf

[19] www.lawcouncil.asn.au/files/web-pdf/SolicitorsConductRulesHandbook_Ver3.pdf

(a) duties to the Supreme Courts; and

(b) obligations in connection with conflicts of interest; and

(c) duties to clients, including disclosure; and

(d) ethical standards required to be observed,

that do not otherwise arise under this Law or the Uniform Rules.[20]

Accordingly, a finding of "unsatisfactory professional conduct", defined as including "conduct occurring in connection with the practice of law that falls short of standards of competence and diligence that a member of the public is entitled to expect of a reasonably competent lawyer"[21], may be made regardless of where there is a technical breach of the Rules. "Professional misconduct" is defined to include "a substantial or consistent failure to reach and maintain a reasonable standard of competence and diligence, and conduct occurring whether or not in connection with the practice of law that would, if established, justify a finding that the lawyer is not a fit and proper person to engage in legal practice".[22]

Key legal ethical obligations include, most relevantly:

- A solicitor's duty to the court and the administration of justice is paramount and prevails to the extent of inconsistency with any other duty.
- A solicitor must not engage in conduct, in the course of practice or otherwise, which demonstrates that the solicitor is not a fit and proper person to practise law, or which is likely to a material degree to be prejudicial to, or diminish the public confidence in, the administration of justice, or bring the profession into disrepute.
- 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, subject to very limited exceptions.
- A solicitor must take care to ensure that the solicitor's advice to invoke the coercive powers of a court is reasonably justified by the material then available to the solicitor and is appropriate for the robust advancement of the client's case on its merits.
- A solicitor must not in any action or communication associated with representing a client make any statement which grossly exceeds the legitimate assertion of the rights or entitlements of the solicitor's client, and which misleads or intimidates the other person.

Clearly, exaggerated statements of entitlement as made by a party's legal counsel to a prospective subpoena recipient of a party's rights to require production of digital data may constitute unsatisfactory professional conduct, as well as actionable misleading or deceptive conduct.

[20] Definition in section 6 of the Legal Profession Uniform Law (NSW) No 16a

[21] Legal Profession Uniform Law s296, Legal Profession Act 2006 (ACT) s386; Legal Profession Act 2007 (QLD) s418; Legal Profession Act 2006 (NT) s464; Legal Profession Act 2007 (WA) s402; Legal Profession Act 2007 (TAS) s420; Legal Practitioners Act 1981 (SA) s68.

[22] Legal Profession Uniform Law s297; Legal Profession Act 2006 (ACT) s389; Legal Profession Act 2007 (QLD) s420; Legal Profession Act 2006 (NT) s466; Legal Profession Act 2007 (WA) s404; Legal Profession Act 2007 (TAS) s422; Legal Practitioners Act 1981 (SA) s70.

Preservation of evidence

The duty to preserve digital evidence based on the existence of pending, threatened, or reasonably foreseeable litigation arises under the common law. It also can arise from a number of other sources, including a contract, a voluntarily assumed duty, a statute or regulation, an ethical code, or another special circumstance.

Related to a party's duty not to destroy discoverable evidence is a lawyer's obligation to instruct clients to preserve all potentially relevant information. Solicitors should ensure that their clients understand the nature and extent of their discovery obligations and have a duty to ensure that full and proper disclosure of documents is made.

Section 177(1) of the now repealed New South Wales Legal Profession Regulations stated that lawyers could not advise clients to destroy documents in their possession or control if they were aware that "it [was] likely that legal proceedings [would] be commenced in relation to which the document may be required". While this provision does not appear in the Uniform Solicitor's Conduct Rules, it seems unarguable that such advice would be in breach of a solicitor's paramount duty to the court and responsibility to advise clients about disclosure obligations.[23]

Under the common law, if a party destroys discoverable material, this can constitute contempt, particularly if litigation is already on foot. In Australia, courts have the power to stay and or dismiss proceedings, in whole or in part, where a party has deliberately destroyed discoverable material.[24] Clients can often be unaware of their duties in regard to disclosure and preserving evidence. Indeed, many clients may be tempted to destroy, delete or remove documents unfavourable to their case. As digital information, including cloud-based information and social media content, may be discoverable, legal practitioners should be particularly careful to advise clients not to destroy information that may be relevant to their case. The destruction of digital evidence may lead to the striking out of claims and other adverse consequences for clients. Of course, it follows that solicitors should never advise clients to 'clean up' their digital holdings, including social media accounts, in preparation for litigation.

Inadvertent disclosure

Rule 31 of the Australian Solicitors Conduct Rules 2012 deals with what lawyers should do when they receive confidential but inadvertently disclosed materials.

Inadvertent disclosure occurs where a lawyer receives material which the lawyer knows, or ought reasonably suspect, to be confidential and which the lawyer is aware has been disclosed inadvertently. If these circumstances exist, then upon receipt the lawyer:

- must not use the material, we
- must return, destroy or delete the material immediately, and

[23] McCabe v British American Tobacco Australia Service Ltd [2002] VSC 73. See further Bathurst CJ, 'Tweeters, Posters and Grammers Beware: Discovery and Social Media Evidence', paper delivered on 21 June 2016, available at www.supremecourt.justice.nsw.gov.au/Documents/Publications/Speeches/2016%20Speeches/Bathurst%20CJ/Bathurst_20160621.pdf

[24] Palavi v Radio 2UE Sydney Pty Ltd [2011] NSWCA 264; Palavi v Queensland Newspapers Pty Ltd [2012] NSWCA 182; Arrow Nominees Inc v Blackledge [2000] EWCA Civ 200; [2000] All ER (D) 854.

- should notify the sender (whether a solicitor or otherwise) of the steps we have taken to prevent inappropriate use of the material.

Where a lawyer only becomes aware that material is confidential and has been disclosed inadvertently after commencing review of the material, the lawyer should notify the sender immediately, not review further the material and take steps to return or destroy the material.

If after receipt of the confidential but an inadvertently disclosed document a lawyer is instructed by a client to review it, the lawyer must refuse to do so.[25]

Dealing with Subpoena

When may subpoena be reasonably issued to gather digital evidence?

Different States and different courts may have slightly different rules, and these should be considered by any party to court proceedings when issuing a subpoena.

Broadly, unless a party is represented by a solicitor in the proceedings, or if the proceedings are in the Federal Court or the small claims division of the Local Court, leave of the court is required.[26]

A subpoena must have a 'legitimate forensic purpose', meaning that the subpoena is likely to uncover something that will have a significant impact on the outcome of a case. In short, there needs to be a good reason for issuing the subpoena. The tests for this are:

- criminal: is it 'on the cards' that the documents would materially assist the accused's defence?[27]
- civil: is it likely that the documents will materially assist on an identified issue, or is there a reasonable basis (beyond mere speculation) that they will be likely to assist?

The law does not allow subpoena to be issued for 'mere fishing expeditions'. "Fishing can be argued where the pursuit of information is random, unguided and the pursuer has no case but seeks to build one".[28] That is, if the subpoena is served not for the purpose of requiring production of specific documents which the person subpoenaed is reasonably expected to hold, but with the intention of seeing what documents may exist, and whether the issuing party has a case at all. There must be something beyond speculation: some reasonably based ground for belief that takes the demand beyond a mere fishing expedition.

The court maintains control over the subpoena to produce at three distinct stages. The court may:

- set aside a subpoena and excuse the respondent from complying with it;
- refuse to allow the parties to examine the documents produced on the subpoena; and
- control the admissibility of evidence obtained on the subpoena.

[25] See further the unanimous decision of the High Court of Australia in Expense Reduction Analysis Group Pty Ltd and Armstrong Strategic Management and Marketing Pty Ltd (2013) 250 CLR 303, particularly at 325.

[26] See Uniform Civil Procedure Rules 2005 (NSW)(**UCPR**) rule 33.5, UCPR regulation 7.3, and rule 24.01(1) of the Federal Court Rules 2011 (Cth) and section 109X(1)(a) of the Corporations Act 2001 (Cth).

[27] R v Salem [1999] NSWCCA 86, Commissioner of Police v Hughes [2009] NSWCA 306.

[28] Martin & Martin and Anor (No 2) [2014] FamCA 232 per Cronin J

Different considerations operate at each of these stages.[29]

A subpoena must describe with reasonable particularity the documents for which it calls. This is a judgment that must be made by reference to an individual subpoena, and in the circumstances of a particular recipient of the subpoena.

A subpoena recipient may argue that the subpoena is invalid, oppressive (i.e. the subpoena recipient would be forced to engage in an unduly burdensome or expensive exercise)[30], vexatious, an abuse of the process of the court or should otherwise be set aside[31]

A subpoena is liable to be set aside as oppressive if it is cast in terms that it places on the person to whom it is addressed the same kind of burden as is placed on a party required to give discovery of documents. In this sense, a subpoena must not require the recipient to form a judgment about the issues between the parties and the relationship of the documents to those issues.

A subpoena is also liable to be set aside as oppressive if, although not amounting to an obligation tantamount to discovery, it nonetheless imposes an onerous task on the recipient to collect and produce documents many of which can have no relevance to the litigation. That is, a subpoena must be couched in terms of reasonable particularity, and if it calls for the production of a large number of documents of doubtful relevance, it will be regarded as oppressive and an abuse of process.

A subpoena recipient may apply to the court, either before the return date or on the return date, to set aside the subpoena.

if a person affected is not the recipient of the subpoena, the person can still apply to the court to have the subpoena set aside if that person has a sufficient interest in the material sought by the subpoena. The subpoena can be set aside on the same grounds as discussed above.[32] For example, if you are a company, and a subpoena is issued to one of your suppliers for their contracts with you, you would have a sufficient interest in the material sought by the subpoena. The categories of people who have a sufficient interest are not closed, and courts have held that any person whose legal rights will be interfered with by the execution of the subpoena is deemed to have a sufficient interest.

The fact that documents or information sought under subpoena are confidential, commercially sensitive or comprise personal information does not mean that the subpoena may be set aside. However, it does mean that a court should more closely scrutinise the subpoena to ensure that the material sought by it is relevant to the case and not oppressive in any way.[33] This is particularly so if the confidentiality in issue is that of a third party.[34] If a party seeking to have the subpoena set aside fails to have the subpoena set aside but still wishes to preserve the confidential nature of the

[29] National Employers' Mutual General Association v Waind [1978] 1 NSWLR 372

[30] Commissioner for Railways v Small (1938) 38 SR (NSW) 564.

[31] National Employers' Mutual General Association v Waind [1978] 1 NSWLR 372; Roux v Australian Broadcasting Commission [1992] 2 VR 577

[32] Rule 33.4 of UCPR; also Hunt v Russell; Schultz v Russell (1995) 63 SASR 402

[33] In the Matter of North Coast Transit Pty Ltd [2013] NSWSC 1912.

[34] Drivetime Radio Australia Pty Ltd v Pivotal Creative Solutions Pty Ltd Trading as Broadcast Group [2010] NSWSC 763

material, it is best to seek confidentiality/ restricted access orders from the court, or leave from the court to mask or redact irrelevant and/or confidential information.[35]

Illegally obtained evidence

The Workplace Surveillance Act 2005 (NSW) provides a legal mechanism for employers to monitor and record activities of their employees, qualified by certain rights of employees.

The Surveillance Devices Act 2007 (NSW) regulates the installation, use, maintenance and retrieval of surveillance devices in NSW.

These Acts relevantly regulate use of 'surveillance devices', means a data surveillance device, a listening device, an optical surveillance device, or a tracking device. A 'device' includes instruments, apparatus and equipment.

The statues create offences for conduct of these activities outside the specific permissions granted by the statutes.

For example, section 11 of the Surveillance Devices Act 2007 (NSW) provides:

> A person must not publish, or communicate to any person, a private conversation or a record of the carrying on of an activity, or a report of a private conversation or carrying on of an activity, that has come to the person's knowledge as a direct or indirect result of the use of a listening device, an optical surveillance device or a tracking device in contravention of a provision of this Part.

'Record' includes an audio, visual, or audio-visual record, a record in digital form and a documentary record prepared from a record referred to in (a) or (b). 'Report' of a conversation or activity includes a report of the substance, meaning or purport of the conversation or activity: section 4.

If a person is not a party to a private conversation it is also an offence for them to knowingly install, use or cause to be used, or maintain a listening device to overhear, monitor, or listen to the private conversation. For example, it is an offence for a person to install an audio bug surveillance device in his home in order to overhear, monitor, or listen to private conversations his wife has with other people, for example to listen to what she says in telephone conversations with other people. In addition, if that person installed a bug on the telephone to intercept and listen or record both sides of the telephone conversation, this would be a federal offence under the Telecommunications (Interception and Access) Act 1979 (Cth).

In New South Wales it is legal to record a conversation to which the person is a party to if all parties consent, expressly or impliedly, to the listening device being used.

However, the relevant rules differ substantially between the Australian and Territories.[36]

[35] Grace v Grace (No 8) [2014] NSWSC 419

[36] Subject to important conditions and exceptions one party may consent in Victoria (Surveillance Devices Act 1999 (Vic)), Queensland (Invasion of Privacy Act 1971 (Qld)), the Northern Territory (Surveillance Devices Act 2007 (NT)); but not in WA (Surveillance Devices Act 1998 (WA)), South Australia (Listening and Surveillance Devices Act 1972 (SA)), the Australian Capital Territory (Listening Devices Act 1992 (ACT)), NSW (Surveillance Devices Act 2007 (NSW)) and Tasmania (Listening Devices Act 1991 (TAS)).

In New South Wales it is also legal to record a conversation to which a person is a party to if one principal party (e.g. the person recording) consents to the recording of the conversation and it is either:

- reasonably necessary for the protection of the lawful interest of that principal party, or
- the recording is not made for the purpose of communicating or publishing the conversation or a report of it to persons who are not parties to the conversation.[37]

The onus of proof for establishing the above exception lies on the party seeking to establish the exception, and that onus is on the balance of probabilities.

There is a distinction between lawful interest and legal interest. Lawful interests are interests which are not unlawful; its meaning is similar to the expressions 'legitimate interests' or 'interests conforming to law'.[38]

Whether a recording is reasonably necessary for the protection of the lawful interests of a party is objectively determined, having regard to the lawful interest existing at the time of making the recording.

Some common scenarios:

- A person in need of protection covertly records the abuse/assaults directed at her.
- A person in need of protection records child contact changeovers.
- It is not an offence for one party to record a changeover at McDonalds with the other party because it is in a public space, with no reasonable expectation that conversation will not be heard by others
- It is not an offence for a woman being assaulted by her partner to record the assault secretly (e.g. mobile phone set to record and placed in her pocket).[39]

If a person has knowledge of a private conversation or the carrying on of an activity that was obtained directly or indirectly through the use of a listening device, an optical surveillance device or a tracking device in contravention of a provision of Part 2 of the Act (Regulation of installation, use and maintenance of surveillance devices), that person is prohibited from publishing or communicating to any person:

- knowledge of the private conversation; or
- a record of the carrying on of the activity, or
- a report of a private conversation or carrying on of an activity.

There are several exceptions that apply. Most relevantly, communication or publication is allowed if it is no more than is reasonably necessary in connection with an imminent threat of serious violence to persons or of substantial damage to property. Of course, a private conversation or recordings of activities can also be shared if it was obtained in such a manner that does not constitute a contravention against this Act.

[37] Sections 7(3)(b)(i) and (ii).

[38] Violi v Berrivale Orchards Ltd (2000) 173 ALR 518, 523

[39] These examples are taken from the excellent Legal Guide to Surveillance Legislation in NSW as prepared by the Women's Legal Services NSW and available at SmartSafe www.smartsafe.org.au/legal-guides/legal-guide-surveillance-legislation-nsw

May illegally obtained evidence be admitted in legal proceedings?

Australian courts have adopted a discretionary approach to determining whether to admit improperly obtained evidence, at least since the 1970 judgment of Barwick CJ in R v Ireland.[40] Section 138 of the Evidence Act 1995 (C'th) provides that illegally or improperly obtained evidence is prima facie inadmissible unless the desirability of admitting the evidence outweighs the undesirability of admitting it. The decisional criteria for weighing the desirability and undesirability of admitting the evidence are defined in s138(3) as being:

- the probative value of the evidence;
- its importance in the proceedings; the nature of the alleged crime;
- the gravity of the impropriety or illegality and whether it was deliberate or reckless or contrary to a right recognised by the International Covenant on Civil and Political Rights;
- whether any other proceeding has been, or is likely to be, taken in regard to the misconduct; and the difficulty of obtaining the evidence without the impropriety or illegality.

These factors are non-exhaustive. No preponderance is ascribed to any of the matters identified in s 138(3) over others; each, if applicable, is to be weighed in the balance in favour of or against the exercise of discretion.[41] Relevant impropriety includes conduct which, although not either criminal or unlawful, is quite or clearly inconsistent with minimum standards that society expects and requires of those entrusted with law enforcement.[42]

Cyber threats to law firms and where they come from

The most significant cyber threats that law firms should be aware of are:

- Data breaches
- Supply chain compromise (i.e. hackers inserting themselves into an email conversation relating to a transfer of funds and then redirecting funds to themselves)
- Phishing
- Ransomware

The primary risk is *data exfiltration*: primarily a security breach that occurs when an individual's or organization's data is illegally copied. Generally, *data exfiltrations* are targeted attacks where the hacker's primary intent is to find and copy specific data from the target machine. The hackers gain access to the target machine through a remote application or by directly installing a portable media device. Statistically, these breaches mainly occurred on systems with a vendor-set default password or very common or easy passwords.

---

[40] R v Ireland (1970) 126 CLR 321 per Barwick CJ. See further the Judicial Commission of New South Wales, Civil Trials Bench Book, at [4-1610] General discretion to exclude evidence, as available at www.judcom.nsw.gov.au/publications/benchbks/civil/discretions_to_exclude_evidence.html. For an excellent analysis by Bathurst CJ of operation of section 138, see Bathurst, TF and Schwartz, 'Illegally or improperly obtained evidence: In defence of Australia's discretionary approach", Judicial Review: Selected Conference Papers: Journal of the Judicial Commission of New South Wales (Volume 13 Issue 1 (Sep 2016)), also available at www.supremecourt.justice.nsw.gov.au/Documents/Publications/Speeches/2016%20Speeches/Bathurst%20CJ/Bathurst_20160302.pdf. For an example of application of s 138, see ASIC v Sigalla (No 2) [2010] NSWSC 792.

[41] ASIC v Macdonald (No 5) [2008] NSWSC 1169 at [27].

[42] Robinson v Woolworths Ltd (2005) 64 NSWLR 612 at [22]–[23]

Most data breaches remain due to human error or poor human practices, not smart activities of malicious actors.[43] Most corporations, and many law firms, are now reasonably good at technical information security.[44] Many businesses remain poor at operational information governance.

It is often not obvious to a law firm that the firm has been hacked – in the vast majority of cases, hackers are using stolen credentials, as opposed to breaking through technical walls.

Even where technical walls are breached, extraction may be by slow burn and therefore not discernible by spike in traffic.

The primary external intrusion threat to date stems from cyber criminals with a financial motive.

The move to digital services in law will provide further avenues for malicious cyber exploitation. (i.e. the extensively (mis-)reported misuse of the Pexa property settlement system.)

There are several factors that make law firms an attractive target for cyber-attack. Law firms:

- hold sensitive client information,
- handle significant funds, and
- are a key enabler in commercial and business transactions,
- often place significant reliance upon professional ethics of lawyers, and many lawyers excessively empower their assistants. Many law firms are a data breach waiting to happen.

Smaller firms may be less attractive targets for financial scale, but more attractive to exfiltration because of less secure networks.

There has been a rapid rise in unconventional cyber-threats – for example, a 2016 media report of hackers over a period of 94 days extracting 7 gigabytes of data from Cravath and Weil Gotshal, allegedly targeting for M&A related client confidential information that could be used for insider trading.[45]

The risks are greater for law firms that advise particularly sensitive clients or work in locations without sophisticated government cybersecurity operations.

---

[43] See further U.K. National Cyber Security Centre and Law Society of England and Wales, The cyber threat to the UK legal sector, 2018, available at https://www.ncsc.gov.uk/content/files/protected_files/article_files/the_cyber_threat_to_uk_legal_sector_NCSC_2.pdf. There are many studies that confirm this observation industry sectors and in multiple jurisdictions. See, for example, the Notifiable Data Breaches Quarterly Statistics Report as published each quarter by the Office of the Australian Information Commissioner (**OAIC**), available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/. The UK Information Commissioner's Office reported in September 2018 that legal sector data security incidents had risen by a significantly above average 112% in two years, with the justice sector up 128% (the average across all sectors being 75%). Human error (as opposed to a cyber incident) accounted for the vast majority of incidents, led by data being emailed to the wrong recipient: https://www.legaltechnology.com/latest-news/ico-legal-sector-data-breach-reports-surge-by-112-in-two-years/.

[44] Principally because the standards, methodologies and tools for managing information security are now relatively mature, and information systems management is now a well development discipline. By contrast, prudent information governance, and training of humans as to good operational practices and processes to reliably protect information, is a relatively young field. See further OAIC, Guide to securing personal information, June 2018, which provides guidance on the reasonable steps entities are required to take under the *Privacy Act 1988* (Cth) to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure; also National Institute of Standards and Technology (NIST), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018 and cross-referenced publications there cited, at https://www.nist.gov/publications/risk-management-framework-information-systems-and-organizations-system-life-cycle.

[45] Wall Street Journal, 'Hackers Breach Law Firms, Including Cravath and Weil Gotshal', March 29 2016 www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504

However, nation states are likely to play an increasingly significant role in cyber-attacks at a global level, to gain strategic and economic advantage. U.S. figures (query their reliability) suggest nation state attackers of private businesses account for 21% of U.S. data breaches, stealing steal data to advance espionage activities or State related business interests.[46]

Firms acting for organisations that engage in work of a controversial nature such as life sciences, or acting for fossil fuel businesses and global corporations, may also be targeted by groups with a political or ideological agenda.

Disclosure by lawyers of confidential information and exposure of third parties

The rise in data breaches has led to a significant increase in scrutiny of a company's cyber security as a data breach. Businesses that do not implement reasonable cyber security measures can face both regulatory investigation and shareholder class action. Data breaches can result in:

- Business disruption
- Significant costs in responding to a data breach
- Reputational damage
- Loss of business and revenue
- Reduction in capital/share value of the business
- Loss of valuable intellectual property/confidential information
- Substantial costs in regaining consumer confidence that the organisation can be trusted with personal information/data
- Regulatory fines
- Compensation claims by individuals/class actions.

In addition to constituting a breach of a lawyer's legal ethical obligations, disclosures of confidential information of clients may give rise to other exposures to legal liability.

The Privacy Act 1988 (C'th) includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government (and Norfolk Island) agencies (APP entities). APP 11 requires APP entities to take active measures to ensure the security of personal information they hold and to actively consider whether they are permitted to retain this personal information. Specifically, APP 11.1 states that an APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

The small business exception to the federal Privacy Act (in section 6C, but with various important carve-ins[47]) excludes businesses with an annual turnover of less than $3 million in aggregate global group revenue. Accordingly, may law firms are not regulated 'APP' entities. However, the fiduciary obligations of law firms are likely to create liability exposure for law firms to clients suffering loss

[46] See further The Council of Economic Advisers (U.S. White House), The Cost of Malicious Cyber Activity to the U.S. Economy, February 2018, www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[47] See OAIC, Privacy business resource 10: Does my small business need to comply with the Privacy Act?, July 2015 www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10.

arising out of inadvertent disclosures of client confidential information, at least where the law firm failed to take reasonable steps to protect that client information.[48]

The more difficult questions are:

- whether obligations of confidentiality can be asserted against third parties to whom that confidential information has been disclosed, and
- whether law firms may be fully exposed to all loss that arises from such exposures.

Equitable principles protecting confidential information operate together with principles governing fiduciary obligations. Given that equity acts on the conscience of a person, a third party recipient of confidential information cannot escape liability, if knowing, the information to be confidential, he or she makes unauthorised use or disclosure of that information.[49] To establish knowledge, it is necessary to look to the facts of each case. Documents marked confidential will convey actual knowledge that the documents were intended to be confidential (as opposed to being determinative of confidentiality), as will a third party closing their eyes to the obvious for fear of discovering confidentiality.[50] Constructive knowledge is also sufficient in Australia, being knowledge of information that a reasonable person in the third party's position would have appreciated was confidential.[51] A third party recipient of improperly disclosed personal information may therefore be restrained from further disclosure, or making use, of improperly disclosed personal information.[52]

Disclosures of confidential information of clients by lawyers may give rise to an obligation for the lawyer as fiduciary to account to the client. In limited circumstances, that obligation to account may also extent to third parties, and lead to an award against misfeasor of all profit arising out of improperly obtained confidential information, and not just the profit directly attributable to a particular misuse of that confidential information. As recently stated by Gageler J in the judgement of the High Court of Australia in Ancient Order of Foresters in Victoria Friendly Society Limited v Lifeplan Australia Friendly Society Limited[53], it is not necessary that the fiduciary need to act dishonestly or fraudulently or otherwise than in good faith, though:

> Where a fiduciary does act dishonestly and fraudulently, however, the dishonest and fraudulent character of the breach of fiduciary duty is not without consequence for the intensity of the equitable remedies available against the defaulting fiduciary. More important for present purposes is that the dishonest and fraudulent character of the conduct of the fiduciary gives rise to the potential for similar remedies to be available in equity against another person who might knowingly participate in the fiduciary's breach. Knowing participation by a non-fiduciary in a dishonest and fraudulent breach of fiduciary duty is conduct which is regarded in equity as itself unconscionable and as attracting equitable

[48] Applying the principles set out in Beach Petroleum NL v Abbott Tout Russell Kennedy [1999] NSWCA 408. See further Marshall v Prescott (No 3) [2013] NSWSC 1949 and Peter Moran and Tim Seton, The Scope of a Solicitor's Fiduciary Duty, LSJ, December 2014.

[49] Foster v Mountford and Ridby Pty Ltd (1976) 14 ALR 71, 75; G v Day [1982] 1 NSWLR 24 at 25; Wheatley v Bell [1982] 2 NSWLR 544 at 550.

[50] Attorney-General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109 per Lord Goff at 281.

[51] Wheatley v Bell [1982] 2 NSWLR 544 at 54

[52] The principles under Australian law for establishing a breach of conference claim against a third party, and the available remedies (including equitable compensation for embarrassment, anxiety and distress) and injunctive relief, are well summarized by Mitchell J in Wilson v Ferguson [2015] WASC 15 at [43]–[85]

[53] Ancient Order of Foresters in Victoria Friendly Society Limited v Lifeplan Australia Friendly Society Limited [2018] HCA 43, at http://eresources.hcourt.gov.au/showCase/2018/HCA/43

> remedies against the knowing participant of the same kind as those available against the errant fiduciary.
>
> Knowing participation in a dishonest and fraudulent breach of fiduciary duty includes knowingly assisting the fiduciary in the execution of a "dishonest and fraudulent design" on the part of the fiduciary to engage in the conduct that is in breach of fiduciary duty. The requisite element of dishonesty and fraud on the part of the fiduciary is met where the conduct which constitutes the breach transgresses ordinary standards of honest behaviour. Correspondingly, the requisite element of knowledge on the part of the participant is met where the participant has knowledge of circumstances which would indicate the fact of the dishonesty on the part of the fiduciary to an honest and reasonable person.[54]

Given the potential impact of extent of operation of equitable principles protecting confidential information and of fiduciary obligations, private rights of action for invasions of privacy will generally not be the principal concern of law firms in relation to data breaches that they may suffer.

However, it should be noted that under the Privacy Act 1988 (Cth), individuals have the right to make complaints to the Privacy Commissioner if they believe that their privacy has been breached by an organisation. The Privacy Commissioner then investigates the complaint and may make a finding about whether the individual's privacy has been breached. If the Privacy Commissioner finds that there has been a privacy breach, the Commissioner has the power to make a determination that certain remedies be provided to the individual whose privacy has been breached, including requiring the organisation to pay compensation to the individual whose privacy has been breached. Remedies awarded by the Privacy Commissioner have included the following:

- An apology.
- A requirement that the agency adopts and implements particular remedial measures in response to privacy breaches.
- A requirement that the agency reviews its privacy/information handling policies and procedures and conduct staff training.
- A requirement that the agency reviews new remedial measures adopted and reports the findings of that review to the OAIC.
- Compensation for non-economic loss ranging from $1,000 to $20,000.
- Reimbursement of reasonably incurred expenses ranging from $3,000 to $5,830.

The Privacy Commissioner can also apply to the Federal Court or Federal Circuit Court for an order requiring an entity to pay a fine for certain privacy breaches or breaches of the credit reporting provisions under the Act. Depending on the type of breach, the fine can range from $525,000 to $2.1 million for a body corporate and from $105,000 to $420,000 for any other entity.

If an entity is fined for a privacy breach or breach of the credit reporting provisions, then an individual who has suffered loss or damage as a result of the breach can make an application to the Federal Court or the Federal Circuit Court for a compensation order for loss or damage suffered, including injury to feelings and humiliation and economic loss.

[54] Ibid.

The status of the private right to sue for a breach of privacy has been unclear in Australia for many years. The High Court left open the possibility of such a cause of action in Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd in 2001.[55] Since then, a tort of invasion of privacy has been recognised by two lower court decisions: Grosse v Purvis in the District Court of Queensland[56] and Doe v Australian Broadcasting Corporation in the County Court of Victoria[57]. However, both cases were settled before appeals by the respective defendants were heard. There have also been cases where the existence of a common law right to sue for breach of privacy has been questioned.

The failure of a right to sue for invasion of privacy to develop at common law has led to calls for the introduction of a statutory right to sue. Over the last 10 years, the Australian Law Reform Commission, the NSW Law Reform Commission and other State and Territory reviews have recommended creation of a statutory right of action for serious invasions of privacy. Media organisations have vociferously opposed introduction of such a right, arguing that it would chill investigative journalism. Neither the Federal nor any State government introduced a statutory right, instead addressing certain more narrow invasions of privacy – addressing non-consensual filming and publication of records of sexual activity or use of public facilities and so on.

In the absence of the development of a common law action for breach of privacy, the most common avenue to seek compensation where there has been an interference with privacy is via a complaint to the Australian Privacy Commissioner pursuant to the Privacy Act 1988 (Cth). For the time being, the prospects for recovering substantial compensation pursuant to operation of the Privacy Act 1988 seem remote. In 2017, a class action against NSW Ambulance Service was brought on behalf of 130 ambulance staff whose medical records were accessed without authorisation by a NSW Ambulance contractor and sold to personal injury lawyers. The law firm involved in the class action, Sydney law firm Centennial Lawyers, said the total damages could reach “millions of dollars”, with individuals claiming for pain and suffering, humiliation, psychological injuries and economic loss.[58]

In June 2018 the same Sydney law firm said it was considering initiating a class action against software-as-a-service provider PageUp, which had released details of a possible data breach that took place in May. Centennial Lawyers today has reached to 17 organisations following media reports that a “massive data breach” may have put personal and confidential information of job seekers and employees from these companies at risk.

How bad can it get for a law firm? The Panama Papers and the Paradise Papers

There has also been spectacular growth in activities of the hacktivist community, targeting law firms to achieve political, economic or ideological ends.

The Panama Papers and the Paradise Papers are the two high profile examples.

[55] [2001] HCA 63

[56] [2003] QDC 151; (2003) Aust Torts Reports 81-706

[57] Jane Doe v Australian Broadcasting Corporation & Ors [2007] VCC 281

[58] Sydney Morning Herald 18 November 2017, ‘Paramedics launch class action over the sale of their medical records to personal injury solicitors’, www.centenniallawyers.com.au/home/our-work/class-actions/

Panama Papers (Mossack Fonseca)

This was an exfiltration (announced in April 2016) of 2.6 terabytes of data (11.5 million documents)[59] from the Panama-based law firm Mossack Fonseca.

A German journalist was contacted by an anonymous source who insisted on the use of encrypted communications for every contact. The journalist claims to have no knowledge of who the leaker was, only that the he or she leaker didn't want any payment, saying that exposing the "crimes" of Mossack Fonseca was enough.

The International Consortium of Investigative Journalists analysed the data and published information about financial dealings of clients of Mossack Fonseca in the Panama Papers series of articles.

At the time Mossack Fonseca was the world's fourth largest provider of offshore financial services. Founded in 1977, it became a key player in the global offshore industry and acted for about 300,000 companies. More than half were registered in British tax havens.

In March 2018 Mossack Fonseca announced in a statement that "The reputational deterioration, the media campaign, the financial circus and the unusual actions by certain Panamanian authorities, have occasioned an irreversible damage that necessitates the obligatory ceasing of public operations at the end of the current month".[60]

The data breach killed the firm.

Paradise Papers (Appelby)

At 1.4 terabytes in size, the Paradise Papers exfiltration is second only to the Panama Papers of 2016 as the biggest data leak in history. Consider the task: 13.4m 'documents' in heterogeneous data formats (emails, PDFs, text documents, images, database files), analysed by (again) the International Consortium of Investigative Journalists (380 journalists from 96 media groups in 67 countries), over a period of one year.[61] Diverse data formats are hard to ingest and cross-reference. The consortium used Nuix and Relativity software and the same tools and techniques as used by international law enforcement agencies for their monitoring and investigations, and by many law firms for e-discovery.

The Paradise Papers were derived from Bermuda based law firm Appelby and two other offshore legal service providers and the company registers of 19 tax havens. Prominent names implicated included Donald Trump, Justin Trudeau's moneyman, Nike, Apple, the Queen, Glencore, and many others.

---

[59] That is a massive amount of data. The easiest way to steal it would be for an insider with direct system access to place the data on a removable drive and simply walk out with it. It is possible that the exfiltration was over the internet by hackers breaking in remotely. 2.6 terabytes is the equivalent of about 20.8 terabits of data being transferred on a network. Hackers would likely use a 'low and slow' data breach technique: the hacker compromises the system and then slowly exfiltrates the data over weeks, to not create any unusual traffic spikes and so evade detection. A slow one megabit per second transfer rate would take about 241 days of continuous data transfer. Alternately (but much more vulnerable to detection), hackers might establish a high bit-rate file transfer connection, shortening the time to about 9 days at a 25 mbps transfer rate.

[60] 'Mossack Fonseca law firm to shut down after Panama Papers tax scandal', The Guardian, 15 March 2018, https://www.theguardian.com/world/2018/mar/14/mossack-fonseca-shut-down-panama-papers.

[61] International Consortium of Investigative Journalists, Paradise Papers, Glencore Fights Transparency On One Continent, Pays $22m Settlement On Another, 28 December 2018, https://www.icij.org/investigations/paradise-papers/glencore-fights-transparency-on-one-continent-pays-22m-settlement-on-another/.

Appleby launched a breach of confidence action in England against the BBC and Guardian as publishers of revelations from the Paradise Papers. 6m Appleby documents were alleged to be confidential legal documents obtained by hacking in circumstances which The Guardian and BBC ought to have inferred were a misuse of confidential information. The case never went to trial. In a settlement statement released by Appelby in May 2018, the firm's managing partner said:

> "The Guardian and the BBC have assisted Appleby by explaining which of the company's documents may have been used to underpin their journalism. This will allow Appleby to initiate meaningful discussions with its clients, colleagues and regulators".[62]

Among other interesting insights, the Paradise Papers revealed that the Australian arm of Swiss-based multinational Glencore has been involved in cross-currency swaps of up to $25bn of a type under investigation by the Australian Tax Office.[63]

According to court documents, Glencore engaged Appleby since 1995, including through King & Wood Mallesons since October 2014, to provide legal advice on Glencore's restructure codenamed Project Everest.

Through the release of the Paradise Papers in November 2017, these documents came into the possession of the ATO.

Glencore in 2018 demanded that the ATO return the Project Everest documents and give an undertaking not to use them. The tax commissioner (relying upon a Full Federal Court decision[64]) refused, prompting Glencore to seek an injunction on the basis that lawyer-client professional privilege, provided it is not waived, should be sufficient basis for a court order to restrain the use of the documents by a third party. These Australian legal proceedings, now pending in the High Court of Australia[65], principally involve the issue of whether legal professional privilege can be claimed over documents obtained by ATO other than through legal processes.

In its submissions, Glencore complained that courts have described legal professional privilege as "a fundamental common law right" paramount to a fair trial, but have "yet to recognise a complete set of remedies to protect that right". Glencore is asking the High Court to recognise that legal professional privilege is not merely a shield to prevent handing over protected communications, but a sword to prevent their use. As put in Glencore's submission:

> In Carter v Northmore Hale Davy & Leake (1995) 183 CLR 121, the Court held that legal professional privilege is so firmly entrenched in the law that it protects from disclosure documents that might otherwise establish the innocence of a person charged with a criminal offence or that may materially assist their defence. Brennan J said that "if the purpose of the privilege is to facilitate the application of the rule of law in the public interest, it is not possible

[62] https://www.theguardian.com/news/2018/may/04/appleby-settles-paradise-papers-litigation-against-guardian-and-bbc. See further Business and Human Rights Resource Centre, Appleby lawsuit against BBC & The Guardian (re Paradise Papers), at https://www.business-humanrights.org/en/appleby-lawsuit-against-bbc-the-guardian-re-paradise-papers

[63] See "The documents Glencore doesn't want the ATO to keep" Australian Financial Review (front page) 8 October 2018.

[64] The Full Federal Court in Federal Commissioner of Taxation v Donoghue (2015) 7 FCR 316 per Kenny and Perram JJ held that the common law of legal professional privilege operates only as an immunity from the exercise of powers requiring compulsory production of documents or disclosure of information and is not a rule conferring individual rights, the breach of which may be actionable.

[65] Glencore International AG & Ors v. Commissioner of Taxation of the Commonwealth of Australia & Ors Case S256/2018. Submissions are available at http://www.hcourt.gov.au/cases/case_s256-2018.

> to allow the interest of an individual accused to destroy the privilege which is conferred to advance that public interest".
>
> Deane J said that the privilege "reflects the common law's verdict that the considerations favouring the 'perfect security ' of communications and documents protected by the privilege must prevail" over the vindication and establishment of truth in the interests of a fair trial.
>
> Yet, despite recognising that legal professional privilege is a fundamental common law right which has paramountcy even over the right to a fair trial, the general law is yet to recognise a complete set of remedies to protect that right. The substantive principle upon which legal professional privilege is predicated should be recognised as entitling a privilege holder to obtain the injunctive relief that has been sought in these proceedings.
>
> That is, common law principles of legal professional privilege ought to enable the privilege to be relied upon not only as a shield to resist disclosure of privileged material, but also, as Professor Tapper has stated, "if not exactly as a sword, at least as a device to disarm one's opponent by preventing him from using evidence in his possession".

The Commissioner's submissions state the current position of Australian law as follows:

> The character of LPP [legal professional privilege] as an immunity from compulsory process - as opposed to a cause of action entitling the privilege holder to restrain the use, and to require the delivery up, of information and documents - has been recognised by Australian intermediate appellate courts including the Full Court of the Supreme Court of South Australia, the Victorian Court of Appeal, and the New South Wales Court of Appeal. Most recently, it was recognized by a Full Court of the Federal Court in Donoghue v Federal Commissioner of Taxation (Donoghue). Given all the authorities cited above, the character of LPP as an immunity from compulsory production of documents or information, and not a cause of action sounding in damages or injunctive relief, reflects the settled law of Australia.
>
> The same position has been reached in other common law jurisdictions. Thus, in Three Rivers DC v Bank of England (No 6), Lord Scott observed that LPP "gives the person entitled to it the right to decline to disclose or allow to be disclosed the confidential communication or document in question". Similarly, the Privy Council in B v Auckland District Law Society, on appeal from the New Zealand Court of Appeal, accepted that "privilege is a right to resist compulsory disclosure of information" (at [67]) and that a claim for the recovery of privileged documents voluntarily supplied to a third party must arise from other common law or equitable foundations. Likewise, in Canada and in Singapore, LPP is characterized as a basis to resist compulsory disclosure, and not as a cause of action affording injunctive or other relief.

How to avoid (or at least mitigate the risk of) being a statistic

Data breaches are now an everyday event. Lawyers have particular obligations to protect themselves and their clients from exposure to these threats. Large law firms, small law firms, and in-house counsel face similar challenges.

Thank you very much for reading this far. You may want to do, or delegate, just a bit more reading. I recommend:

U.K. National Cyber Security Centre and Law Society of England and Wales, The cyber threat to the UK legal sector, 2018, available at https://www.ncsc.gov.uk/content/files/protected_files/article_files/the_cyber_threat_to_uk_legal_sector_NCSC_2.pdf

Office of the Australian Information Commissioner, Guide to securing personal information, June 2018, available at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

American Bar Association, Lawyers Obligations After an Electronic Data Breach or Cyberattack, Formal Opinion 483, 17 October 2018, available at https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf

American Bar Association, Securing Communication of Protected Client Information, Formal Opinion 477R, revised 22 May 2017, available at https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf

Practical steps? Implement the following:

1. Understand the nature of the threat.
2. Understand how client confidential information is transmitted and where it is stored.
3. Understand and use reasonable electronic security measures.
4. Determine how electronic communications about client matters should be protected.
5. Label client confidential information.
6. Mind the gap between technical controls and good governance and operational controls and safeguards. See cybersecurity and management of confidential electronic information as principally an organisational cultural and operational problem, not a technical problem. This may mean entering into a challenging negotiation with your information systems personnel as to areas of focus and propriety for expenditure. Who better than a lawyer to lead that negotiation?
7. Train lawyers and nonlawyer assistants in good data handling practices and responsible uses of technology and information security. Insist upon this training being entertaining and rich in real world examples of what happens (to others) when things going wrong. Lawyers are practical people who like to gossip about their competitors and learn from example rather than principle. They also have a high resistance to believing sermons and horror stories (having heard them from their own mouths so often).
8. Conduct device hygiene on BYODs (bring-your-own devices) and home devices used to access your network. Make clearance of devices a condition of access to your system. Promote these requirements to your staff yourself, as not being a 'heavy handed intervention' from your IT department, but instead a staff benefit, to the benefit of their families as well as themselves.

9. Require strong passwords, and ideally pass phrases instead of passwords. Use two factor identification.
10. Aggressively security patch your computer systems (laptops, servers, etc.). If you are up-to-date on security patches, it is much harder for hackers to take advantage of your computer systems.
11. Be a regular user, not an administrator. "Administrator" and "user" are designations that define how much authority you have to make changes on a computer system. Logging in as an "admin" exposes the access device to hacking: it is more secure to log in as a "user".
12. Invest in email message and attachment scanning tools.
13. Invest in web-filtering tools.
14. Invest in system monitoring tools.
15. Conduct due diligence on vendors providing communication technology and services. Make sure contractors use temporary access codes and the theses are promptly revoked.
16. Be alert, not alarmed. Many legal technology service vendors ensure their products implement good and up-to-date industry practice in information security and in threat assessment and mitigation. Ensure your technology staff also understand good and up-to-date industry practice.

Peter Leonard
23 March 2019

Extracts from Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015

3 **Paramount duty to the court and the administration of justice**

3.1 A solicitor's duty to the court and the administration of justice is paramount and prevails to the extent of inconsistency with any other duty.

5 **Dishonest and disreputable conduct**

5.1 A solicitor must not engage in conduct, in the course of practice or otherwise, which demonstrates that the solicitor is not a fit and proper person to practise law, or which is likely to a material degree to:

5.1.1 be prejudicial to, or diminish the public confidence in, the administration of justice, or

5.1.2 bring the profession into disrepute.

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 information which is confidential to a client 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.

21 **Responsible use of court process and privilege**

21.1 A solicitor must take care to ensure that the solicitor's advice to invoke the coercive powers of a court:

21.1.1 is reasonably justified by the material then available to the solicitor,

21.1.2 is appropriate for the robust advancement of the client's case on its merits,

21.1.3 is not made principally in order to harass or embarrass a person, and

21.1.4 is not made principally in order to gain some collateral advantage for the client or the solicitor or the instructing solicitor out of court.

21.2 A solicitor must take care to ensure that decisions by the solicitor to make allegations or suggestions under privilege against any person:

21.2.1 are reasonably justified by the material then available to the solicitor,

21.2.2 are appropriate for the robust advancement of the client's case on its merits, and

21.2.3 are not made principally in order to harass or embarrass a person.

21.3 A solicitor must not allege any matter of fact in:

21.3.1 any court document settled by the solicitor,

21.3.2 any submission during any hearing,

21.3.3 the course of an opening address, or

21.3.4 the course of a closing address or submission on the evidence,

unless the solicitor believes on reasonable grounds that the factual material already available provides a proper basis to do so.

21.4 A solicitor must not allege any matter of fact amounting to criminality, fraud or other serious misconduct against any person unless the solicitor believes on reasonable grounds that:

21.4.1 available material by which the allegation could be supported provides a proper basis for it, and

21.4.2 the client wishes the allegation to be made, after having been advised of the seriousness of the allegation and of the possible consequences for the client and the case if it is not made out.

21.5 A solicitor must not make a suggestion in cross-examination on credit unless the solicitor believes on reasonable grounds that acceptance of the suggestion would diminish the credibility of the evidence of the witness.

21.6 A solicitor may regard the opinion of an instructing solicitor that material which is available to the instructing solicitor is credible, being material which appears to the solicitor from its nature to support an allegation to which Rules 21.1, 21.2, 21.3 and 21.4 apply, as a reasonable ground for holding the belief required by those Rules (except in the case of a closing address or submission on the evidence).

21.7 A solicitor who has instructions which justify submissions for the client in mitigation of the client's criminality which involve allegations of serious misconduct against any other person not able to answer the allegations in the case must seek to avoid disclosing the other person's identity directly or indirectly unless the solicitor believes on reasonable grounds that such disclosure is necessary for the proper conduct of the client's case.

21.8 Without limiting the generality of Rule 21.2, in proceedings in which an allegation of sexual assault, indecent assault or the commission of an act of indecency is made and in which the alleged victim gives evidence:

21.8.1 a solicitor must not ask that witness a question or pursue a line of questioning of that witness which is intended:

(i) to mislead or confuse the witness, or

(ii) to be unduly annoying, harassing, intimidating, offensive, oppressive, humiliating or repetitive, and

21.8.2 a solicitor must take into account any particular vulnerability of the witness in the manner and tone of the questions that the solicitor asks.

30 **Another solicitor's or other person's error**

30.1 A solicitor must not take unfair advantage of the obvious error of another solicitor or other person, if to do so would obtain for a client a benefit which has no supportable foundation in law or fact.

31 **Inadvertent disclosure**

31.1 Unless otherwise permitted or compelled by law, a solicitor to whom material known or reasonably suspected to be confidential is disclosed by another solicitor, or by some other person and who is aware that the disclosure was inadvertent must not use the material and must:

31.1.1 return, destroy or delete the material (as appropriate) immediately upon becoming aware that disclosure was inadvertent, and

31.1.2 notify the other solicitor or the other person of the disclosure and the steps taken to prevent inappropriate misuse of the material.

31.2 A solicitor who reads part or all of the confidential material before becoming aware of its confidential status must:

31.2.1 notify the opposing solicitor or the other person immediately, and

31.2.2 not read any more of the material.

31.3 If a solicitor is instructed by a client to read confidential material received in error, the solicitor must refuse to do so.

34 **Dealing with other persons**

34.1 A solicitor must not in any action or communication associated with representing a client:

34.1.1 make any statement which grossly exceeds the legitimate assertion of the rights or entitlements of the solicitor's client, and which misleads or intimidates the other person,

34.1.2 threaten the institution of criminal or disciplinary proceedings against the other person if a civil liability to the solicitor's client is not satisfied, or

34.1.3 use tactics that go beyond legitimate advocacy and which are primarily designed to embarrass or frustrate another person.

34.2 In the conduct or promotion of a solicitor's practice, the solicitor must not seek instructions for the provision of legal services in a manner likely to oppress or harass a person who, by reason of some recent trauma or injury, or other circumstances, is, or might reasonably be expected to be, at a significant disadvantage in dealing with the solicitor at the time when the instructions are sought.