FOLEY'S | LIST

I SPY WITH MY LITTLE iPhone: PHONE RECORDINGS, EMAILS AND SOCIAL MEDIA

Author: Belle Lane and Alison Burt

Date: 7 April, 2016

"I spy with my little i(Phone): phone recordings, emails and social media"

Belle Lane and Alison Burt
Foley's list
Victorian Bar
April 2016

A. The conundrum

More and more people are recording their lives on social media and they or their friends are putting that information in the public domain. Our private and unguarded activities are far more public than they have ever been. Such information is easy pickings for potential employers, stalkers, former partners and family lawyers.

At the same time, most of us have smart phones which we carry everywhere. They are in effect personal computers that carry details of our daily lives, both public and private. They are also very handy recording devices: both audio and video.

So how can we as family lawyers advise our clients about their access to and use of this information? How do we walk an ethical line? If a client presents us with information that s/he has gathered, how do we determine if and how we can use it?

B. Ethical obligations

Where do we start? As always with our ethical obligations.

In New South Wales and Victoria, our professional obligations are governed by the Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015 under the Legal Profession Uniform Law which commenced operation on 1 July 2015. In Western Australia, the Legal Profession Conduct Rules. They all have similar obligations and confirm our primary duty, as they reflect the common law.

1. Primary duty to the Court

As barristers and solicitors, our paramount duty is to the Court and the administration of justice:

Rule 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.*[1]

In Western Australia the duty to the Court over and above the duty to a client is even more express:

Rule 5 *A practitioner's duty to the court and the administration of justice is paramount and prevails to the extent of inconsistency with any other duty, including but not limited to a duty owed to a client of the practitioner.*

The difficulty for practitioners is that so much of our legal practice is built on building good relationships with clients. In family law, we are dealing with the most intimate parts of our client's lives, and often building warm, friendly relationships with them. Sometimes our desire to see justice done, to not disappoint a client or disrupt a relationship has us questioning these boundaries. Sometimes the boundaries themselves are not clear. In such cases, go back to first principles: read your professional ethical obligations. Discuss the situation with a colleague or mentor.

One only needs to read some of the decisions of the legal practice boards to see the consequences of breaches. See Lambert v Jackson [2011] FamCA 257 & [2011] FamCA 275 (costs judgment), Kyle v Legal Practitioners' Complaints Committee [1999] WASCA 115.

2. Recordings: telephone and video

It is important to distinguish between telephone / video recordings that are covered by Commonwealth Legislation, the Telecommunications (Interception & Access) Act 1979 and those covered by State Legislation. In Victoria this is covered by the Surveillance Devices Act 1999 (Vic) ("SDA (Vic)") and in Western Australia, the Surveillance Devices Act (WA)("SDA (WA)").

The Commonwealth legislation deals with "interception of telecommunications". That is the recording must occur during its passage over the telecommunication system.

Section 6(1) Telecommunications (Interception & Access) Act 1979 (Cth) ("TIA Act"):

> *"For the purpose of this Act, but subject to this section, interception of a communication passing over a telecommunications system consists of listening to, or recording, by any means, such a communication in its passage over the telecommunication system without the knowledge of the person making the communication."*

[1] Rule 3.1 Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015 (Vic & NSW), Legal Profession Conduct Rules 2010 (WA) and WA Barristers' Rules 2012.

3. Interaction between Commonwealth and State laws

Cth legislation covers the cases where there are listening devices installed in telephones or phone / wire taps. It does not cover the recording or listening when the message or communication has left the telecommunication system, such as a message on an answering machine or where a recording device is held externally to the phone. The listening into a phone conversation on an additional handset has been held to fall under the Commonwealth legislation.[2]

When considering the interaction between the Cth and State legislation, His Honour Judicial Registrar Haligan in Byrne & Byrne (2003) FamCA 887 held:

> *"29. On the authority of Miller [1978] HCA 44 and Edelsten v Investigating Committee of NSW (1986) 80 ALR 85, the Interception Act covers the field in relation to the interception of a communication passing over a telecommunications system, and a State law cannot operate to render lawful that which is unlawful under the Commonwealth Act, or to render unlawful that which is lawful under the Commonwealth Act."*

The question whether a recording is lawful or unlawful therefore falls to be determined first by reference to the Commonwealth Act. Only if it was made in circumstances not covered by the Commonwealth Act can the State law then be considered. This is important to remember when considering the question of admissibility of recordings in Western Australia.

4. Interception of telecommunications

The first question to ask is how was the call recorded? Under section 7(1) of the TIA Act, a person is prohibited from intercepting, authorizing, suffering, permitting or enabling another person to intercept a communication passing over a telephone system.[3] The interception provisions relate to communications that are "passing over a telecommunications system", that is, "live" or "real-time" communications such as telephone call conversations and other communications in transit over the Internet including while passing through ISPs' equipment such as routers, etc.

In this context communication is defined as including a conversation and message, or any part thereof, whether in the form of speech, music, other sounds, data, text, visual images (animated or not), signals or any other form or combination.[4] So the TIA covers the interception of text messages sent by SMS, recording phone calls with software / apps and recording / listening into Skype conversations: see Kawada.

---

[2] See Miller & Miller [1978] HCA 44

[3] Section 7 Telecommunications (Interception & Access) Act 1979.

[4] Section 11(a) Telecommunications (Interception & Access) Act 1979

A telecommunication system is defined as a telecommunications network that is within or partly within (but only to the extent that it is within) Australia and includes equipment, line or other facility connected to the network and is within Australia.[5] So we require a geographical connection with Australia, but the entire call does not have to take place within Australia.

The important elements of an interception under section 6(1) TIA Act above are the interception of the communication when it is passing over a telecommunications system and the lack of knowledge of the party being recorded.

Pursuant to section 105 of the TIA Act breaching the above provisions is an indictable offence and is punishable by imprisonment, generally 2 years maximum.[6] There are also civil remedies available to a person who is aggrieved as a consequence of a breach of section 7 or 63.[7]

When one thinks of a listening device, we think of a physical device inserted into a phone. However, there is a wide variety of software that can record conversations on mobile phones and third party applications for recording Skype calls. As our clients become increasingly tech savy, we should expect to see more of such recordings or information prepared from them.

Some examples are: the case of Kawada & Kawada and Ors [2011] FamCA 659 dealt which with Skype recordings. The case of Russell and Russell [2012] FamCA 99 which dealt with the surreptitious recording of mobile phone conversations through software installation. Chapman and Timms [2014] FamCA 316 dealt with recorded telephone conversations, although the mechanics of the recording were not explained to the Court. R v Catena [2012] WASC 144 which dealt with the admissibility of phone recordings on a work phone system.

Once your client informs you that he or she has made a recording, a red flag should be going up. You will need to take very clear instructions about how the recording came into existence, determine what the criminal and civil consequences of breach may be and then consider whether or not you can or should use the recording?

5. What can you do with a recording?

Assuming that the recording of these calls (video or audio) is caught by the TIA Act, it is illegal. In such circumstances what use can be made of the recording inside and outside Court?

[5] Section 11(b) Telecommunications (Interception & Access) Act 1979
[6] Sections 105 Telecommunications (Interception & Access) Act 1979
[7] Section 76A Telecommunications (Interception & Access) Act 1979

The TIA Act itself contains provisions that render the use of intercepted communications inadmissible as evidence, except in limited circumstances.[8]

> ***63 No dealing in intercepted information or interception warrant information***
>
> *(1) Subject to this Part, a person shall not, after the commencement of this Part:*
> *(a) communicate to another person, make use of, or make a record of; or*
> *(b) give in evidence in a proceeding;*
>
> *lawfully intercepted information or information obtained by intercepting a communication in contravention of subsection 7(1).*

Pursuant to the Act, our clients are potentially committing further breaches of the TIA Act when they make a transcript (record) of the conversation and when they communicate the recording to other people.

If our clients intend to give evidence about acts that would constitute a breach of the TIA Act, you will need to consider obtaining a certificate section 128 Evidence Act or section 11 Evidence Act (1906)(WA)(privilege against self-incrimination). You must apply for a certificate prior to your client giving evidence, whether orally or by way of affidavit. Certificates are not granted retrospectively, so if your client swears/affirms an affidavit giving evidence of the breach and it is filed with the Court, it is before the Court without any protection.

The provisions relating to the use of the offending recording seem clear. Under the TIA Act as set out above, under section 63 TIA Act, an illegally obtained recording cannot be used. Despite this mandatory provision, there has been some debate in the Family Law Courts about the interaction of this section and section 138 Evidence Act which gives the Court discretion as to whether or not to exclude improperly or illegally obtained evidence. Section 138 Evidence Act is set out below.

s.138 Discretion to exclude improperly or illegally obtained evidence

> *s.138(1) Evidence that was obtained:*
> *(a) improperly or in contravention of an Australian law; or*
> *(b) in consequence of an impropriety or of a contravention of an Australian law;*
> *is not to be admitted unless the desirability of admitting the evidence outweighs the undesirability of admitting evidence that has been obtained in the way in which the evidence was obtained.*
> *(2) Without limiting subsection (1), evidence of an admission that was made during or in consequence of questioning, and evidence obtained in consequence*

[8] Section 77 Telecommunications (Interception & Access) Act 1979

of the admission, is taken to have been obtained improperly if the person conducting the questioning:

(a) did, or omitted to do, an act in the course of the questioning even though he or she knew or ought reasonably to have known that the act or omission was likely to impair substantially the ability of the person being questioned to respond rationally to the questioning; or

(b) made a false statement in the course of the questioning even though he or she knew or ought reasonably to have known that the statement was false and that making the false statement was likely to cause the person who was being questioned to make an admission.

(3) Without limiting the matters that the court may take into account under subsection (1), it is to take into account:

(a) the probative value of the evidence; and

(b) the importance of the evidence in the proceeding; and

(c) the nature of the relevant offence, cause of action or defence and the nature of the subject-matter of the proceeding; and

(d) the gravity of the impropriety or contravention; and

(e) whether the impropriety or contravention was deliberate or reckless; and

(f) whether the impropriety or contravention was contrary to or inconsistent with a right of a person recognised by the International Covenant on Civil and Political Rights; and

(g) whether any other proceeding (whether or not in a court) has been or is likely to be taken in relation to the impropriety or contravention; and

(h) the difficulty (if any) of obtaining the evidence without impropriety or contravention of an Australian law.

Section 138 Evidence Act 2008 (Cth) is not repeated in the Evidence Act (1906) WA, however in Western Australia the common law applies. The High Court in Bunning v Cross [1978] 141 CLR 54 sets out the common law position, which was codified in the Commonwealth Evidence Act.

Their Honours Mason CJ, Deane and Dawson JJ in Ridgeway v R [1995] 184 CLR 19 summarised the law as follows:

> 15. At least since **Bunning v. Cross**, it has been "the settled law in this country" that a trial judge has a discretion to exclude prosecution evidence on public policy grounds in circumstances where it has been obtained by unlawful conduct on the part of the police. That discretion is distinct from the discretion to exclude evidence of a confessional statement on the grounds that its reception would be unfair to the accused. The discretion extends to the exclusion of both "real" (or non-confessional) evidence and confessional evidence. As Barwick CJ pointed out in Reg. v. Ireland, in a judgment with which the other four members of the Court agreed, the rationale of the discretion is that convictions obtained by means of unlawful conduct "may be obtained at too high a price". In its

> exercise, a trial judge must engage in a balancing process to resolve "the apparent conflict between the desirable goal of bringing to conviction the wrongdoer and the undesirable effect of curial approval, or even encouragement, being given to the unlawful conduct of those whose task it is to enforce the law". The basis in principle of the discretion lies in the inherent or implied powers of our courts to protect the integrity of their processes. In cases where it is exercised to exclude evidence on public policy grounds, it is because, in all the circumstances of the particular case, applicable considerations of "high public policy" relating to the administration of criminal justice outweigh the legitimate public interest in the conviction of the guilty.

Returning to the case of the Commonwealth Evidence Act, how does the Court wrestle with the seemingly contradictory provisions of section 138 Evidence Act and s.63 TIA Act?

His Honour Justice O'Reilly dealt with this question in Kawada & Kawada and Ors [2011] FamCA 659. In that case the Wife recorded Skype conversations between the husband and the parties' child. At Court, her counsel admitted that the recordings breached the TIA Act. The issue before the Court was the admissibility of the transcript of the recordings and the interplay between the section 63 TIA Act and section 138 Evidence Act. There is an inconsistency between the provisions of the Acts.

His Honour Justice O'Reilly held that section 63 TIA Act overrode the provisions of section 138 Evidence Act due to the operation of section 8 Evidence Act.

> ***s.8 - Operation of other Acts etc.***
>
> *(1) This Act does not affect the operation of the provisions of any other Act, other than sections 68, 79, 80 and 80A of the Judiciary Act 1903 .*
> *(2) This Act does not affect the operation of regulations that:*
> *(a) are made under an Act other than this Act; and*
> *(b) are in force on the commencement of this section.*
> *However, this subsection ceases to apply to a regulation once it is amended after that commencement.*
> *(3) This Act has effect subject to the Corporations Act 2001 and the Australian Securities and Investments Commission Act 2001 .*

However His Honour Justice Young in Russell and Russell [2012] FamCA 99 found the reverse, allowing a transcript of a recording that breached the TIA Act into evidence.

In a subsequent decision of Badger & Badger & Ors [2013] FMCAfam 124, Myers FM (as he then was) held that a police officer had illegally taped a telephone conversation without the other party's knowledge and therefore offended the provisions of the TIA Act. His Honour followed the line of reasoning in Russell, by

not applying a mandatory exclusion and went on to say that the provisions of s.138 Evidence Act applied and that the evidence should be excluded as a police officer should be held to a higher standard of conduct.

With due respect to His Honour Justice Young and His Honour Judge Myers, it is hard to understand how they are correct. However, it seems that you may be able to get in such recordings in practice. The matter appears ready for the Full Court.

6. State legislation

Surveillance Devices legislation operates on a State by State basis.[9] The legislation has slight variations and you will need to read the provisions of any State in which the recording is said to have occurred. The relevant purposes of the Victorian legislation are[10]:

(a) first, to regulate the installation, use and maintenance of surveillance devices;
(b) secondly, to restrict the communication and publication of records of private conversations and activities obtained through the use of surveillance devices; and
(c) thirdly, to create offences for the improper installation or use of surveillance devices.

7. What is a surveillance device?

Section 3 of the Surveillance Devices Acts of Western Australia (SDA(WA)) and Victoria (SDA(Vic) both define a "surveillance device" a listening device, an optical surveillance device or a tracking device. However the SDA(Vic) also includes a data surveillance device.

Data surveillance device means any device capable of being used to record or monitor the input of information into or the output of information from a computer, but does not include an optical surveillance device.

Listening device means any device capable of being used to overhear, record, monitor or listen to a private conversation or words spoken to or by any person in private conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear. This definition clearly includes mobile phones with recording capacity.

An optical surveillance device is any device capable of being used to record visually or observe a private activity, but does not include glasses, contact lenses

[9] Surveillance Devices Act 1998 (WA) and Surveillance Devices Act 1999 (Vic)
[10] While the purpose of SDA(WA) is more limited, in reality it has the same effect.

or anything similar which is used by a person with impaired sight to overcome vision impairment.[11] Again, this includes mobile phones with video function.

A tracking device is an electronic device the primary purpose of which is to determine the geographical location of a person or an object.[12]

Presumably this would not include a mobile phone with an app such as "Glimpse" or "Find my phone", as geographical location is not the primary purpose of the phone.

8. What is prohibited?

Section 6 SDA(Vic) prohibits a person knowingly installing, using or maintaining a listening device to overhear, record, monitor or listen to a private conversation to which the person is not a party, without the express or implied consent of each party to the conversation.[13]

The SDA(Vic) and SDA(WA) prohibit the use of an optical surveillance device in like terms[14]. A person must not knowingly install, use or maintain an optical surveillance device to record visually or observe a private activity to which the person is not a party, with the express or implied consent of each party to the activity.

The prohibition relates to the audio recording, visual recording or audiovisual recording and any document arising therefrom.

9. Who is a party?

A party to a private activity is defined as a person who takes part in the activity. A party to a private conversation, means a person by or to whom words are spoken in the course of the conversation.

This may mean that many of the recordings that we would see would not offend the legislation, as often our clients are parties to the conversations.

However, what about the case of a third party witness? It may be that the person who made the recording was not a party, but then it may be arguable that the conversation was not private.

10. What is private conversation or activity?

A *private activity*[15] is defined as an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include—

---

[11] Section 3 SDA(Vic), section 3 SDA(WA)
[12] Again slight variation of wording in definition sections of the Acts
[13] Section 6 of the SDA(WA) omits the word "overhear"
[14] Section 7 of the SDA(Vic) and s.6(1) SDA(WA)
[15] s.3 SDA(Vic) and s.3 SDA(WA)

(a) (in Victoria) an activity carried on outside a building[16]; or
(b) an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else;

Both the SDA(Vic) and the SDA(WA) define a "private conversation" as meaning a conversation carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be heard only by themselves, but does not include a conversation made in any circumstances in which the parties to it ought reasonably to expect that it may be overheard by someone else[17]. While the Victorian legislation specifically excludes conversations outside a building, a conversation in a public place would normally be at risk of being heard.

It will be important to take instructions about the location of the conversation, who else was present or within the hearing of the conversation, the loudness of the conversation if you wish prove that it was not a private conversation.

11. What can you do with a recording that offends the State Act?

Assuming that the conversation or activity falls under the legislation above, there are restrictions on the knowing communication or publishing of a record or report of the private conversation or activity, if that recording or report has been made as a direct or indirect result from the use of the prohibited device. There are significant criminal penalties arising from a breach.[18]

Section 11 of the SDA (Vic):

s.11. Prohibition on communication or publication of private conversations or activities

(1) Subject to sub-section (2), a person must not knowingly communicate or publish a record or report of a private conversation or private activity that has been made as a direct or indirect result of the use of a listening device, an optical surveillance device or a tracking device.

Penalty: In the case of a natural person, level 7 imprisonment (2 years maximum) or a level 7 fine (240 penalty units maximum) or both;
In the case of a body corporate, 1000 penalty units for a first offence and 2000 penalty units for a subsequent offence.

(2) Sub-section (1) does not apply—

[16] The SDA(Vic) only
[17] s.3 SDA(Vic) and s.3 SDA(WA)
[18] Section 11 SDA 1999. Level 7 imprisonment (2 years maximum) or level 7 fine (240 penalty units) or both.

(a) to a communication or publication made with the express or implied consent of each party to the private conversation or private activity; or

(b) to a communication or publication that is no more than is reasonably necessary—

(i) in the public interest; or

(ii) for the protection of the lawful interests of the person making it; or

(c) to a communication or publication in the course of legal proceedings or disciplinary proceedings; or

(d) to a communication or publication made by a law enforcement officer—

(i) to a person authorised by the chief law enforcement officer in relation to that officer and for the purpose of investigating or prosecuting an offence; or

(ii) to the occupier of premises of a record or report of a private activity that has been made as a direct or indirect result of the use on those premises of an optical surveillance device in the circumstances referred to in section 7(2)(c); or

(iii) to the sheriff or to a person employed in the Department of Justice in the administration of Schedule 7 to the Magistrates' Court Act 1989(enforcement of infringement penalties); or

(iv) otherwise in the performance of his or her duty; or

(e) to a communication to a member of the police force by a person authorised to do so by an authorised police officer; or

(f) to a communication or publication authorised by a law of the Commonwealth relating to the security of the Commonwealth.

In Western Australia:

s.9 Prohibition of publication or communication of private conversations or activities

(1) Subject to subsection (2), a person shall not knowingly publish or communicate a private conversation, or a report or record of a private conversation, or a record of a private activity that has come to the person's knowledge as a direct or indirect result of the use of a listening device or an optical surveillance device.
Penalty:
(a) for an individual: $5,000 or imprisonment for 12 months, or both;
(b) for a body corporate: $50,000.

(2) Subsection (1) does not apply —
(a) where the publication or communication is made —
(i) to a party to the private conversation or the private activity;
(ii) with the express or implied consent of each principal party to the private conversation or private activity;
(iii) to any person or persons authorised for the purpose by the Commissioner of Police, the Corruption and Crime Commission or the Chair of the Board of the Australian Crime Commission;
(iiia) to a designated Commission or to any person or persons

authorised for the purpose by a designated Commission;

(iv) by a law enforcement officer to the Director of Public Prosecutions of the State or of the Commonwealth or an authorised representative of the Director of Public Prosecutions of the State or of the Commonwealth;

(v) in the course of the duty of the person making the publication or communication;

(vi) for the protection of the lawful interests of the person making the publication or communication;

(vii) in the case of the use of a listening device or an optical surveillance device in the circumstances referred to in section 5(3)(d) or 6(3)(b)(iii), as the case requires, in the course of reasonable action taken to protect the lawful interests of the principal party to the conversation or activity who consented to the use of the device;

(viii) in accordance with Part 5; or

(ix) in the course of any legal proceedings;

(b) where the publication or communication is made to a member of the police force of the State or of another State or a Territory in connection with —

(i) an indictable drug offence or an external indictable drug offence; or

(ii) any other indictable matter of such seriousness as to warrant the publication or communication; or

(c) where the person making the publication or communication believes on reasonable grounds that it was necessary to make that publication or communication in connection with an imminent threat of serious violence to persons or of substantial damage to property.

In *Huffman v Gorman* (No2) [2014] FamCA 1077, the father included in his affidavit evidence lengthy transcripts of conversations with the mother recorded without her knowledge or consent. Unusually in family proceedings, a voir dire was held. Justice Hannam found that the recordings involved a breach of the relevant NSW legislation. [19] His Honour declined to exclude it under either s 135 or 138 of the Evidence Act, considering that it was of considerable probative value, that the father's conduct in making the recordings was at the least serious end of the spectrum and that there was no basis to find that its admission would be unfairly prejudicial to the mother.

Justice Austin dealt with a recording made in similar circumstances in *Howard & Lipschitz* [2014] FamCA 272. However in the context of that case, a recording of the father swearing at his children was of limited probative value, largely because of similar evidence from other sources, and on that basis His Honour excluded the recording under s 138 of the *Evidence Act.*

[19] Listening Devices Act 1984 (NSW) s 5(3)(b)
Surveillance Devices Act 2007 (NSW) ss 7(3)(b), 11(2)

12. Exemptions to prohibition on communication, publication and use

From our clients' point of view, the important exemptions in Victoria will be:

(a) express or implied consent,
(b) the publication or communication being in the public interest;
(c) for the protection of the lawful interests of the person making it; or
(d) in the course of legal or disciplinary proceedings

In Western Australia the important exemptions will be (a), (c) and (d) noting that there is no public interest exemption.

How to proceed?

If your client arrives with a recording, you should obtain detailed instructions from the client about how it was obtained:

(a) if it was a recording from a phone, how was it recorded, was the recording intentional, accidental or inadvertent? If it was the latter it should absolve them of the requisite intention for the offence.
(b) What knowledge did the person who was being recorded, having of the recording at the time? Was there actual or implied consent to the recording?
(c) Did the recording occur while the information was passing through the telecommunications system or was it recorded once it left the system?
(d) If it was a recording or video made external to a telecommunications system, was our client a party to the conversation or activity?
(e) Was each participant who was recorded aware of the recording?
(f) Was the conversation or activity intended to be private? Where did it take place? Who else was in the vicinity? Were the parties behaving in a manner that indicated that they believed the conversation or activity to be private?
(g) Is the publication or communication of the recording in the public interest;
(h) Is the publication or communication of the recording for the protection of the lawful interests of the person making it; or
(i) Is it to be published or communicated in the course of legal or disciplinary proceedings?

While the recordings cannot be put into evidence, they can potentially be used in the course of the proceedings but care must be taken to ensure that you are not exposing your client to criminal liability. Any recording would need to be highly probative.

13. Recordings of Family Report writers and counselors

Our clients are well aware of the influence of Family Reports over the outcome of their cases – and this can lead to the temptation to monitor or record the interviews on which such reports are partly based.

In *Hazan v Elias* [2011] FamCA 376, a father had made a secret recording of his interview with the Family Consultant and then sought to rely upon it. The recording was not caught by TIA; it was made in Queensland but was not illegal under the relevant state legislation.[20]

The father argued that section 11C Family Law Act 1975 provided an absolute right for the admission of both the recording and the transcript:

> **FAMILY LAW ACT 1975 - SECT 11C**
>
> **Admissibility of communications with family consultants and referrals from family consultants**
>
> *(1) Evidence of anything said, or any admission made, by or in the company of:*
>
> *(a) a family consultant performing the functions of a family consultant; or*
>
> *(b) a person (the professional) to whom a family consultant refers a person for medical or other professional consultation, while the professional is carrying out professional services for the person;*
>
> *is admissible in proceedings under this Act.*

Whilst s 11C contains no express limitations, His Honour Justice Watts noted a number of contrary provisions, in particular s 69ZU, which allows the opinions of Family Consultants to be taken into account only where they are the subject of sworn evidence or with the consent of both parties.

His Honour found that in making the recording, the father had contravened the Rule 1.19 of the Family Law Rules:

> ***Rule 1.19: permission to record court event***
>
> *A person must not photograph, or record by electronic or mechanical means, any court event[21].*

The father attempted unsuccessfully to argue that an interview conducted for the preparation of a s 62G report was not a court event; His Honour found there to be no substantive difference between an interview conducted pursuant to s11F and one, as here, conducted for s 62G purposes. On that basis His Honour

---

[20] The effect of the *Invasion of Privacy Act* 1971 (Qld) ("IPA") is that in Queensland one party to a conversation may secretly record that person's private conversation with another person and may communicate that recording to a court (see sections 4, 43 and 45 of IPA)

[21] The Dictionary in the *Family Law Rules* indicates that a court event includes:

(a) a hearing or part of a hearing
(b) a trial or part of a trial
(c) a conference; and
(d) an attendance by the parties with family consultant as part of the Child Responsive Program

exercised the discretion provided by section 138 of the Evidence Act to exclude the recording which His Honour found to have been obtained both illegally and improperly.

14. Emails

Inadvertent disclosure

The rush to get work out and predictive text can be a dangerous combination, especially where emails are concerned. There is probably not a practitioner amongst us who has not sent out an email to the wrong person. So what do you do when you receive one from your opponent? What duty do we owe to our client and to our colleague? Fortunately our ethics have clarified our obligations.

> 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.

In Western Australia it is governed by rule 24.

> ***24. Inadvertent disclosure***
>
> *A practitioner to whom material is disclosed by another practitioner in circumstances where the first mentioned practitioner knows or reasonably suspects that the material is privileged and that the disclosure was inadvertent —*
>
> *(a) must not disclose the material or its substance to the practitioner's client or use the material in any way; and*
>
> *(b) must immediately, in writing, notify the practitioner's client and the other practitioner —*
>
> *(i) that the material has been disclosed; and*
>
> *(ii) that the practitioner will return, destroy or delete the material (as appropriate) at a time set out in the notice (being not less*

than 2 clear business days and not more than 4 clear business days from the date of the notice);

and

(c) must return, destroy or delete the material as set out in the notice; and

(d) must notify the practitioner's client and the other practitioner in writing as soon as the practitioner has returned, destroyed or deleted the material.

Less innocent ways

Our clients will often want to show us emails sent by or to the other party that may have come to their attention in innocent or less innocent ways.

The questions that arise are similar to those involving recordings:

- Was the material obtained in breach of any Commonwealth legislation?
- Was the material obtained in breach of any state legislation?
- Should it be excluded under s 138 of the *Evidence Act* on the basis that it was obtained either unlawfully or improperly?

Commonwealth legislation

Parties who seek to rely on others' emails may fall foul of section 478.1 of the *Criminal Code* (Cth):

478.1 Unauthorised access to, or modification of, restricted data

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised access to, or modification of, restricted data; and

(b) the person intends to cause the access or modification; and

(c) the person knows that the access or modification is unauthorised.

Penalty: 2 years imprisonment.

(3) In this section:

***restricted data** means data:*

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer.

What does 'unauthorised access' mean here?

Section 476.2 offers a wonderfully circular definition:

476.2 Meaning of unauthorised access, modification or impairment

(1) In this Part:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer; or

(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means;

by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

State legislation

There are also various offences under State criminal legislation.

In Victoria, the relevant legislation is s s.247G of the *Crimes Act 1958* (Vic). It replicates the provisions of s 478.1, with the distinction that the jurisdiction of s.478.1 is triggered by s.478.1(1)(d)(iii) where one uses a telecommunications service to access the restricted data.

In Western Australia it is the Criminal Code Act 1913, section 440A (reprinted below)

How have the Family Law courts dealt with email access?

In Anders & Anders[2008] FMCAfam 1125, the father had obtained copies of emails sent by the mother using her password; he accepted in evidence that she had not given him permission to do so post-separation. Relevantly, he had sought and obtained a certificate under s 128 Evidence Act before giving evidence. Federal Magistrate Kemp found that there was insufficient evidence as to whether there had been a breach of 308H of the Crimes Act 1900 (NSW) and s.478.1 of the Criminal Code Act 1995 (Cth). In response to the mother's

submission that the emails should in any event be excluded on the basis that they had been improperly obtained, he found that the probative value of the material (relating to allegations about the mother's involvement in witchcraft!) was of sufficient probative value to outweigh the undesirability of admitting material obtained in this manner.

By way of contrast, the evidence accepted by the court in Yardborough & Chesterman [2014] FCCA 44 was that the wife had given the husband express permission to use her email password and that the parties understood that each was free to access the other's emails. On that basis, Judge Turner rejected the argument that the husband had acted improperly and the wife's attempt to rely on s 138 Evidence Act to exclude the emails relevant to the wife's credit failed.

Somewhat surprisingly there are no reported decisions that have grappled in any detail with possible offences under s 478.1 of the Criminal Code. Where a client has 'hacked' into the other party's email account, knowing that s/he does so without the consent or knowledge of the other party, it is likely that an offence under s 478.1 has been committed. It would be wise to consider seeking a certificate under s 128 Evidence Act or section 11 Evidence Act 1906 (WA) before proceedings further.

The crucial questions to consider with a client who shows you emails to which s/he had not prima facie access are as follows:

- How did the client obtain access to the email?
- Did the client use any software designed to enable access to another person's email account?
- Did s/he use someone else's password to do so? If so, when and on what basis did she acquire the password?
- Did the other party give specific consent at any time to the client accessing his or her emails? If so, has that consent been withdrawn?
- What was the understanding between the parties as to access to each other's emails – both during and after the relationship?

Criminal Code Compilation Act 1913 (WA)
Chapter XLIVA — Unauthorised use of computer systems

440A. Unlawful use of computer

(1) In this section —

computer system includes —

(a) a part of a computer system;

(b) an application of a computer system;

password includes a code, or set of codes, of electronic impulses;

restricted-access computer system means a computer system in respect of which —

(a) the use of a password is necessary in order to obtain access to information stored in the system or to operate the system in some other way; and

(b) the person who is entitled to control the use of the system —

(i) has withheld knowledge of the password, or the means of producing it, from all other persons; or

(ii) has taken steps to restrict knowledge of the password, or the means of producing it, to a particular authorised person or class of authorised person;

use a computer system means —

(a) to gain access to information stored in the system; or

(b) to operate the system in some other way.

(2) For the purposes of this section a person unlawfully uses a restricted-access computer system —

(a) if the person uses it when he or she is not properly authorised to do so; or

(b) if the person, being authorised to use it, uses it other than in accordance with his or her authorisation.

(3) A person who unlawfully uses a restricted-access computer system is guilty of a crime and is liable —

(a) if by doing so the person —

(i) gains a benefit, pecuniary or otherwise, for any person; or

(ii) causes a detriment, pecuniary or otherwise, to any person,

of a value of more than $5 000, to imprisonment for 10 years;

(b) if by doing so the person —

(i) gains or intends to gain a benefit, pecuniary or otherwise, for any person; or

(ii) causes or intends to cause a detriment, pecuniary or otherwise, to any person, to imprisonment for 5 years;

(c) in any other case, to imprisonment for 2 years.

Summary conviction penalty in a case to which paragraph (c) applies: imprisonment for 12 months and a fine of $12 000.