#Sext, roll, troll and lol: social media crimes and evidence

NSW Aboriginal legal Service, Western Region Conference, 13 March 2014

INTRODUCTION

This paper is an update of a paper given to the Legal Aid NSW Children's Legal Service Conference in 2011 entitled "Sex, Lies and Youtube tapes: Sexting, Mobiles and Cyber Evidence". That paper was a joint paper with my colleague Julianne Elliott. Her paper focussed on social media crimes, principally sexting and cyberbullying. My paper focussed on evidence.

For this Aboriginal Legal Service Conference, I have updated Julianne's paper too and that is attached. I have renamed the papers simply so that I could indulge in creativity and demonstrate my proficiency (or lack thereof) in internet jargon.

The past few years has seen an explosion in developing technologies and access to such technologies, especially by young people. Most young people are now users of smart phones and have access to the internet and, in particular, social networking sites (SNS) – eg Facebook, Bebo, Myspace, Twitter etc.

The law is struggling to catch up with how the use of these technologies can be governed (if at all). Inevitably, with new technologies come new crimes and new ways to use the technology to investigate and prosecute crime. The use of the internet in criminal proceedings raises a number of evidentiary concerns and also privacy and ethical concerns. Hence, it is vital for criminal lawyers to have some understanding of the technology, the offences, the ethical concerns and the evidentiary issues.

What this paper is about

This paper deals with social media evidence. The mobile phone is the most portable of the tools in which to engage with social media. Hence, this paper will also examine evidence that is obtained from mobile phones in particular.

I do not claim to be a tech head and, whilst some basic explanation is necessary, this paper does not seek to explain how a mobile phone or computer/internet works. There are several other papers by experts which already provide detailed information about how the technology works; where possible, I have included references to them.

COMMONWEALTH MATTERS

There are both State and Commonwealth offences which rely on mobile phone and social media evidence. It is thus worth noting that Section 68 of the *Judiciary Act 1903 (Cth)* applies state and

territory procedure to Commonwealth matters, which means that the *NSW Evidence Act 1995* and *Criminal Procedure Act 1989* apply in Commonwealth matters heard in NSW state courts[1].

MOBILE PHONES

Almost all clients will have a mobile phone and many prosecution briefs will now have some reference to a mobile. Mobiles are used in crimes in a variety of ways, including:

- Sexting and cyberbullying
- Robberies of mobiles
- Use of mobiles in drug deals
- Contacting of co-offenders
- Filming/taking pictures of the crime

There are a now a myriad of different types of mobiles and plans and the latest generation of mobiles are used as portable computers with internet and GPS capabilities. To the extent where such phones deal with social media evidence, I will leave that discussion till later. This section will focus on evidence that is obtained from the mobile phone itself.

Generally, mobiles can provide the following evidence:

- Caller/receiver identification
- Time and date of call and/or messages (ie SMS[2] or MMS[3])
- Duration of the call
- Call charge details
- Whether the call/text was sent/received
- Content of messages
- Content of calls (where a telephone intercept is used)
- The cell site used and (arguably) the location of the caller/receiver
- Contents of the phone/SIM

Such evidence can be obtained from telecommunication companies (telcos) either by way of police request and/or by prosecution/defence subpoena. The police have agreements with most telcos and easily obtain records by simply requesting them. Often the evidence will simply be in the form of a simple statement by a telco employee, with attachments which are tendered as business records. Sometimes, a telco expert will be required to give evidence.

SIM, IMEI and IMSI

It is common knowledge that in order to use a mobile you require a mobile phone handset and a SIM card. SIM cards can be removed from the handset. Details such as messages, photos, videos, and contacts can be stored either on the SIM card and/or the handset.

---

[1] See further Angela Cook and Frith Way, "Essentials of Commonwealth Criminal Law", 2007 and Lincoln Crowley (Cth DPP), "The Basics of Commonwealth Crime", presented to NSW Bar Association, 13 March 2007.
[2] Short message service. Also known as text.
[3] Multimedia Messaging Service – eg sending a picture and text

The handset is identified by an IMEI number. IMEI stands for International Mobile Equipment Identity number. It is the unique identifier or serial number assigned to each mobile phone handset produced. The IMEI is generally located in the back of the phone and generally found underneath the battery. Call charge records and reverse call charge records will generally include the IMEI number of the handset making the call[4].

IMSI stands for International Mobile Subscriber Identity number. This is the unique identifier or serial number assigned to each SIM card produced. The IMSI is located on the underside of the SIM card. Subscriber details will record the IMSI number of the subscriber's service[5].

Given that SIMs can be removed from handsets, care should be taken when looking at records to notice what the record relates to – the SIM and/or the handset.

Call charge records

Prosecution mobile phone evidence often takes the form of subscriber details and call charge records (CCR). These are records that the police obtain from telcos (carriers). Once the police have obtained information about a handset and/or phone number they can request subscriber details and call charge records. Sometimes several call charge records will be obtained in relation to different phones (eg caller and receiver) who may be using different carriers. Call charge records will include not only details of calls but messages too.

It is worth noting that the records relate to calls which are charged. Thus, it will not record calls that were not answered and calls/messages which were not charged (eg free calls/messages). However, note that reverse call charge records can also be obtained.

Some similar information may also be obtained from phone bills but phone bills will often not have as much details as call charge records. However, if you are after your client's records it may be more cost effective to get their phone bills rather than subpoena a telco for a CCR.

Subscriber details

Each telco maintains a register of subscriber details.

Almost every client has a mobile. Some have several mobiles[6]. They also frequently change their mobiles, their plans and/or their SIM(s) and/or share their SIM/handset with their friends. Because children cannot enter into contracts, many will have mobiles which have been provided by their parents/relatives/friends. A subscriber check will only reveal who initially subscribed to the mobile but may not necessarily establish a direct link to your client. If the subscribing parent does not give evidence that the phone was used by the child, the police may have difficulties in establishing a nexus between the client and the phone/SIM.

I could not find any reported cases where the issue of subscription versus use of the phone has arisen and been the subject of a court's decision. Evidence that a parent is the subscriber is still circumstantial evidence that may be admissible. In any event, I could foresee that if this issue did

[4] Mark Dennis, *Identification, Alibi and the "Electronic Snail Trail"*, 2009, p 59
[5] Ibid.
[6] There can be a variety of different innocent explanations for have several phones – it is not necessarily an indication that they are involved in a drug trade.

become an evidentiary problem for the police the legislature might consider something similar to a Form of Demand where the subscriber would have to reveal the user of the phone, much like the owner of a car must reveal who drove their car if it is linked with a serious crime.

Further complications arise for pre-paid mobiles. "Beware of prepaid mobiles with false identities registered as the subscriber details. It is a matter of routine for even the most amateur offenders to register pre paid phones under false identities"[7].

The contents of the phone/SIM

Often evidence is obtained directly from the contents of the mobile phone handset and/or SIM that is located on and/or associated with a defendant.

Some examples include:

- The client uses their SIM card in the robbery victim's mobile handset and/or used the victim's SIM in their own mobile handset
- The client has taken photographs/video on their phone of the proceeds of crime
- The client has photographed/videoed the actual crime itself using their mobile
- There are text admissions on the client's mobile

Evidence of the contents on mobiles/SIMs can corrobate call charge records or provide evidence that can't be obtained from call charge records (eg contacts list, missed calls log). The contents of a mobile/SIM may include (but is not limited to):

- Contacts – this is handy to prove an association between co-accused. The police could find the co-accused name (or nickname) in the contacts and then do a subscriber check on the co-accused number(s) listed. Sometimes contacts will also list addresses and emails.
- Call log – showing dialled, missed and received calls
- Missed calls- shows the phone numbers of unanswered received calls, if available on the network. Will show as "no number" if the number is unknown, eg a call from a public phone.
- Received calls logs
- Call duration log
- Voice messages
- Messages – this includes text messages and picture messages. The message folder of a phone could include evidence from the inbox (including evidence about whether the message was opened), outbox (including items which may not have been sent due to some error) , sent items, saved items, drafts (eg messages that were typed but not sent yet)
- Message log – counts how many messages are sent/received. Thus, even if messages are deleted from the message folder they will still appear as a figure in the message log, unless the counter has been cleared.
- Emails
- Date and time settings
- Photo gallery

[7] Mark Dennis, *op cit*.

- Video gallery
- Audio recordings
- For phones with internet access – the cache (which stores some data about sites which are visited).

Any evidence of the contents of a phone/SIM should be compared with CCRs for discrepancies. A message may appear on a phone inbox or a call appear on a phone's call log but not appear correspondingly in the CCR. The date/times may not match. There may be some explanation for the inconsistency – eg the messages/calls were not charged, the phone's clock is inaccurate. However, it is up to the prosecution to provide these explanations and any lack of a satisfactory explanation may raise questions in the tribunal's mind in relation to the admissibility of the evidence or the weight to be given to it. See *R v Edwin (No 2)* [2013] ACTSC 84 where it was argued that text messages should be excluded as unreliable because they appeared to be partially inconsistent with usage records relating to the mobile phone numbered alleged to have been used by the accused. The discrepancies in that case were not significant enough to render the evidence unreliable.

Similarly, if you have been served with CCRs you may wish to compare them with the contents of the phone/SIM. If the mobile phone is in police custody as an exhibit, this may mean you need to request to examine the exhibit yourself, obtain a forensic expert to examine it or request that the police's use their expert to examine it.

<u>Searches of mobile phone/SIM contents</u>

Sometimes there may be an argument about whether the police can search the contents of defendant's mobile. The legislation and case law relating to the legality/propriety of police searches applies equally to the seizure and searches of mobiles. Police cannot seize and search a mobile without reasonable suspicion. So, if a child is arrested for offensive language, without more, the police cannot go through the contents of the child's mobile. If the police do have a reasonable suspicion in relation to the phone (eg the victim says that the offender videoed the offence using their phone) they could seize and search the phone. If access to the phone is password/PIN protected, it is arguable whether the police can force the owner to provide the password/PIN. Would refusal to do so amount to hindering a police officer in the execution of their duty? Is it analogous to refusing to unlock the front door of a house that is subject to a search warrant?

In *Semaan v Poidevin* [2013] NSWSC 226, Rothman J said (at 73):

> I shall consider first, the word 'hinder' alone. What must be proved against an alleged offender is conduct that, as a whole, is correctly characterized as a hindering. 'Hindering' is a complex fact comprising, in my opinion, acts by the alleged offender –movements or sounds or both; knowledge or appreciation that something is apparently being done or attempted by another; a realization that the probable consequence of what he, the offender, is doing will be to impede or obstruct the other person's acts or attempted acts; and an actual impeding or obstruction of the other person's acts or attempted acts in consequence of what the alleged offender did".

Generally, mere inaction is not hindering: *Leonard v Morris* (1975) 10 SASR 528.

However, In *Towse v Bradley* (1985) 60 ACTR 1[8] the failure of a person to obey the direction of a police officer to move from a room during a search warrant was held to be hindering:

In *Curran v Thomas Borthwicks & Sons Ltd* (1990) 26 FCR 241*,* the defendant refused to allow union officers to see records. Gray J said (at 257-258):

> Among the obligations of an employer pursuant to s 286 of the Act is an obligation to make available certain documents and records for inspection. If an authorised officer attends at premises, and asks to see certain documents or records which he or she is entitled to inspect, some positive act will usually be required on the part of the employer, or the occupier of the premises, to make those documents and records available…Merely to indicate that the relevant documents and records can be found somewhere in a filing cabinet within a large building would amount to a hindrance or obstruction of the right to inspect. The exact content of the positive obligation will depend upon the circumstances. If records are stored in a computer, it may be necessary for an employee with knowledge of the operation of the computer and the relevant codes to make available the relevant records for inspection. Failure to do so will amount to a hindrance or obstruction. …

See also *Darlaston v Parker* [2010] FCA 771 and *Preece v Boyd & McDougall* [2003] NSWSC 172.

Whether failure to provide the mobile's password/PIN to a police officer who seeks to search the phone is hindering or not, the police's State Electronics Evidence Branch(SEEB) could probably obtain access to the phone's content without the password/PIN anyway.

Finally, I note that there are general search and seizure powers within the Law Enforcement (Powers and Responsibilities) Act 2002 but s 87M *specifically* relates to mobiles:

87M Power to seize and detain things

(1) A police officer may, in connection with a search under this Division:
    (a) seize and detain, for a period of not more than 7 days, a vehicle, mobile phone or other thing if the seizure and detention of the vehicle, phone or thing will assist in preventing or controlling a public disorder, or
    (b) seize and detain all or part of a thing (including a vehicle) that the officer suspects on reasonable grounds may provide evidence of the commission of a serious indictable offence (whether or not related to a public disorder).

(2) The Local Court may, on the application of a police officer, authorise the continued detention of a vehicle, mobile phone or other thing under subsection (1) (a) for an additional period not exceeding 14 days if satisfied that its continued detention will assist in preventing or controlling a public disorder. More than one extension of the detention may be authorised under this subsection, so long as each extension does not exceed 14 days.

(3) A power conferred by this section to seize and detain a thing includes:
    (a) a power to remove a thing from the place where it is found, and
    (b) a power to guard the thing in or on the place where it is found.

[8] (1985) 73 FLR 341; (1985) 14 A Crim R 408

(4) The regulations may make provision for or with respect to the seizure, detention and return of vehicles, mobile phones or other things referred to in subsection (1) (a).

This power was introduced as a result of the Cronulla riots – to prevent the calling of others to join in a riot. I note that this power relates to the seizure of mobiles for a *specified* purpose: the prevention or control of a public disorder or if there is reasonable suspicion that the mobile may provide evidence of the commission of a serious indictable offence (ie not just any lesser offence).

I also note that the section provides for the *seizure* of mobiles but does not provide power per se for *searching* the contents of such mobiles, though such a search may be implied by the phrase "may provide evidence" in s 87M(1)(b).

Date and time[9]

The date and time of calls/messages from phones is only as accurate as the date/time settings on the device that records them or the telco's clock. Thus, the accuracy of a date or time stamp should not be assumed. Neglect in regards to the setting of clocks can lead to significant inaccuracies. Two common sources of neglect include missing the 29 February (ie the leap year) and not adjusting for daylight saving[10].

When considering dates and times it is important to recognise what the date and time actually signifies. The time that a message is sent is not necessarily the time that a message is received. The time that the message is sent may not even be the time that the sender pressed the "send" button. There may be a delay between the pressing of the "send" button and the message being sent due to a lag in the carrier sending the message.

Where possible, compare the dates/times of phone records to the dates/times of other applicable computer records or internet records for corroboration or inconsistencies. See *R v May* [2007] QCA 333 where the appellant contended the verdict was unreasonable because of discrepancies between the evidence of internet chat usage and his telephone and work records.

Audio conversations

The substance of a phone audio conversation will generally not be obtainable without a telephone intercept (TI). Be aware that a telephone intercept can pick up more than just the conversation between the caller/receiver. For instance, my client was alleged to have been in the getaway car with the co-accused whose mobile was subject to a TI. The co-accused made a phone call to another person. *Even before the call was answered* the TI picked up conversation between the co-accused and my client in the car; ie the mobile was acting like a listening device. This evidence, combined with mobile phone location evidence (see below), provided a nexus between my client, the co-accused and the offence.

[9] The remarks here about clocks applies equally to internet evidence: eg you cannot assume the accuracy of the date/time stamp on the header of an email. Time stamping on social media, which may involve overseas offices, is even more complicated because it may involve several time zones.
[10] Mark Dennis, *op cit*, p 58

Similar to the above example, asides from recorded *phone* conversations, witnesses and victims are increasingly using their mobile phones like listening devices to record conversations surreptitiously. These recordings may be contravening Part 2 of the Surveillance Devices Act 2007, eg:

> 7 Prohibition on installation, use and maintenance of listening devices
>
> (1) A person must not knowingly install, use or cause to be used or maintain a listening device:
>
> (a) to overhear, record, monitor or listen to a private conversation to which the person is not a party, or
>
> (b) to record a private conversation to which the person is a party.
>
> Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

However, s 7(3) provides:

> (3) Subsection (1) (b) does not apply to the use of a listening device by a party to a private conversation if:
>
> (a) all of the principal parties to the conversation consent, expressly or impliedly, to the listening device being so used, or
>
> (b) a principal party to the conversation consents to the listening device being so used and the recording of the conversation:
>
> (i) is reasonably necessary for the protection of the lawful interests of that principal party, or
>
> (ii) is not made for the purpose of communicating or publishing the conversation, or a report of the conversation, to persons who are not parties to the conversation.

Where a victim is recording a conversation in connection with the commission of an offence, it is arguable that they are protecting their lawful interest. See *Prosha Pty Ltd v AXL Pty Ltd (RAD)* [2011] NSWADTAP 36.

Messages

Another common way that police can obtain evidence of conversations (eg with admissions) is be looking at conversations held via messages (most commonly SMS messages). These can be obtained from telcos or by directly from the mobile phones involved in the texting.

Carrier transcription

Call charge records from all telcos will show the fact of SMS messages having been sent/received. Some telcos have the capacity to record the contents of the messages but this is often not possible.

"SMS/MMS communications are "store and forward" messages. Unlike the direct transmission of an email from server to server via a network, SMS/MMS messages are relayed by the sender's device

indirectly to the recipient via a short message service centre (SMSC) or a mobile message service centre(MMSC). The SMS/MMS message sits in the SMSC/MMSC which is essentially a processor. The processor attempts to forward the message to the recipient device, often making several attempts over a defined period, such as 24 hours, before the delivery is successful. It is informative to note that the time when a mobile handset displays "message sent" it simply means that the message has been received by the SMSC. The two parts of the SMS message, the mobile originated and the mobile terminated, are independent of each other. Due to the enormous volume of messages transmitted to the SMSC/MMSC in any given period, messages are routinely deleted by carriers on a daily basis"[11].

Also, beware that (for unknown reasons) for some time Vodafone had its SMS service running on New Zealand time (2 hours ahead of Sydney)[12]. "Also, be aware of the capacity to generate SMS messages from personal computers and attribute them to particular mobile phone accounts"[13].

Police transcription

Where the actual messages are not obtainable from the telco, police often can obtain them from seized phones, although they may need to view the sender and receiver phones to get the full conversation, especially if some messages have been deleted from one phone. Police sometimes simply transcribe what they see on the phone and/or do a screenshot of the phone. One common way of obtaining a "screenshot" is to place the handset on the photocopier and photocopy it – the difficulty with this is that it will only capture what is on the screen at the particular time. If the message is bigger than the screen the police will need to scroll down in order to capture the full message; they sometimes neglect to do this.

You should never assume that a police officer's transcription is accurate. Police sometimes only transcribe what they think is relevant and may miss exculpatory evidence or miss other messages which provide context. They also may not provide verbatim transcription. They may not record the full time down to the second. They may miss emoticons (eg ☺ or ☹) which may change the context of a message. The insertion of a :-P or ;-) ie a "sticking out a tongue" or "winking", or a "lol" (ie laugh out loud) may mean that the message is a joke. They may transcribe "today" instead of "2day" etc. Some of these discrepancies may not be significant by themselves, but when added together they may cast doubt on the accuracy of the transcriptions and lead to the transcription being unreliable and inadmissible or given less weight.

With regards to context, particular care must be taken to piece together a two way conversation[14], noting the times that messages were actually sent/received/read. Be aware that there may be overlaps in the sending of messages. You may have to take care to work out what a message is in response to.

[11] Sarah Alderson, "Interception of and access to communications", *Communications law and Policy in Australia*, Lexisnexis
[12] Mark Dennis, *op cit*, p 60.
[13] Mark Dennis, *op cit*, p 61
[14] Additional difficulties arise when there are even more than two parties or when someone is using someone else's phone.

For example

A: how you going?

A: are you right to go ahead with robbery?

B: ok

Is very different from:

A: how you going?

B: ok

A: are you right to go ahead with robbery?

SEEB transcription

The police have access to a State Electronics Evidence Branch (SEEB) which can use software to download messages. Where the police have not used SEEB and just transcribed messages manually themselves, they could be questioned about whether they had considered the use of SEEB to do the job properly.

Some downloads of phone/SIM content can be performed by ordinary police with special equipment, without recourse to the SEEB, but not all police may be familiar with the use of such equipment: see discussion below. A SIM card can be placed in a SIM reader and software (SIM Manager) will download the SIM's contents so that it can be printed out. However, the SIM Manager will not be able to access deleted material from the phone; only SEEB may be able to do that.

A printout of a phone/SIM download (either by SEEB or ordinary police) may still be subject to objection. There is a question about whether mobiles and computers fall within the category of "notorious scientific instruments". There is a common law presumption that readings of "notorious" scientific or technical instruments (eg clocks, speedometers, thermometers) are prima facie evidence of the facts which they purport to register[15]. They can be received into evidence without specific proof of their accuracy. The rule is sometimes described as the presumption of accuracy of scientific instruments[16]. The rule has applied to printouts of computerised data[17] . However, in *Bevan v Western Australia* (2010) 202 A Crim R 27; [2010] WASCA 101 the court considered the admissibility of mobile phone data downloaded by a computer software program. The court found that mobile phones and computers were notorious scientific instruments but nevertheless ruled that there was insufficient evidence that the software was reliable and that the downloading process was operated properly. It is helpful to extract the full reasons so that the technical aspects of the download process can be understood. Blaxwell J said at [34]-[38]:

Whether the text messages were admissible

[15] *Porter v Kolodzeij* [1962] VR 75 at 78.
[16] *Cross on Evidence* at [3070], LexisNexis.
[17] *Mehesz v Redman (No 2)* (1980) 26 SASR 244; *R v Weatherall* (1981) 27 SASR 238. See also *Philpott v Boon* [1968] Tas SR 97; H*olt v Auckland City Council* [1980] 2 NZLR 124; *Castle v Cross* [1985] 1 All ER 87; *R v Jarrett (No 1)* (1994) 62 SASR 443; *R v Ciantar* (2006) 16 VR 26.

34 Mobile phones and laptop computers are ubiquitous items which have been in common use in the community for a number of years. Most people (including school children) are very familiar with the processes of sending and receiving text messages on mobile phones, and of downloading data from computers. It is also a matter of general knowledge and experience that these processes are accurate in the sense that the data displayed (or printed out) replicates what is actually there. It follows that mobile phones and laptop computers each fall into the category of 'notorious' scientific instruments.

35 In my view, the downloading of data from a mobile phone into a laptop computer is a process which probably requires very little evidence to be readily understood, but which is not yet generally known to be accurate. Accordingly, relevant data obtained in this way will be admissible if there is evidence from a suitably qualified person to prove that the process produces accurate results, as well as evidence to show that the downloading was properly carried out on the particular occasion in question. (There is no reason why evidence as to both of these matters cannot come from a person who has had sufficient experience of the process on previous occasions).

36 In the present case, Constable Brouwer carried out two separate downloading operations, one from the SIM card, and the other from the mobile phone itself. He was experienced in carrying out the first operation in that he had downloaded SIM cards using the same software and successfully produced similar data on at least eight previous occasions. Although this evidence suggests that the downloading was carried out properly on the particular occasion in question, it permits only a vague understanding of what was involved. In this regard, and as a matter of common knowledge, a SIM card cannot be 'hooked up' directly to a computer. Of necessity, some additional device must have been involved.

37 There are greater difficulties in understanding the second downloading process (from the mobile phone memory). Constable Brouwer was not asked to explain this process in any detail, but he made mention of a web camera taking film of the text messages while they were displayed on the mobile phone. It was the first time he had experienced the relevant software and he did not have any formal training in its use. It was also his evidence that the software 'tried to do its best job at doing it'. To my mind this clearly raised questions as to the reliability of the software and of Constable Brouwer's correct use of it. In my view, the prosecution failed to establish that the downloading process was of a type generally accepted by experts as being accurate, and that the particular downloading by Constable Brouwer was properly performed.

38 It follows that ground 2 has been made out, and that the trial judge erred in law in admitting the text messages into evidence.

See also *Bevan v Western Australia* [2012] WASCA 153.

Extract/ summary of transcript or explanatory material

As illustrated above simply tendering the CCRs, subscriber details and SEEB downloads may not provide an easily decipherable picture of the actual conversation. Thus, the prosecution or defence may seek to tender extracts and/or summaries of the transcript or explanatory material. This may be permissible under ss 29 and 48 Evidence Act.

Section 48:

(1) A party may adduce evidence of the contents of a document in question by tendering the document in question or by any one or more of the following methods:

(b) tendering a document that:

(i) is or purports to be a copy of the document in question; and

(ii) has been produced, or purports to have been produced, by a device that reproduces the contents of the documents;

(d) if the document in question is an article or thing on or in which information is stored in such a way that it cannot be used by the court unless a devise is used to retrieve , produce or collate it – tendering a document taht was or purports to have been produced by use of the device

(e) tendering a document that:

(i) forms part of the records of or kept by a business (whther or not the business is still in existence); and
(ii) is or purports to be a copy of, or an extract from or a summary of, the document in question, or is or purports to be a copy of such an extract or summary

s 29(4):

Evidence may be given in the form of charts, summaries, or other explanatory material if it appears to the court that the material would be likely to adi its comprehension of other evidence that has been given or is to be given.

See *R v Georgiou* [2005] SNWCCA 237 for a discussion of these two sections, especially s 48.

Never sent messages

It is worth noting that messages which are never sent are still representations within the Dictionary definition in the Evidence Act:

"representation includes:

(c) a respresentation not intended by its maker to be communicated to or seen by another person, or

(d) a representation that for any reason is not communicated".

See *Dragon v R* [2010] NSWCCA 329 at [359]-[367].

Admissibility of messages

Generally, in relation to evidence that is taken from a mobile phone or received from a mobile phone (eg messages, pictures/videos etc), see the discussion below about the admissibility of social media evidence (eg authentication, hearsay etc). Those issues apply equally to mobile phone evidence. The only difference is that there are subscriber checks done on mobile phones which may provide more cogent evidence of who may have used a mobile phone or mobile phone number. Arguably, there is more verification of identity when subscribing to a mobile plan than there is when subscribing to Facebook.

As well as authentication issues about who *sent* a text message there may sometimes be issues that arise about who is *receiving* the text message. In *R v Edwin (No 2)* [2013] ACTSC 84 the parents of a friend of a child (CR) took CR's phone without her permission and engaged in communications with

the accused, as a result of concerns that CR was being groomed. It was alleged that the accused thought he was communicating with CR. It was argued that the text messages he sent were illegally obtained because the parents had contravened s 474.5(1) of the Criminal Code 1995 (Cth) – wrongful delivery of communications.

> 474.5 Wrongful delivery of communications
>
> (1) A person is guilty of an offence if:
>
> (a) a communication is in the course of telecommunications carriage; and
>
> (b) the person causes the communication to be received by a person or carriage service other than the person or service to whom it is directed.
>
> Penalty: Imprisonment for 1 year.

The phrase "communication in the course of telecommunications carriage" is defined in s 473.1 of the Criminal Code 1995 (Cth):

> "communication in the course of telecommunications carriage" means a communication that is being carried by a carrier or carriage service provider, and includes a communication that has been collected or received by a carrier or carriage service provider for carriage, but has not yet been delivered by the carrier or carriage service provider.

Burns J said (at 37-38):

> A communication ceases to be "a communication in the course of telecommunications carriage" once it is received: see the definition in s 473.1..there is nothing to suggest that CR's mobile phone was part of a carriage service, or that she or it come within the definitions of "carrier" or "carriage service provider" in the Telecommunications Act. It should not be forgotten that the communication was sent to, and received by, a device, being CR's mobile phone. The carrier or carriage service provider delivers them to the device, not to the person who owns or is in possession of the device. As such, delivery of the relevant communications between the accused and CR (as he thought was occurring) occurred when the text messages were received on CR's mobile phone.
>
> In my opinion, s 474.5 of the Criminal Code 1995 (Cth) protects the integrity of the carriage service, and is not concerned with what becomes of the communication after it is received by the device to which it is sent. The section addresses the diversion or hijacking of a communication whilst it is being carried by the carriage service.

<u>Tendency/coincidence evidence</u>

Sometimes the prosecution will seek to adduce evidence of phone calls/messages which don't relate directly to the offence charged. For example, in drug supply matters the fact that a phone was constantly receiving calls/messages and messages describing the price of products (often using not

very imaginative code words). Unless the evidence is somehow admissible as transaction evidence, it is tendency/coincidence evidence and notice should be served.

Location

Police may also seek to use mobile phones as evidence of the location of an accused at the time of an offence. This is done by inferring the location of the mobile phone user from the base station that the mobile is using. This type of evidence was used to convict Mr Phuong Ngo in 2000 of the assassination of John Newman[18].

The production by a carrier service of a mobile call history is not a matter of expert evidence but simply a business record. However, any interpretation of those records, beyond the fact that a call was made at a particular time to a particular phone for a recorded time, is a matter of expert opinion. Opinions about location should not be accepted at face value but rather carefully scrutinised. There are a number of factors which can influence which base station is used, including:

- Signal strength of base station attenae
- Terrain (obstructions by buildings or hills) – city base stations often have a smaller geographical coverage than suburban or rural base stations
- Customer demand – a signal may skip to the next closest base station if the one sought to be used is too congested. There are peak periods of the day where skipping is more likely to occur

In *Western Australia v Coates* [2007] WASC 307 at 215-219 Blaxell J said:

> "I have received evidence of a technical and/or semi-expert nature as to the significance of the cell tower details in the Telstra and Optus records. This evidence shows that each provider has its own network of cell towers (or radio base stations) through which mobile telephone calls are transmitted and received. The number and geographical location of base stations depends upon factors such as customer demand, local terrain and the presence of buildings or other obstructions.
>
> Each network is designed so that the field of influence of each individual base station is limited to a restricted area...However these distances can be affected by local obstructions such as buildings or hills and the line of sight connection between a mobile telephone and the nearest base station might bend slightly depending upon the nature of the obstruction...
>
> The fact that a call was transmitted or received via a particular base station is strong but not conclusive evidence..."

See also *R v Aboud; R v Stanley* [2003] QCA 499 at para 24-26 and *Wood v R* [2012] NSWCCA 21.

Many phones now have GPS installed. This technology has its own difficulties in establishing the location of the phone.

[18] There was lively public debate about whether this conviction was safe and the NSW Chief Justice established an inquiry about the issue.

For an in depth discussion about this topic see:

- Reg Coutts and Hugh Selby, *Safe and Unsafe Use of Mobile Phone Evidence*, Public Defenders Criminal law Conference 2009[19].
- Tim Moors, *Locating Users of Mobile Phones*
- Ajoy Ghosh, *Computer Evidence 101 for Criminal Lawyers*
- Mark Dennis, *Identification, Alibi and the "Electronic Snail Trail"*, 2009

[19] Available from the NSW Public Defenders website.

SOCIAL MEDIA EVIDENCE

Social media evidence falls within the broader definition of electronic evidence. This paper will not discuss electronic evidence obtained from a computer's hard drive. For information about that topic see:

- Allison Stanfield, *Computer Forensics, Electronic Discovery and Electronic Evidence*, LexisNexis Butterworths, Australia, 2009
- Ajoy Ghosh, *Computer Evidence 101 for Criminal Lawyers*

See also *R v McConhie* [2010] ACTSC 137 for a recent case discussing a computer forensic examiner's methods of examining electronic evidence.

Web 2.0

What is known as Web 2.0 is the "social web". It includes (but, no doubt, is not limited to) the following:

- Social networking sites which build virtual communities where users can create their own web page and community with others via online chat, instant messaging services, blogging and audio/video. Examples including Facebook, Myspace, Bebo and Linkedin.
- Blogs – websites that contain an online journal and often hyperlinks
- Tweeting – users upload short messages from computers/mobiles
- Wikis – websites that allow users to add, remove or edit content, such as Wikipedia
- User generated sites which allow users to create content. Examples include Youtube where users upload/watch videos or Flickr where users share photos
- Mash ups – websites that create content by combining content from difference sources, such as iGoogle
- AJAX (Asynchronous Javascript and XML) that allows the development of Web applications such as GoogleMaps[20].

This paper will not deal with all of the above but focus on those which are most likely to be used in criminal proceedings: Facebook, Twitter, Youtube and Snapchat. I will firstly briefly introduce each service (what they do, what is required to register/access, what information is collected/privacy policies, and policies in relation to law enforcement) before dealing with evidentiary issues which may be common to all. As most social media evidence will come from Facebook, for ease, I may refer only to Facebook even though the issue may also be relevant to other social media.

[20] Stanfield, A, *Computer Forensics, Electronic Discovery and Electronic Evidence*, LexisNexis Butterworths, Australia 2009, pp 333-334; Stanfield, A. And Pham, N, *Web 2.0 technologies as evidence*, Internet Law Bulletin, 2010 Vol 12 No 9.

I note that The Australian Government has recently established a Consultative Working Group on Cybersafety and a "Cooperative arrangement for complaints handling on social networking sites". Facebook and YouTube have submitted cooperative arrangements to the Working Group.

Youtube

Youtube is a video sharing website which is now a subsidiary of Google. There between 10.3 million - 11 million users of Youtube in Australia and over 1 billion unique global users each month[21].

Youtube is a video sharing website that allows users to upload, view and comment on videos. Videos uploaded to the site are publicly accessible. You can watch videos on YouTube without having a Youtube account or a Google account. For some activities on YouTube, like uploading videos, posting comments, flagging videos or watching restricted videos, you need a YouTube or Google account. You need to provide an email address and a password. When you create a YouTube account, some information about your YouTube account and your account activity will be provided to other users of YouTube. This may include the date you opened your account, the date you last logged into your account, your age (if you choose to make it public) the country and the number of videos you have watched. You may choose to add personal information such as your name, gender, profile picture[22].

With the wide availability of mobile phones with video cameras, offences can be filmed and then distributed on the internet via way of YouTube. Evidence from YouTube may be used against your client if possession/dissemination of the clip can be traced back to your client or your client is visible on the footage[23].

Twitter

"Twitter is a real time information network powered by people all around the world that lets users share and discover what's happening now. Users send 140 character messages through Twitter's website and mobile site, client applications or any variety of third party applications"[24]. Tweets are publicly accessible but users may also send private messages to other users[25].

There are 2.1 million users of Twitter in Australia and, globally, 554 million registered users each month[26]. Surprisingly, the average age is 38 years old. Twitter does not provide services to children under 13 years old.

Twitter Inc is owned by Google.

---

[21] Some statistics obtained from Dr David Bright, Kimberley Lee and Peter McGhee, "Social media – its impact on you and your clients", ANZAPPL NSW seminar, Public Defenders, 29 August 2011. See also Blackham, Alysia; Williams, George, 'Australian Courts and Social Media' [2013] UNSWLRS 66 (last updated 27 September 2013).
[22] See Youtube Privacy Notice, 8 December 2010.
[23] See discussion of *McKeogh v John Doe 1 & Ors* [2012] IEHC 95 below.
[24] http://support.twitter.com/groups/33-report-a -violation/topics/148-policy-information.
[25] Blackham, Alysia, *op cit*.
[26] Blackham, Alysia, *op cit.*

When you create or reconfigure a Twitter account you provide personal information such as name, username, password and email address. Your name and username is made public. Other additional information may be provided to the public: a short biography, your location, a picture. Twitter's servers automatically record information (log data) created by your use of the services. Log data may include information such as your IP address, browser type, the referring domain, pages visited, your mobile carrier, device and application IDs, and search terms. If Twitter hasn't already deleted the log data ealier, they will either delete it or remove any common account identifiers (such as username, full IP address or email address) after 18 months.

Twitter and law enforcement

Twitter's Guidelines for Law Enforcement states: "Non public information about Twitter users is not released except as lawfully required by appropriate legal process such as a subpoena, court order, or other valid legal process document. Some information we store is automatically collected, while other information is provided at the user's discretion, Though we do store this information, it may not be accurate if the user has created a fake or anonymous profile. Twitter doesn't require email verification or identity authentication".

Twitter Inc is located in California and "will only respond in compliance with US law to valid legal process". Its terms of services state: “All claims, legal proceedings or litigation arising in connection with the Services will be brought solely in the federal or state courts located in San Francisco County, California, United States, and you consent to the jurisdiction of and venue in such courts and waive any objection as to inconvenient forum”.

However, it's privacy policy states "we may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issue; or to protect Twitter's rights or property”.

Snapchat

Snapchat is a photo messaging application released in September 2011. Users can take photos, record videos, add text and drawing and send them to a controlled list of recipients. These sent photographs and videos are known as “snaps”. The user sets a time limit (up to 10 seconds) for how long recipients can view their Snaps, after which they will be hidden from the recipient’s device and deleted from Snapchat’s servers.

There have been concerns raised that Snapchat is being used regularly for sexting.

On 9 May 2013, *Forbes* magazine reported that Snapchat photos do not actually disappear and that the images can be retrieved with minimal technical knowledge after the time limit expires[27].The Electronic Privacy Information Centre consequently filed a complaint against Snapchat with the Federal Trade Commission, stating that Snapchat deceived its customers by leading them to believe that pictures are destroyed within seconds of viewing.

[27] Kashmir Hill, ‘Snapchats Don’t Disappear: Forensics Firm has Pulled Dozens of Supposedly-Deleted Photos from Android phones’, *Forbes*, 9 May 2013.

Facebook

Facebook has over a billion monthly users worldwide and 618 million daily active users. It has 11.5 million users in Australia[28]. The free social networking site allows users to create one or more of the following:

1) Facebook profile – a personal profile eg Aaron Tang
2) Facebook page – eg a corporate page, a page on a topic – eg Aaron Tang's Drinking Fund
3) Facebook Group – eg Aaron Tang drinks too much- discuss.

Most clients will have a Facebook profile and evidence is most likely to come from a profile[29].

What is required to register a profile?

To sign up for a Facebook profile you need to provide your:

- Name
- Email address
- Gender and
- Date of birth

Thus, anyone with an email account (noting that various free email accounts are available without any checks of personal information being conducted) can create a Facebook profile of themselves or someone else. In their Appendix to the above mentioned "Cooperative arrangement for complaints handling on social networking sites", Facebook states "One of Facebook's most important safeguards is our real name culture. ..We have tools to detect fake accounts; and we block the registration of accounts under common fake names".

Once you have registered and set up an account you can edit your profile so that you hide all (or part) of the gender and date of birth fields. You can even change your gender or date or birth, although you can only change your date of birth a limited number of times! The fact that a user can change their date of birth is significant especially for cases involving child sexual offences where knowledge as to the child's age may be important – for example, the defendant claims that they thought the complainant was over 16 years old because their Facebook profile used to say so.

You can also hide your email address. Only your name and profile picture do not have privacy settings. You do not need to upload a profile picture either. Thus, you can hide all your personal information except your name.

The information that you provide for your profile will appear on the page and be visible in accordance with your privacy settings (see below).

Some Facebook functions

Facebook is primarily used to share content with others. Once you have established a Facebook profile you can add/delete "Friends" – ie others with a Facebook account. You can:

[28] Blackham, Alysia, *op cit.*

[29] If I inadvertently refer to a "Facebook page" I am not restricting myself to a Facebook Page (as defined above) but am encompassing any Facebook webpage (Profile, Page or Group) and am mostly likely referring to a Profile.

- View what your Friends have put on their pages (subject to their privacy settings – see below). A "news Feed" informs you of activity on your Friend's pages – eg if Felicity has uploaded a photo, if Dark Menace has changed his status…
- Post messages on a Friend's "wall" (publicly accessible), receive messages on your wall: eg *Just rolled someone today.*
- Comment on other's posts: eg *Aaron Tang likes this.*
- Post messages directly to your Friend's message inbox, receive messages to your inbox: eg *Jane, don't forget to get rid of that knife we used in the roll*
- Update your status: *just finished rolling, have cash for drugs*
- Ask questions
- Add photos/videos: eg *here's a photo of us with the cash from the roll taken with victim's own mobile; here's video of roll*
- Subscribe to applications and websites.
- invite/or be invited to Events: eg *let's go rolling Saturday nite*
- Material can also be "tagged" by Friends – eg if my Friend uploads a photo of me they can tag it as Aaron Tang and the photo is thus linked to my profile page: eg *Tangsta bashing shit out of victim, Dark Menace standing nearby*

Privacy settings

There are three default privacy settings:

- Custom – seen/accessed only by the people you specifically choose
- Friends – seen/accessed only by those you have friended.
- Public – seen/accessed only by anyone who has facebook

There is an option to limit the audience of any past post – eg you can change ex public posts so that they are seen only by Friends.

You can blocked persons, applications, websites, events.

New changes to priacy settings now also allow you to "lock" any activity you engage in on Facebook. This enables Facebook users to choose who they make the activity visible to and who they can hide the activity from. For example, if you post a message on someone's wall, you have the option of choosing exactly who you want to see it and who you don't want to see it.

Despite these privacy settings, in May 2011, Ben Grubb (a journalist from the Sydney Morning Herald) published a story where a security expert demonstrated to him that Facebook had a security weakness that allowed users to access privacy protected photographs without being a friend of the person who loaded the photographs. Mr Grubb was arrested by Queensland police for questioning in relation to the story but was ultimately not charged[30].

Information that Facebook collects:

Facebook keeps track of some of the actions you take on Facebook, such as adding connections (including joining a group or adding a friend), creating a photo album, sending a gift, poking a user,

[30] http://www.news.com.au/technology/facebook-story-arrest-disputed-on-twitter/story-e6frfro0-1226057758607

indicating you like a post. Aside from the actual content (eg a video), Facebook might log the fact that you shared it too.

When you access Facebook from a computer, mobile or other device, Facebook may collect information from that device about your browser type, location and IP address, as well as the pages you visit[31].

Facebook also collects "cookie" information (small pieces of data stored for an extended period of time on your computer/mobile/other device) – eg storing your login ID and automatically inserting it to make it easier for you to login. "Facebook uses cookies to confirm that you are logged into Facebook and to know when you are interacting with Facebook Platform applications and websites, our widgets and Share buttons and our advertisements. You can remove or block cookies using the settings in your browser, but in some cases that may impact your ability to use Facebook"[32].

Facebook also collects information from other users – eg when a friend tags you in a photo/video, provides friend details or indicates a relationship with you.

Statement of Rights and Responsibilities

All Facebook users sign up to a Statement of Rights and Responsibilities[33], last updated 15 November 2013. That Statement includes (inter alia):

- You will not provide any false personal information on Facebook or create an account for anyone other than yourself without permission
- You will not create more than one personal profile
- If we disable your account, you will not create another one without our permission
- You will not use Facebook if you are under 13
- You will not use Facebook if you are a convicted sex offender
- You will not share your password, let anyone else access your account or do anything else that might jeopardize the security of your account

Facebook and law enforcement

Data centres (where data is stored) for popular social networking sites like Facebook are not located within Australia (but in California) and so foreign data protection laws apply[34]. Facebook has a page on "Facebook and Law Enforcement". The page states that "Federal law (Stored Communications Act, 18 USC 2701 et seq. prohibits Facebook from disclosing the contents of an account (such as messages, Wall posts, photos etc) except in response to a civil subpoena or court order. There are ways that we an provide a limited amount of information to help law enforcement officials do their jobs". The Help page: Report Abuse or Policy Violations –Law enforcement and Third Party Matters" provides further details on how Facebook works with law enforcement:

> We work with law enforcement where appropriate and to the extent required by law to ensure the safety of the people who use Facebook. We may disclose information pursuant to subpoenas, corut orders , or other requests (including criminal and civil matters) if we have a good faith belief that he

[31] www.facebook.com/policy.php
[32] www.facebook.com/policy.php
[33] See https://www.facebook.com/legal/terms
[34] Stanfield, A and Pham, N "Discovery of Content on Social Networking Sites: are private sites protected by privacy?" *Internet Law Bulletin* Sept 2010 p 93.

> response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the reponse is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity to prevent imminent bodily harm or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.

Facebook's appendix to the "Cooperative arrangement for complaints handling on social networking sites", revised 11 May 2012, states (at p 2) that Facebook Ireland is the "entity with whom Australian users contract". Facebook's page states that complaints regarding their data use policy or practices can be directed (if you are located outside of the United States or Canada) to Facebook Ireland:

> Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland. Registered in Ireland (Companies Registration Office) Company No. 462932

Facebook has recently agreed to work with the Attorney General department to establish local police guidelines to assist with investigations which involve activity on Facebook[35]. However, there has previously been an uneasy relationship between Facebook and the Australian Federal Police (AFP). In May 2010 there was a public slanging match between the two. The AFP High Tech Crime Centre Assistance Commission Neil Gaughan complained of Facebook's lack of cooperation, whilst Facebook's chief security officer, Joe Sullivan, also accused the AFP of being unresponsive to their requests. The AFP were requesting:

- A Report Abuse button on Facebook profiles
- Verification software to stop children under 13 years old from registering
- Facebook guidelines to take account of Australian legal terminology: citing one instance where Facebook ignored a warrant because it was issued by a judicial official rather than a court.
- A dedicated law enforcement official for Australia: both state and federal police reported difficulties in getting Facebook to comply with Australian police requests or court warrants[36].

Facebook indicated that they had drafted law enforcement guidelines specifically which the Attorney General had responded to but not the AFP. In 2011, I requested Facebook for a copy of any up to date law enforcement guidelines between Facebook and Australian police but my request went unanswered.

Mr Sullivan (Facebook) rejected the need for an Australian based liaison citing that "the data is stored in the US, the tools that we use to access the data are here in the US and our team is staffed to have people on call during the week, during the weekend and at night so physical location is really not going to impact that in the least". The Californian based Australian liaison for Facebook was

[35] Timson, L and Gray, P "Facebook to draw local police guidelines" *the Age*, 16 May 2010; Kelly, L "Privacy on Facebook: issues and implications for individuals and employers" *Internet Law Bulletin* 2010 Vol 13 No 4.
[36] Fitzimmons, C, "Facebook hits back in spat with Australian Federal Police", *The Australian*, 31 May 2010.; Cowling, D, "Australian Federal Police want a Facebook cop", *Social Media News.com.au*, 26 May 2010.

Genevieve Ovalle[37] in 2011. Facebook presently has a confirmed contact person with whom the Australian Government can discuss issues but I could not find (at least not on any publicly available information) the name or contact details for that contact person.

See below in relation to subpoenas to Facebook.

USES OF SOCIAL MEDIA EVIDENCE

A simple search on legal databases will reveal that social media evidence has been used in numerous cases (in Australia, the UK and the US). They include the use of social media evidence in:

- The commission of offences, including sexual offences (eg child porn, grooming etc), fraud and even murder. In *R v Acar* [2011] VSC 310 the offender murdered his infant daughter out of revenge against her mum and posted messages on Facebook in the process: eg "bout 2 kill ma kid", "it's ova i did it", "pay bk u slut". In *R v Dannevig, Christopher James* [2012] NSWSC 1013 the offender murdered his 18 year old victim after meeting her via Facebook where he used a fictitious name.
- In investigations and prosecutions: see, for example, the discussion below on identification via social media.
- Use by jurors. The use of Facebook (and the internet more broadly) by jurors or prospective jurors has been the subject of many cases about whether an accused can receive a fair trial. See *R v Abrahams [*2013] NSWSC 729 and Greene, E and O'Leary J., 'Ensuring a Fair Trial for an Accused in a Digital Era: Lessons for Australia'[38].
- Use in sentencing. Prosecutors have used Facebook evidence to rebut submissions about rehabilitation and remorse (eg photos/videos of a drunk offender facing sentence for drink driving). See *R v Price; ex parte Attorney General (Qld)* [2011] QCA 87 at [34]-[37] for a recent Australian example. On the other hand, evidence of how Facebook photos were used by the media to harass swimmer, Nicholas D'arcy, was used to try and establish extra curial punishment[39]. See also *Duncan v R* [2012] NSWCCA 78.

Identification via social media

Increasingly, identification of suspects is occurring from photos/videos on the internet. This identification is being made by both police and witnesses. Of course, such identification is fraught with danger, above and beyond the normal dangers associated with identification evidence:

- Internet identification is not subject to the same controls as an identification parade/photo identification parade

[37] Fitzimmons, *supra.*
[38] In Keyzer, P, Johnston, J and Pearson M., *The Courts and the Media: Challenges in the era of digital and social Media*, Halstead Press, 2007, p 101
[39] DPP v D'Arcy [2009] NSWLC 1

- Images on the internet may be altered (intentionally or unintentionally – eg resolution changes when images are uploaded/downloaded etc)
- Images may be accompanied by other prejudicial material which may influence the identification
- You have little control over images of you that others may place on the internet

Often, a prosecution witness may be directed to a webpage containing a photo/video of the defendant with the pre-conceived idea that the photo/video they are viewing is that of a suspect: eg the police, media and/or other parties have named the defendant as a suspect. Recently, I was involved in a case where the child client was charged after an identification of his photo on the internet by the victim. The victim had been informed by friends of friends of friends that my client might have been the offender or at least present at the scene of the offence. He then conducted a search of Facebook and identified my client's Facebook photo(s). Other witnesses then followed suit. The relevant photos were never served with the brief. Of course, identification in such circumstances is subject to the displacement effect and strongly argued to be inadmissible: *Alexander v R* (1981) 145 CLR 395; *Davies and Cody v R* (1937) 57 CLR 170. However, each case must be examined in light of its own circumstances. As is apparent from the cases reviewed below, my above example is not uncommon.

In *Murdoch v R* [2007] NTCCA 1, the witness (Ms Lee) had witnessed the murder of her boyfriend Peter Falconio. Whilst she was working in Sicily she was informed by police that they had a suspect. She became aware that Mr Murdoch was arrested and a suspect in a unrelated rape of a child and mother. She was also informed by a friend that there was an article on the internet that portrayed her in a positive fashion. She claimed that she went on the internet to look at the article only to see what it said about her and she did not expect to see a photo of Mr Murdoch. When Mr Murdoch's photo did appear on the page, she identified him as the offender in her matter. The article also mentioned that his DNA was found at the scene of Falconio's murder.

Unfortunately, no evidence was elicited at trial or appeal about the written contents of the document, whether she read them, whether they came up first before the image, the formatting of the page at the time that she viewed it. Whilst noting the relevant authorities on the dangers of identification evidence, the trial judge found that the identification was *spontaneous*[40] and admitted the evidence. The Court of Criminal Appeal did not disturb that finding.

In *R v Kearney* [2013] SASC 121 the prosecution alleged that Mr Sanderson punched the complainant, Mr Robertson, in the head and the defendant joined in the assault. Ms Harrison was also assaulted. Ms Harris, a friend of Ms Harrison's, viewed a Facebook photo of another friend Sarah and the defendant. When Mr Harrison viewed this photo she recognised the defendant as the second assailant. She sent the photo via MMS to Mr Robertson with the text "I've found him". Mr Robertson allegedly recognised the offender before reading the text. The photo was forwarded to the police but the police did not make any notes or take any statement about how the two victims had made the Facebook identification. The police conducted photo identification parades with both victims who picked out the defendant. It was argued that the evidence of the Facebook identification should be excluded because of the risk of unfair prejudice, since the witnesses were

[40] Similar to *R v Williams* [1983] 2 VR 579

presented with the single photograph in suggestive circumstances. It was further argued that the photo identification parades should also be excluded because of the risk of displacement.

Blue J referred to the distinction between identification in the pre-detection phase and identification in the post-detection phase:

> In general terms, where the police have arrested or charged a person, it is improper and unfair for the police to use photographic identification rather than a line up unless the person concerned refuses to participate in a line up. On the other hand, in the pre-detection phase, the public interest in the detection of persons who have committed a criminal offence tends towards the non exclusion of the evidence (at 26).

The court considered cases such as *Alexander v The Queen* [1981] HCA17; (1980) 145 CLR 395 and *Festa v The Queen [2001] 208 CLR 593,* and *R v Deering* (1986) 43 SASR 252. It compared the present case with the circumstances in *R v Murdoch* and found that there was spontaneous identification in the pre-detection phase and the failings of the police to not make notes did not have a significant effect on the victims' evidence. With regards to the argument that the photo identification parades were contaminated by the earlier identification, the court found that the Facebook photo was significantly different to the photo board photo and that, with appropriate directions, the jury could properly assess and appreciate the risk of contamination.

In *R v Jannissen* [2013] QCA 279 three offenders committed an armed home iinvasion of the two victims. The victims knew one of the offenders as Rosco. One of the victim's visited Rosco's Facebook page to look for the appellant's photo. She stated that she could not see the Facebook photo properly. She subsequently performed a photo identification parade. Noting that she had not seen the Facebook photo properly, the court held that there was less risk of error associated with displacement and the judge could properly address the risk via jury directions.

Strauss v Police [2013] SASC 3

On the other hand, identification evidence was soundly rejected in *Strauss v Police* [2013] SASC 3, where Peek J gave an in depth analysis of identification evidence in the age of Facebook[41]. He was also critical of police failures.

In that case, the victim, Mr Hurley, was assaulted by two men. It was alleged that one of the offenders said to him "I heard you said something about my girlfriend". It is alleged that Mr Hurley had earlier insulted Mr Daley's girlfriend. Mr Hurley and a witness, Ms Wright, made identifications of the appellant by accessing photographs of the appellant on Facebook. Ms Wright, in collusion with another witness, made the initial identification via looking at Mr Daley's Facebook page. They went to Mr Daly's page because of the girlfriend comment. On that page, the appellant was tagged in a photograph with his name. One of the witnesses then informed Mr Hurley that the person who was involved in this incident was Brenton Strauss, which caused him to look Strauss up on Facebook.

[41] See "Part 2" of his judgment commencing at 12.

The prosecution did not provide a copy of the Facebook photo where Strauss was identified. The prosecution argued that the appellant could have referred to images from his own Facebook profile. However, Peek J, noted (at footnote 65):

> "a defendant to a criminal charge cannot be compelled to produce such documents. In any event, a defendant is entitled to know precisely *which* image had been used and reference to "a photograph" on his Facebook page is far too vague. If there are various images on the appellant's Facebook (and of course they may be changed frequently) there will very likely be later disputes as to precisely which image had been involved. This problem is magnified by the tagging process which allows other Facebook users to upload and subsequently remove images of the appellant"

Peek J also noted the police investigation was attended by several failures, including failure to:

- take a full description of the offenders from the victim or from any of witnesses at the scene of the crime. Peek J said (at 47) "the taking of a full description of the offenders at the earliest possible time in an investigation in any case where there may be a question as to the identity of the assailants is absolutely critical, and even more so in the current era of social media. Such a description forms the benchmark against which subsequent evidence of identification evidence must be measured and checked and should also form the basis of a selection of a group of appropriate persons or photographs in an identification parade…"
- take statements from relevant witnesses.
- conduct formal photo identification procedures with Mr Hurley or Ms Wright at any stage (instead choosing to rely only on the Facebook identifications). Peek J referred to *R v Britten*(1988) SASR 567 where King CJ stated "there seems to be a tendency on the part of police officers to suppose that, because judgements of courts have pointed out that the value of identification by means of a line up is impaired by prior identification from photographs, there ought not to be an identification parade following identification by means of photographs. *An identification parade would give an honest and careful identifying witness an opportunity to correct a mistake in the identification from photographs*.." Failure to provide an identification parade denies the accused an opportunity for a formal identification procedure where any prior mistake may be corrected.
- ignoring a independent witness (who was not involved in the discussions that the other witnesses had after the offence), gave a description that the offender had long hair and did not pick the appellant in a photo identification parade (the appellant had short hair).
- Not investigating Mr Daley at all.

Peek J noted the following problems with Facebook:

- It leads to a substantial increase in the risk of contamination of evidence (at 31-33)
- It has spawned a new generation of private investigators, allowing users to search profiles ("Facebook stalking") (at 34).

> "The process has very great problems in relation to the potential contamination of evidence necessary for a conviction in a court of law. Such problems are likely to arise when a victim of a crime, or a witness to it, searches Facebook looking for the offender using what information they have, *or think they have,* about the offender.

Considering the case of *McCullough [2011] EWCA Crim 1413*, Peek J noted that it has been argued that Facebook identification is no different to a street identification. However, Peek J said there are considerable differences. With many social networking site identifications a witness will be directed to search for a particular individual…there is clearly a danger of predetermination with SNS identifications[42].

Peek J also considered the decision of *R v Murdoch* and noted that the feature that the exposure of the image of Mr Murdoch to the focus of the witness was "s*udden, unexpected and incidental*" was crucial to the decision. In the present case, Peek J found that the identification by the witnesses was far from being sudden, unexpected and incidental but was "*studied, expected and direct*" (at 115).

Peek J found, inter alia, that the magistrate had erred by failing to exercise her discretion to exclude the identification evidence. The appeal was allowed and the conviction quashed.

Dia v Regina [2014] NSWCCA 9

The NSW Court of Criminal Appeal took a different view in the recent case of *Dia v Regina* [2014] NSWCCA 9. In that case the appellant and co-accused Mr Fawaz were charged with a home invasion. The witness Ms McCann recognised Fawaz from prior associations. On the night of the offence, police interviewed McCann and asked if she was a member of Facebook. Using the detective's mobile they searched Fawaz's profile and downloaded a photo of a group of Middle Eastern people outside Bankstown Railway Station. The following day, McCann went back onto Fawaz's Facebook and went through his photos to see if she could identify any of the other faces from the offence. She came across the appellant's profile and recognised a photo of him on that profile as an offender.

The appellant did not dispute that it was his Facebook page (under the name of Ali Khawaja) but he also claimed that he was depicted in the Bankstown Railway Station photo. Moreover, that photo had been altered because it had originally been taken at Paul Keating Park and the background was changed. He argued against the admission of Ms McCann's identification because of her expectation of identifying an offender when she searched for his photo and because of the displacement effect, having seen his image already from the Bankstown Railway Station photo.

Hoeben J (Schmidt J and Barr AJ agreeing) downplayed the displacement effect, noting that McCann had not been looking at the Bankstown photo to identify other offenders but to confirm the identification of Fawaz and that photo had been downloaded from the detective's mobile and was grainy. In relation to her expectation of making an identification of an offender, the court said (at 67-68):

[42] Peek J referenced O'Floinn and Omerod, 'Social networking material as criminal evidence' [2012] *Criminal Law Review* 486, at 500.

> There are obvious dangers associated with any identification from a photograph and there were some particular dangers associated with this mode of identification. These matters were not only put to Ms McCann in cross-examination but clear warnings as to the reliability of the identification were given by his Honour to the jury.
>
> While there are dangers in such a process of identification, it is also a method which is acceptable and evidence concerning such identification is admissible. The process of identification undertaken by Ms McCann was analogous with her attending a police station and examining a photographic array or going to a police station to view a line-up.

With respect, I disagree that such a Facebook identification is "analogous with her attending a police station and examining a photographic array..or line up". On Facebook, none of the safeguards of such formal identification procedures are in place.

In any event, the court found that all of the dangers associated with the identification had been raised in cross examination and in jury directions. The appeal against conviction was dismissed.

Recent United Kingdom criminal cases on social media identification

Recent English cases include *R v Alexander and McGill* [2013] 1 Cr App R 26. The victim of a robbery looked at the Facebook profiles of two of his sister's friends who lived in the area where the robbery occurred. He identified the two men as his assailants. The police viewed the Facebook pictures with the victim and his sister but did not make any record of what had happened. Subsequently, the victim identified the defendants in an identification parade. Prior to trial, the defendants requested disclosure of the Facebook pages but this request was not met. The Court of Criminal Appeal held that the evidence of identification was properly admitted and it was perfectly possible for the jury, properly directed, to consider the considerable disadvantage at which the defendants had been put and the reliability of the identification in those circumstances.

Nevertheless, the court said (at 38) 'if, as is to be anticipated, future identifications occur by looking through Facebook, it is incumbent upon the police and the prosecutor to take steps to obtain, in as much details as possible, evidence in relation to the initial identification – for example, it would be prudent to obtain the available images that were looked at and a statement in relation that happened"

See also *H* [2009] EWCA Crim 1453 and *Jenkins* [2011] HCJAC 86 where A initially identified SPJ, having seen a photo of him on Bebo, but subsequently claimed this identification was flawed and that the true perpetrator was JJ.

Incidentally, if you do have a client who has been wrongly identified via social media, it may be interesting to read the Irish case of *McKeogh v John Doe 1 & Ors* [2012] IEHC 95. In that case of zemblanity, the plaintiff was wrongly identified as someone who had done a runner on a taxi (he was in fact in Japan at the time), the taxi driver having posted a video of the offender on YouTube. The plaintiff was subsequently defamed in various social media and print media and successfully applied

to the court for injunctions and also for orders for social media sites to provide him the names of web users who had defamed him.

ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

The only NSW decision I could find about the admissibility of social media evidence was *Petroulias v R* [2010] NSWCCA 95. That decision did not turn on the admissibility of the evidence – it was merely one possible ground of appeal that was considered by the NSW Court of Criminal Appeal. The applicant sought to argue a miscarriage of justice and referred to internet messages which were alleged to have been between jurors. The senders of the messages did not disclose their identities but used nicknames. Barr AJ (Rothman and Hodgson JJ agreeing) stated (at 51-53):

> "It seems to me that the applicant would have enormous difficulties in relying on this material in the appeal.
>
> First, the authors of these messages unidentified. No court would , in my view, infer without substantially more evidence than this that the authors or any of them were members of this jury. There is a fundamental problem of provenance, and therefore of relevance. Even if that problem could be overcome, the material relied on would be inadmissible as hearsay. Thirdly, the material would be inadmissible as breaching the confidence of the jury room…
>
> In my opinion no ground of appeal based upon this material would have a strong prospect of success"

The above statement raises some of the main concerns regarding the admissibility of social media evidence, namely:

- Relevance: authenticity; and
- Hearsay

Relevance: Authenticity

How does the party seeking to adduce social media evidence prove that it is authentic –eg that the printout is of the actual Facebook page, that the page is really your client's page, that your client was the one who posted the admission on the page?

One of the most common complaints against social media evidence is that the posting could have been made by an imposter. As discussed above, unlike with a mobile phone where there is usually some form of identification verification during subscription, almost anyone can create a Facebook profile without much validation. There have been cases where children have taken photos of teachers using their mobile phone and then created Facebook profiles for the teachers and produced inappropriate content. However, if you already have an existing Facebook profile, it may be more difficult for an imposter to create another profile for you.

Even if the posting is from your genuine Facebook page it may have been the result of unauthorised access to your page. Of course, a user requires your username and password before they can access your page. However, asides from hacking, there are other ways that your username and password may be compromised. For example, some computers will autofill your username and password

when you login so if someone else uses that computer they will have access to your page. Alternatively, someone could simply use your profile whilst you are still logged on.

Fillipetti

Where the prosecution seek to rely on mobile phone evidence (eg text messages from your client's phone) a *Fillipetti* argument could be raised that the prosecution need to establish that the mobile was within the exclusive possession of your client. The prosecution case is, of course, stronger if they have evidence that the phone is password/PIN protected. Nevertheless, as discussed above, there are still ways that others can access a mobile phone that is password/PIN protected.

The same *Fillipetti* argument could be raised for postings from or on your client's Facebook profile (assuming that there is no issue that it is your client's profile). However, unlike mobile phones, someone can access the profile from anywhere but the profile is always password protected. Thus, I expect that the prosecution would start with the presumption that your client had exclusive possession of the profile and would only need to rebut this if there was something to indicate that the security of the profile had been compromised.

Evidence Act, ss 57, 58

Sections 57 and 58 deal with relevance and authentication.

> *57 Provisional relevance*
>
> (1) If the determination of the question whether evidence adduced by a party is relevant depends on the court making another finding (including a finding that the evidence is what the party claims it to be), the court may find that the evidence is relevant:
>
> (a) if it is reasonably open to make that finding, or
>
> (b) subject to further evidence being admitted at a later stage of the proceeding that will make it reasonably open to make that finding.
>
> (2) Without limiting subsection (1), if the relevance of evidence of an act done by a person depends on the court making a finding that the person and one or more other persons had, or were acting in furtherance of, a common purpose (whether to effect an unlawful conspiracy or otherwise), the court may use the evidence itself in determining whether the common purpose existed.

> *58 Inferences as to relevance*
>
> (1) If a question arises as to the relevance of a document or thing, the court may examine it and may draw any reasonable inference from it, including an inference as to its authenticity or identity.
>
> (2) Subsection (1) does not limit the matters from which inferences may properly be drawn.

Incidentally, see also s 183:

> 183 Inferences
>
> If a question arises about the application of a provision of this Act in relation to a document or thing, the court may:

(a) examine the document or thing, and
(b) draw any reasonable inferences from it as well as from other matters from which inferences may properly be drawn.

Note: Section 182 of the Commonwealth Act gives section 183 of the Commonwealth Act a wider application in relation to Commonwealth records and certain Commonwealth documents.

In *National Australia Bank Ltd v Rusu* (1999) 47 NSWLR 309 Bryson J considered ss 57 and 58 and considered that authenticity should be distinguished from relevance.

He said (at 19):

> In the language used in s 57(1), a finding that the evidence is what the party claims it to be is distinguished from the question whether the evidence is relevant; authenticity is something on which relevance depends....
>
> A question of authenticity is not a question as to the relevance of documents within s 58(1), which treats authenticity as part of the material on which relevance may be determined.

And (at 17):

> 17 Before a business record or any other document is admitted in evidence it is obviously necessary that there should be an evidentiary basis for finding that it is what it purports to be. Documents are not ordinarily taken to prove themselves or accepted as what they purport to be; there are exceptions under the Common Law and under statutes for public registers and for many kinds of documents when certified in various ways: and see the method of proof provided in some cases by ss 170 and 171 of the Evidence Act 1995. At the simplest, the authenticity of a document may be proved by the evidence of the person who made it or one of the persons who made it, or a person who was present when it was made, or in the case of a business record, a person who participates in the conduct of the business and compiled the document, or found it among the business's records, or can recognise it as one of the records of the business.

Odgers suggests that it is unclear whether Bryson J took the view that s 57 did not apply to the question of authentication and that the court could not draw reasonable inferences from a document as to its authenticity. If so, Odgers argues that this interpretation is at odds with the intention of the provisions:

> It was the clear intention behind this provision that a finding as to authentication (on which relevance depends) need not be obtained before the evidence is found to be relevant and admissible, so long as it is "reasonably open" to find that the document is authentic (s 57(1)(a)) or an undertaking is given that further evidence will be adduced "at a later stage of the proceeding that will make it reasonably open to make" the finding that the document is authentic: s 57(1)(b). That approach was followed by Carr J in *Cordelia Holdings pty Ltd v Newkey Investment Pty Ltd* [2002] FCA 1018 at 52-54[43].

[43] Odgers, Stephen, *Uniform Evidence Act 10th edition*, Thomson Reuters, 2012, p 241

Odgers suggests that what was plainly intended by the legislature was that, for the purposes of determining the admissibility (s 56) of a document, a question of prima facie authenticity[44] may be decided with the assistance of reasonable inferences from the document itself[45].

Bryson J's approach was also doubted by Madgwick J in *Lee v Minister for Immigration & Multicultural & Indigenous Affairs* [2002] FACFC 305 at [25][46], and *O'Meara v Dominican Fathers* [2003] ACTCA 24 at 85 per Gyles and Weinberg JJ.

In *Australian Securities &Investments Commission v Rich* (2005) 216 ALR 320, Austin J (at [117]) concluded that Bryson J did not deny that inferences may be drawn from the document itself, relevant to the question of authenticity, but that "authenticity cannot be achieved *solely* by drawing inferences from the face of the document where there is no other evidence to indicate provenance" (my emphasis).

In *Acqua- Marine Marketing Pty Ltd v Pacific Reef Fisheries (Australia Pty Ltd(No 4)* [2011] FCA 578, Collier J noted the following principles (at 14) after the judgment of Austin J in *Australian Securities and Investment Commission v Rich* [2005] NSWSC 417:

- It is important not to set the bar too high for the authentication of documents, because if too much is demanded, the authentication requirement will fight against the policy underlying the business records provisions[47]. That policy recognises that any significant organisation depends for its efficiency upon the keeping of proper records, to be used and relied upon in the everyday carrying on of the activities of the business and therefore likely to be accurate, and likely to be a far more reliable source of truth than memory (*Rich* at 116)
- The party tendering the document must establish authenticity, which cannot be achieved soley by drawing inferences from the face of the document where there is no other evidence to indicate provenance (*Rich* at 117)
- Authentication is about showing that the document is what it is claimed to be, not about assessing, at the point of the adducing of the evidence, whether the document proves what the tendering party claims it proves (*Rich* at 118)[48].
- There is a distinction between matters of authenticity going to the adducing of evidence and matters going to the credibility and weight of document evidence once it has been authenticated and judged admissible (*Rich* at 118)

See also *Australian Competition and Consumer Commission v Allphones Retail Pty Ltd* 2011) 280 ALR 97 at 76-81 per Nicholas J.

<u>Requests for evidence of authenticity</u>

[44] Under s 57(1) it is only necessary that it be reasonably open to find that the document is what the party adducing it claims it to be.
[45] Odgers , S, *op cit. , p 243.*
[46] See also *Cordelia Holdings Pty LTd v Newkey Investment Pty Ltd* [2002] FCA 1018 at [52]-[53] per Carr J
[47] For a discussion about business records, see beow.
[48] See also *New South Wales Crime Commission v Trinh* [2003] NSWSC 811.

If there is a doubt that is raised about authenticity a request could be made for further evidence establishing authenticity: ss 166-169.

166 Definition of request

(1) In this Division:

"request" means a request that a party ("the requesting party ") makes to another party to do one or more of the following:

(c) to produce to the requesting party the whole or a part of a specified document or thing,
(d) to permit the requesting party, adequately and in an appropriate way, to examine, test or copy the whole or a part of a specified document or thing,
(e) to call as a witness a specified person believed to be concerned in the production or maintenance of a specified document or thing,
(f) to call as a witness a specified person in whose possession or under whose control a specified document or thing is believed to be or to have been at any time,
(g) in relation to a document of the kind referred to in paragraph (b) or (c) of the definition of
"document" in the Dictionary-to permit the requesting party, adequately and in an appropriate way, to examine and test the document and the way in which it was produced and has been kept,
(h) in relation to evidence of a previous representation-to call as a witness the person who made the previous representation,
(i) in relation to evidence that a person has been convicted of an offence, being evidence to which section 92 (2) applies-to call as a witness a person who gave evidence in the proceeding in which the person was so convicted.

Failure to comply with the request may affect admissibility.

Defence lawyers may need to make tactical decisions about whether and when to make such a request, taking into account that making a request may notify the police that they need to obtain further evidence to establish authenticity, thereby possibly strengthening their case.

Computer produced evidence

In relation to computer produced evidence, the evidence will be relevant if it is reasonably open to find that the computer system does what is claimed for it (or subject to further evidence being admitted at a later stage of the proceedings that will make it reasonably open to make that finding). Sections 146 could be utilised[49]; it provides a presumption in relation to the correct operation of equipment.

s 146 Evidence produced by processes, machines and other devices

(1) This section applies to a document or thing:

[49] And where appropriate s 147.

(a) that is produced wholly or partly by a device or process, and
(b) that is tendered by a party who asserts that, in producing the document or thing, the device or process has produced a particular outcome.

(2) If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document or thing on the occasion in question, the device or process produced that outcome.

Example:
It would not be necessary to call evidence to prove that a photocopier normally produced complete copies of documents and that it was working properly when it was used to photocopy a particular document.

147 Documents produced by processes, machines and other devices in the course of business

(1) This section applies to a document:
(a) that is produced wholly or partly by a device or process, and
(b) that is tendered by a party who asserts that, in producing the document, the device or process has produced a particular outcome.

(2) If:
(a) the document is, or was at the time it was produced, part of the records of, or kept for the purposes of, a business (whether or not the business is still in existence), and
(b) the device or process is or was at that time used for the purposes of the business,

it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document on the occasion in question, the device or process produced that outcome.

(3) Subsection (2) does not apply to the contents of a document that was produced:
(a) for the purpose of conducting, or for or in contemplation of or in connection with, an Australian or overseas proceeding, or
(b) in connection with an investigation relating or leading to a criminal proceeding.

Note: Section 182 of the Commonwealth Act gives section 147 of the Commonwealth Act a wider application in relation to Commonwealth records and certain Commonwealth documents.

<u>Some recent Australian criminal cases about authenticity/provenance</u>

In *Police v Flavel* [2013] SASC 166 the respondent was charged with exceeding the speed limit according to a photo taken by a speed camera. The magistrate excluded the photo, on the basis that the prosecution had failed to prove the provenance of the photo, and accordingly dismissed the charge on the basis that there was no evidence of the commission of the offence. On appeal, David J held that the magistrate had erred in refusing to allow the tender of the photo. The notations on the

photo, combined with a tendered "Certificate of Operation and Testing of Approved Photographic Detection Device", provided a clear inference that the photograph related to the particular speed camera whose details were contained in the certificate.

In *Police v M, M [2012] SASC 83,* the respondent was charged with performing a grossly indecent act in a public place. The incident was captured on CCTV which the CCTV operator, Mr Anderson, showed and handed over to police. The prosecution was put on notice by the defence that they would object to the tender of the CCTV without proper proof of its provenance and authenticity. White J discussed the need to establish the provenance of video tape footage. He noted (at 22):

> it was not necessary for the High Court in *Butura v DPP (Vic)* [1987] HCA 58; (1987) 164 CLR 180 to consider the conditions of admissibility of an audio tape but Mason CJ, Brennan and Deane J did observe (at 184):
>
> > It is obvious that the provenance of the tape recording must be satisfactorily established before it is played to the jury
>
> This seems to imply that the Court must be satisfied of the provenance of an audio or video tape before it admits the tape into evidence.

At 26:

> 26. The word "provenance" is usually understood as a reference to the source or origin of an object. However, in the present context, the word has a slightly different connotation, involving notions of authenticity, accuracy and integrity. They are the matters with which a court considering the reception of a video tape will ordinarily be concerned. Proof of the source or origin of the video tape may be an important aspect of the proof of those matters. Thus in *Butera*, Mason CJ, Brennan and Deane JJ spoke of the proof of a conversation "by tendering the tape recording and, one assumes, proving the circumstances in which the recording had been made and the custody in which the recording had been kept until it was played to the court at the trial".

at 28:

> In the case of video tape, there is no reason in principle why a court may not be able to determine its admissibility in part by the inferences which can be drawn from the tape itself as to its authenticity, accuracy and integrity. Much will depend on the circumstances, including evidence as to the source of the tape and any acknowledgements made by the defendant. In most cases, a viewing of the video tape will be a natural place to commence a consideration of whether a video tape shows signs of tampering or discontinuities which may raise questions about its authenticity, accuracy and integrity.

And at 35:

> As already indicated, there is no inflexible rule to the effect that the manner of taking of CCTV footage must always be proved before that footage becomes admissible. Nor is there an inflexible rule that any possibility of tampering with a film be excluded before it can be

admitted. Account must be taken of the particular circumstances of each case. In this case, those circumstances included the features to which I have just referred, and in particular the respondent's acknowledgement that she was shown in the film on the Festival Plaza in a "disgusting" act. That being so, the absence of evidence from the Skycity Casino as to the means by which the CCTV footage was taken, and of the circumstances in which it was held during the 24 hours or so before the police took their copy was not decisive. The absence of evidence about those matters was something which the Magistrate had to consider in relation to issues of authenticity, accuracy and integrity but could not reasonably be regarded as decisive of them.

In *R v J, SM [2013] SASCFC*, the provenance of a Facebook photo was questioned. Unfortunately, the case does not deal directly on point with determining how much evidence is necessary to prove authenticity/provenance.

The defendant was convicted of sexual offences against his daughter S. The complainant's brother, A, gave evidence of complaint. The trial judge disallowed a question during cross examination of "A" about whether he believed the complainant should be believed on her testimony. The judge also ruled that the defendant's counsel could not cross examine "A" about his alleged Facebook entry that contained an adverse comment about the complainant's credibility, for example: "uv lied all ur 21 years of ur life I do not no who to believe anymore so I'm going to say no more".

The prosecutor contended that the provenance of the three Facebook pages had not been established and she sought an assurance from the defendant's counsel that he was in a position to prove the provenance of the three pages. Counsel responded that he did not know the provenance beyond having received the three pages from the defendant's mother and beyond the inferences which could be drawn from their appearance. He had not made any further enquiries.

The case dealt with the oath –belief rule, the common law rule that allows questioning of witnesses about whether they believe another witness has kept their oath. The Court of Criminal Appeal (Kourakis CJ, White and Blue JJ) held that the defence should have been allowed to cross examine about oath belief. As to the second ground of appeal (about the ability to cross examine with the Facebook pages) the court held (at 111-114):

> 111. The defendant contends that his counsel was entitled to put the Facebook document to witness A pursuant to section 29 of the Evidence Act[50].
> 112. The reason given by the Judge for upholding the prosecutor's objection was that the defendant had not proved the provenance of the document which his counsel sought to put to the witness. The Judge erred in upholding the objection on that particular ground. The issue of proof of the provenance of the document would not arise until a later stage at which the defendant sought to tender the document, depending upon the answers received to the questions asked of A.
> 113. However, the defendant relies upon and asserts the continuing existence of the oath-belief rule set out at [29] above as the justification for the line of questioning involving the Facebook document and for putting the Facebook document before the witness A. The oath-belief rule itself precludes A being asked about the particular facts, circumstances or

[50] Section 29 relates to cross examination as to previous statements in writing

incidents which might have formed the basis of an opinion by A that he would not believe S on her oath.

114. The avowed purpose of counsel for the defendant in seeking to put the Facebook document before A was to elicit, if possible, evidence from A that S had told lies over the course of her 21 years of life. Such questions are expressly precluded by the third limb of the oath-belief rule as advanced by the defendant himself. The defendant could not achieve via the back door of putting to A a document what he could not achieve directly by asking questions about the conduct of S which was relevant only to credibility.

115. The second ground of appeal should be rejected.

Some recent United Kingdom criminal cases about authenticity/provenance

T v The Crown [2012] EWCA Crim 2358 involved an allegation that the appellant had sexually assaulted the complainant. The appellant sought to tender a photograph of the complainant that was allegedly sent via email to him around Valentines Day, showing the complainant dressed in a bikini or underwear. He also sought to tender Facebook messages by the complaint to the defendant (with no response). The prosecution successfully objected to both tenders and the court of appeal upheld the trial judge's decision, stating (at 12-13):

> The prosecution were sceptical and rightly sceptical as to the provenance of the photograph which could so easily have been obtained by means other than a direct email posting to the defendant, in the absence of any evidence as to the email which accompanied it. There was no explanation given as to why it was adduced so late…
>
> This ambush by the defence led, as so often it tends to do, to error. That is part of the danger which arises from an unjustifiable breach of the rules of advance disclosure. It was incumbent upon the defence to give advance notice of the Facebook photograph and the Facebook entries so as to give the prosecution sufficient time to consider whether it wanted to obtain evidence as to the different means by which a photograph might have reached the defendant and the question whether it was credible that the Facebook entries, typical as they were of exchanges between teenagers were so one sided.

As discussed above, defence practitioners may need to consider whether they make a s 166 about authenticity when police serve social media evidence in a brief. On the other hand, if defence seek to rely on social media evidence, this case of *T v The Crown* suggests that they may need to notify the prosecution earlier so that the prosecution have time to test authenticity. I note, however, that the UK does have different rules about advance notice.

In *R v Quinn* [2010] NICC 27 the defendant was charged with managing a meeting in support of a prescribed (terrorist) organisation, being the Continuity IRA. The prosecution sought to rely on a DVD compiled by the police, including downloaded YouTube footage. The defendant did an interview where alleged admissions about the footage were made. The trial judge excluded the footage saying:

> Material could only be admitted if prima facie authentic. That requires more than the mere production of a piece of film. It requires that the provenance of the film is established by the prosecution, by evidence, in a way that permits the defence to investigate and examine the

> provenance and reliability of the material. This process further requires the prosecution to establish that the material is reliable in the sense that it has not been manipulated or altered. The evidence before me does not include any evidence as to the provenance of the material other than that it was posted on the "You Tube" site. The mere posting of such material on such a site does not invest it with any authenticity, rather the evidence that I have heard concerning the way in which this can be done raises very real concerns that material on this site can be altered and manipulated easily and freely and that the defence would have little if any opportunity of investigating and determining the authenticity and reliability of such films. …
>
> I am not satisfied that the Crown have established the authenticity of this film. I can see a great many ways in which this material could have been manipulated and to that extent I am not prepared to admit the film in evidence in this trial.

The court of appeal in Rv Quinn [2011] NICA 19 further stated (at 11):

> There is no evidence of continuity from the point at which each film was made to it being downloaded from YouTube by Sergeant Bleakley. It appears that the material was uploaded on to YouTube by a person who has previously uploaded similar propaganda material on 22 occasions but it appears that no investigation or enquiry has been made to determine his or her true identity. It is accepted that once downloaded, digital material can be altered, edited and changed in many respects and can thereafter be uploaded once more in its new altered form. There is no way of knowing whether it has been manipulated or altered unless one has the original unedited material with which to compare it. In the absence of a valid comparative standard the learned trial judge considered that the test for admissibility was not met. He held that the provenance of the film had to be established by the prosecution by evidence in a way that permitted the defence to investigate and examine that provenance and the reliability of the material. In the absence of such evidence the video was not prima facie admissible. Although he was referred to the interviews the learned trial judge noted that at no time in the course of the interviews did the defendant expressly acknowledge or accept that he was the person shown in the videos.

However, the inferences could be drawn from statements that the defendant's solicitor made during the interview which might amount to an admission. The court of appeal said (at 15) "authenticity like most facts may be proved circumstantially and it seems to use to follow that authenticity can also be established by admission".

See also *R v Murphy and Another* [1990] NI 306.

United States cases

In the United States, generally, evidence can be categorized into evidence that self authenticates and evidence that requires authentication before it may be admitted[51]. On occasion, electronic evidence has been determined to be self authenticating like the printouts of postings on the United States Census Bureau's website. However, as a general rule, electronic evidence, such as information from social networking sites, will not be of the type that will be self authenticating. It will usually be

[51] Fleming, M and Wells, J, "Ethical, Evidentiary and Constitutional Concerns of Utilizing Social Networking Web Sites in Civil and Criminal Cases: The Good, the Bad and the Ugly", *Southern Law Journal* Fall 2010, Vol 20, p 37.

necessary for the proponent attempting to offer this evidence to establish its authenticity from extrinsic evidence[52]. There are divergent US decisions about authentication.

The earlier American decisions did not admit social media evidence because it could not be authenticated. One key decision that voiced complete opposition to such evidence was *St Clair v Johnny's Oyster and Shrimp Inc*[53]. In that case, the court stated:

> While some look to the internet as an innovative vehicle for communication, the court continues to warily and wearily view it largely as one large catalyst for rumour, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the internet is inherently untrustworthy. Anyone can put anything on the Internet. No website is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any website from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules...

This was followed by *Tolliver v Federal Republic of Nigeria*[54] and *United States v Jackson*[55], where the court refused to admit insufficiently authenticated web postings attributed to white supremacist groups.

However, either as a sign of changing times or a reflection of differing opinions in different States, courts in California took a different view. *Johnny's* case and *Jackson* were distinguished and evidence admitted in *Florida Conference Association of Seventh day Adventists v Kyriakides*[56]. Other States followed suit and found various ways of authentication.

Authentication may occur by a witness with personal knowledge of the material. In *St Luke's Cataract's Laser Institute v Sanderson*, the court stated "to authenticate printouts from a website, the party proffering the evidence must produce some statement or affidavit from someone with knowledge of the website...for example a web master or someone else with personal knowledge would be sufficient" [57]. Likewise, in *United States v Safavian*[58], an email could be authenticated by a witness with knowledge that the email is what it is claimed to be.

---

[52] Fleming and Wells, *op cit*, p 37, although I note that Facebook thinks that its business records are self authenticating. Its help centre states the following:

> Do I need a Facebook representative to testify at a civil trial?
>
> No. the account owner, or any person with knowledge of the contents of the account can authenticate account content. Further, under Federal and California law, business records produced by Facebook are self authenticating.

[53] 76 F.Supp.2d 773 (S.D.Tex.2000); Perfect 10, Inc., 213 F.Supp.2d at 1146 at 774-75
[54] 265 F.Supp 2d 873 (W.D.Mich. 2003)
[55] 208 F.3d 633 (7th Cir.2000)
[56] 151 F.Supp.2d 1223 (C.D.Cal.2001)
[57] No 8:06-cv-223-T-NSS, 2006 U.S.Dist.LEXIS (M.D.Fla.2006) at *5
[58] 435 F.Supp.2d at 40 n.2 (D.D.C. 2006).

In *Johnson-Woolridge v Woolridge*[59] authenticity could be established by the testimony of any witness that typed in the URL associated with the web site that he or she logged onto the site and reviewed what was there and that a printout accurately reflected what the witness saw. In this respect the witness authenticating the printout was no different from a crime scene officer authenticating a photograph of a crime scene they witnessed.

Some emails may be authenticated by distinctive characteristics. In *United States v Sidiqui*[60] the court allowed the authentication of an email entirely by circumstantial evidence, including the fact that the email bore the defendant's work email address, the contents of the email involved specific topics very familiar to the defendant, the email used the defendant's nickname and there was witness testimony that the defendant spoke to these witnesses shortly after they received the email about the subjects contained in the email.

Some other cases dealing with the authentication of emails include:

- *Commonwealth v Jermey M Amaral* (Mass.Ct.App.2011): by the defendant's picture, phone number and appearance at designated meeting spots to meet with an undercover officer posing as a 15 years old girl
- *Purdy v Massachusetts* (Mass.2011): the account name resembled the defendant's name, the emails originated from an account that the defendant's friends knew he used and the emails were later discovered by police on a a hard drive belonging to the defendant

Some cases dealing with the authentication of text messages include:

- *In re FP.*878 A.2d91, 93-95 (Pa.Super.Ct.2005): instant messages were authenticated through the use of screen names and the context of the messages and surrounding circumstances.
- *Dickens v State* 175 Md.App.231, 927 A.2d 32, 36-38 (2007): threatening text message received by the victim on her cell phone were properly authenticated when circumstantial evidence provided adequate proof that the message sent by the defendant

In relation to material from social media websites, some American legal journals opine that it is reasonable to presume that material on a website (other than chat room conversations) was placed there by the owner of the website[61]. The fact that Facebook sites are password protected would allow a reasonable jury to conclude that posts made on someone's page are authored by that person: *California v Archuletta* (Cal. Ct. App.april 9, 2013). The appearance, contents, substance, internal patterns or other distinctive characteristics of Facebook evidence may also combine to be sufficient to authenticate a piece of evidence. In *United States v Grant* (A.F.Ct.Crim.App.2011),

[59] 2001 Ohio App.LEXIS 3319 at *11 (Ohio App.July 26, 2001)
[60] 235 F.3D 1318, 1322-23 (11th Cir.2000)
[61] Joseph, G, "internet and Email Evidence" *The Practical Litigator*, March 2002; 13, 2; ProQuest Research Library, p 46.

authentication occurred through Grant's name and picture accompanying each message, he communicated with the complainant immediately before meeting in person, he provided via Facebook his phone number and flight information and made plans with the complainant via Facebook. In *Campbell v Texas* (Tex.Ct.App.2012) the court noted authentication via the defendant's speech pattern (the defendant spoke with a Jamaica dialect), the communications referenced the underlying nature of the defendants charge known only to a few people and only he had access to his Facebook account and his electronic signature.

Nevertheless, in *Connecticut v Eleck* (Conn.App.2011) even though Eleck agreed that a Facebook account was his, the proponent of the Facebook evidence still needed to negate his assertion that his account had been hacked. The mere fact that the defendant held and managed the account did not provide a sufficient foundation for admitting the printout.

Myspace is similar to Facebook. Some cases involving the authentication of Myspace pages include:

- *Burgess v State* (Ga.april 29, 2013), including authentication by the use of the defendant's nickname
- *California v Zamora* (Cal Ct.App. Jan.31, 2013): the defendant confessing to his probation officer that he used and operated the Myspace page
- *Tienda v Texas* (Tex.Crim.App.2012): the numerous pictures of the defendant on the page that displayed his unique tattoos, reference to the victims death and details about the victim's funeral (in a case involving murder), a connection between the Myspace page and an email address resembling Tienda's name, witness testimony about Myspace subscriber records
- *California v McKinney* (Cal.Ct.App. Mar 29,2013)
- *Ohio v Yates* (Ohio Ct.App.2012)
- *California v Valdez* (Cal.Ct.App.2011)
- *Commonwealth v Myers* (Mass.App.Ct.Dec.3.2010)
- Michigan v Goins(Mich.Ct.App.Jan 21, 2010)
- *Griffin v State of Maryland* No 1132 (Md.Ct.Spec.Apps 2010)

Chat rooms are an exception because chat room postings are made by third parties, not the owner of the site. Further, chat room participants usually use screen names (pseudonyms) rather than their real names. The type of evidence necessary to attribute a chat room posting to a particular individual may include, for example, proof that:

- the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question);
- when a meeting with the person using the screen name was arranged, the individual in question showed up;
- the person using the screen name identified him or herself as the individual (in chat room conversations or otherwise), especially if that identification is coupled with particularized information unique to the individual such as a street address or email address
- the individual had in his or her possession information given to the person using the screen name (such as contact information provided by the police in a sting operation); or

- a user of the computer used the screen name in question (this can be established by examining the comptuer's hard drive) [62].

See generally *United States v Tank*[63], *United States v Simpson*[64] and *Jackson v Arkansas*[65] where, in 2009, the court said that even anonymous postings on a social networking site may be authenticated by circumstantial evidence. No webmaster or technology expert need authenticate material presented from web sites in part because "social networking ...site members create and control their own profiles". The appeals court allowed transcripts of a chat room showing a criminal defendant's stalking of a 14 year old online.

Expert evidence to prove authenticity

There are ways of proving who created a Facebook profile, despite the lack of identity validation during registration. One could subpoena Facebook for the IP addresses used to log in to the account, and the "real name" given at the creation of the account. Then, you would have to determined the internet service provider (ISP) who provided the IP address and subpoena the identity of the owner of that particular IP address at that particular time. Assuming you got the email address, you could subpoena the email provider for the subscriber information, eg real name given for the account, IP address used to sign up, log in, etc as well as the contents of emails to help establish the identity of the person who used the email account"[66].

See also the article by John Patzakis, 'Overcoming Potential legal Challenges to the Authentication of Social Media Evidence', X1 Discovery. This article states that metadata and file level hash values associated with electronically stored information can be sufficient circumstantial evidence to establish its authenticity. The article lists metadata fields for individual Facebook posts (such as a photo or status update) that together provide important information to establish authenticity of the tweet, if properly collected and preserved.

Conclusions

The Evidence Act provisions and the Australia, UK and US case law appears to support the proposition that some evidence is necessary to prove authenticity, with some cases claiming this should be more than just the document itself; ie more than just self authentication.

Such evidence could include:

- Witness testimony
- Expert evidence such as evidence about metadata
- Distinctive characteristics of the document

[62] Joseph, G, *supra*, p 48.
[63] 200 F.3d 627, 630-31 (9th Cir.2000)
[64] 152 F.3d at 1249-50 (10th Cir. 1998)
[65] 2009 Ark. App.466 (Ct.Apps.Ark. 2009)
[66] Robert Ellis Smith, "Point, click and admit?" *Privacy Journal*, October 2010, Vol 36, Number 12, p 6.

- Evidence about surrounding circumstances
- Admissions about authenticity

Where there is doubt about authenticity this must be raised to such an extent that the onus falls back on the party adducing the evidence to provide more proof of its authenticity.

See also the following articles:

- Facebook Evidence Disallowed by Court due to lack of "identifying characteristics", October 3, 2001 at http://blog.x1discovery.com/2001/10/03
- Scott Milligan, 'Authentication of social media evidence' at www.wassom.com/authentication -of-social-media-evidence-guest-post.html
- Elicia Lin, 'Can your social media page be used in evidence?' on www.rostroncarlyle.com/article/can-your-social-media-page-be-used-in-evidence.
- Legg, Michael; Dopson, Lara, 'Discovery in the Information Age- The Interaction of ESI, Cloud Computing and Social Media with Discovery, Depositions and Privilege' [2012] UNSWLRS 11

Hearsay

Evidence of a Facebook printout is hearsay and thus will not be admissible unless an exception applies: s 59 Evidence Act.

Under the Commonwealth and NSW Evidence Act the following exceptions could apply:

- Business records (s 69)
- Electronic communications (s 71)
- Admissions (s 81)

Business records

69 Exception: business records

(1) This section applies to a document that:
  (a) either:
    (i) is or forms part of the records belonging to or kept by a person, body or organisation in the course of, or for the purposes of, a business, or
    (ii) at any time was or formed part of such a record, and
  (b) contains a previous representation made or recorded in the document in the course of, or for the purposes of, the business.

(2) The hearsay rule does not apply to the document (so far as it contains the representation) if the representation was made:
  (a) by a person who had or might reasonably be supposed to have had personal knowledge of the asserted fact, or
  (b) on the basis of information directly or indirectly supplied by a person who had or might reasonably be supposed to have had personal knowledge of the asserted fact.

(3) Subsection (2) does not apply if the representation:

(a) was prepared or obtained for the purpose of conducting, or for or in contemplation of or in connection with, an Australian or overseas proceeding, or

(b) was made in connection with an investigation relating or leading to a criminal proceeding.

(4) If:

(a) the occurrence of an event of a particular kind is in question, and

(b) in the course of a business, a system has been followed of making and keeping a record of the occurrence of all events of that kind,

the hearsay rule does not apply to evidence that tends to prove that there is no record kept, in accordance with that system, of the occurrence of the event.

(5) For the purposes of this section, a person is taken to have had personal knowledge of a fact if the person's knowledge of the fact was or might reasonably be supposed to have been based on what the person saw, heard or otherwise perceived (other than a previous representation made by a person about the fact).

Note:
1 Sections 48, 49, 50, 146, 147 and 150 (1) are relevant to the mode of proof, and authentication, of business records.
2 Section 182 of the Commonwealth Act gives section 69 of the Commonwealth Act a wider application in relation to Commonwealth records.

It is arguable whether a Facebook entry would constitute a business record of Facebook. In *Waverley Council v Tovir Investments Pty Ltd and Rappaport (No 2)* [2013] NSWLEC, the council charged the respondents with permitting premises to be used as backpackers accommodation. Several websites, including Facebook pages, allegedly promoted the premises via internet marketing. It was argued that evidence from those websites were admissible as business records but the court said (at 5-6)

> The records of a business are the documents (or other means of holidng information) by which activities of the business are recorded. Business activities so recorded will typically include business operations so recorded, internal communications, and communications between the business and third parties.
>
> On the other hand, where it is a function of the business to publish books, newspapers, magazines, journals… such publications are not records of the business. They are products of the business, not a record of its business activities.
>
> The distinction between the records of the business and the products of the business has been applied in other cases…*Roach v Page (No 27)* [2003] NSWSC 1046 at 9-11 per Sperling J. In the latter case it was held that publication on a website of information extolling the virtues of a business is not a record of a business because it is not a recording of business activities in the course of carrying on the business.While there is good reason for the courts to treat records of business activities made in the course of a carrying on a business as reliable and therefore admissible as business records, the same thinking does not extend to advertisements or documents produced for public relations purposes, which should be received with healthy scepticism.

Several of the websites were not business records. It is unknown whether they included the Facebook pages, but in any event, these Facebook pages were allegedly being used in the conduct of the *backpacker* business, not *Facebook* itself.

It is also noteworthy that even if website material may constitute business records of the owner of the site, they are not business records of the Internet service provider (ISP). ISPs are merely conduits and the fact that they are able to retrieve information that its customers posted does not turn that material into a business record of the ISP: *United States v Jackson* (supra).

Electronic communications

71 Exception: electronic communications

The hearsay rule does not apply to a representation contained in a document recording an electronic communication so far as the representation is a representation as to:

(a) the identity of the person from whom or on whose behalf the communication was sent, or
(b) the date on which or the time at which the communication was sent, or
(c) the destination of the communication or the identity of the person to whom the communication was addressed.

Note:

1 Division 3 of Part 4.3 contains presumptions about electronic communications.

2 Section 182 of the Commonwealth Act gives section 71 of the Commonwealth Act a wider application in relation to Commonwealth records.

3 "Electronic communication" is defined in the Dictionary

The Evidence Act Dictionary defines "electronic communication" as having the same meaning as it has in the *Electronic Transactions Act 1999 (Cth)* or *Electronics Transactions Act 2000 (NSW).* Both statutes have the same definition:

Electronic communication means:

(a) A communication of information in the form of data, text or images by means of guided or unguided[67] electromagnetic energy, or both, or
(b) A communication of information in the form of sound by means of guided or unguided electromagnetic energy, or both, where the sound is processed at the destination by an automated voice recognition system.

Information that is recorded, sorted or retained in an electronic form but is not transmitted immediately after being created is intended to fall within the scope of the definition[68].

[67] The term "unguided" is not intended to refer to the broadcasting of information but instead means that the electronic magnetic energy is not restricted to a physical conduit, such as a cable or wire...: *Electronics Transactions Act 1999 (Cth) Explanatory Memorandum*

Section 161 contains presumptions about electronic communications

161 Electronic communications

(1) If a document purports to contain a record of an electronic communication other than one referred to in section 162, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that the communication:
    (a) was sent or made in the form of electronic communication that appears from the document to have been the form by which it was sent or made, and
    (b) was sent or made by or on behalf of the person by or on whose behalf it appears from the document to have been sent or made, and
    (c) was sent or made on the day on which, at the time at which and from the place from which it appears from the document to have been sent or made, and
    (d) was received at the destination to which it appears from the document to have been sent, and
    (e) if it appears from the document that the sending of the communication concluded at a particular time-was received at that destination at that time.
(2) A provision of subsection (1) does not apply if:
    (a) the proceeding relates to a contract, and
    (b) all the parties to the proceeding are parties to the contract, and
    (c) the provision is inconsistent with a term of the contract.

Note: Section 182 of the Commonwealth Act gives section 161 of the Commonwealth Act a wider application in relation to Commonwealth records.

I note that s 71 is limited only to representations about the identity of the sender, the date and time of communication and the destination/identity of the receiver. It does not cover other representations.

Admissions

81 Hearsay and opinion rules: exception for admissions and related representations

(1) The hearsay rule and the opinion rule do not apply to evidence of an admission.
(2) The hearsay rule and the opinion rule do not apply to evidence of a previous representation:
    (a) that was made in relation to an admission at the time the admission was made, or shortly before or after that time, and
    (b) to which it is reasonably necessary to refer in order to understand the admission.

Specific exclusionary rules relating to admissions are as follows:

- evidence of admissions that is not first-hand (section 82)
- use of admissions against third parties (section 83)
- admissions influenced by violence and certain other conduct (section 84)
- unreliable admissions of accused persons (section 85)

[68] *Electronics Transactions Act 1999 (Cth) Explanatory Memorandum*

- records of oral questioning of accused persons (section 86)

Example:

D admits to W, his best friend, that he sexually assaulted V. In D's trial for the sexual assault, the prosecution may lead evidence from W:

(a) that D made the admission to W as proof of the truth of that admission, and
(b) that W formed the opinion that D was sane when he made the admission.

An admission is defined in the dictionary

"admission" means a previous representation that is:

(a) made by a person who is or becomes a party to a proceeding (including a defendant in a criminal proceeding), and

(b) adverse to the person's interest in the outcome of the proceeding

American examples where evidence from websites were admissible as admissions include *Van Westrienen v Americontinental Collection Corp*[69]*; MGM Studios, Inc. V Grokster Ltd*[70]*; Telewizja Polska USA Inc. V Echostar Satellite Corpi*[71].

Where your client has made an admission on Facebook, you should check to see whether an exclusion to admitting the evidence applies (ss 82-86) or whether there is some other method of exclusion (eg ss 90, 137, 138, s 13 Children (Criminal Proceedings) Act 1987).

[69] 94 F.Supp.2d at 1109 (D.Or. 2000)
[70] 454 F.Supp.966, 970 (C.D.Cal.2006)
[71] 2004 U.S. Dist.LEXIS at 20845

DEFENCE USE OF SOCIAL MEDIA EVIDENCE

Protect your client

Whenever our clients are charged with serious offences we often advise them strongly about their right to silence. This right to silence involves not speaking to the police about the alleged offence but also not speaking to anyone else about it, except their lawyer. I explain to clients that it is possible that whoever they speak to may be subpoenaed by the police to give evidence against them. Practically speaking, a quiet face to face conversation with a family member or friend may not be discovered by the police, unless the police have a telephone intercept or listening device. However, there is no such thing as a "private conversation" on the internet. Police are increasing conducting Facebook searches as a routine part of their investigations, even where there may be no leads pointing them in that direction. Facebook searches by police may be fishing expeditions but they all too often turn up inculpatory evidence.

Furthermore, your advice to your clients may have to go further than telling them not to speak about the allegations. It may involve advising a client to close down their Facebook page, for the following reasons:

- Even if they don't contribute to a discussion about the alleged offence they cannot prevent others from posting comments on their page about the allegations
- There is the risk that the police, witnesses, or even jurors may visit their page and be influenced by what they see there.

Doing your own searches

Just as the police are conducting Facebook, Youtube etc searches in order to find inculpatory evidence, your own searches may produce exculpatory evidence for your client and inculpatory evidence for prosecution witnesses. Searches of potential witnesses may provide valuable information for cross examination. For example, a Google search of an expert witness may reveal information about their background and qualifications. Facebook posting about a witness's drug habits or lifestyle may affect their credibility; see *R v Winchester* [2011] QCA 247. Facebook conversations between witnesses may also show collusion.

Of course, you need to be mindful when searching that if you do discover evidence that you wish to use, you will be confronted with the same hurdles to admissibility that are referred to above in this paper.

Obtaining evidence from the net

The internet has a wealth of material that may assist your case. The police are already frequently using aerial photos as evidence in matters where location is important. Products such as Google Maps are valuable assets in providing aerial maps, measurement of distances, calculations of the most direct route between two or more points etc. Information about weather conditions can also be obtained from the Bureau of Meteorology (www.bom.gov.au).

The internet (esp Facebook and other SNSs) can also be a useful tool to try and locate witnesses for which you may not otherwise have contact details. See *R v Smith [No 1]* [2011] NSWSC 725 in relation to an application for a permanent stay of a "cold case" where the police sought (unsuccessfully) to locate a witness via Google and Facebook searches.

HOW TO OBTAIN EVIDENCE FROM TWITTER/ YOUTUBE/ FACEBOOK

Sometimes you will be able to find evidence from Twitter/Youtube/Facebook and simply obtain a printout which you can seek to use in court. When the sites in question are public there is no ethical impediment to browsing their content to discover evidence unfavourable to the prosecution or prosecution witnesses[72].

But what if the material you are after is not publicly accessible? For example, the complainant's Facebook page has content which you cannot view because of its privacy settings. You may be able to get access if you have a defence witness who has access (eg they are a Facebook Friend), although you must be very careful about how you conduct your investigations and communications with such witness/es.

Is it ethical for you to become the complainant's Friend in order to look at her Facebook, or to pretend to be Justin Beiber so that she'll befriend you and you can sneek a peek at her page? Is it ethical for you to get someone else to befriend her for that purpose?

The precise issue of whether lawyers violate ethical rules of conduct by using trickery or deceit in order to obtain access to another's individual social networking site has not yet been addressed by the courts. However, both the New York and Phildelphia Bar have provided opinions on the matter[73]. The New York Bar believed that the Rules of Professional Conduct were violated whenever an attorney "friends" an individual user under false pretenses to obtain evidence from a social networking website. There have been other cases where similar covert operations (not involving SNS) have been found to be unethical: *People v Pautler*, 35 P.3d 571 (Colo. 2001); *In re v Gatti*¸ 330 Ore. 517 (2000). US courts have found such unethically obtained evidence to be inadmissible: *Midwest Motor Sports v Arctic Cat Sales, Inc*, 347 F.3d at 696.

Such conduct would also be unethical and in breach of the NSW Solicitors Rules or NSW Barrister's Rules:

> Solicitors Rules 34 – Communications
>
> A practitioner must not, in any communication with another person on behalf of a client:

[72] Dal Pont, G, "Social networking sites can prove ethically dangerous", *Law Society Journal,* June 2011, p 47.
[73] Philadelphia Bar Association, Professional Guidance Committee, Opinion 2009-02, March 2009, available at http://wwww.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebserverResources/CMSResources/Opinion_2009-2.pdf; New York City Bar, The Association of the Bar of the City of New York Committee on Professional Ethics, Formal Opinion 2010-2, *Obtaining evidence from social networking websites* .

1. Represent to that person that anything is true which the practitioner knows, or reasonably believes, is untrue; or
2. Make any statement that is calculated to mislead...

Barristers Rules

5. Principles

(c) barrister as specialist advocates in the administration of justice, must act honestly, fairly, skilfully and with competence and diligence...

12. Advocacy Rules – General

A barrister must not engage in conduct which is

a) Dishonest or otherwise discreditable to a barrister...

Even if you somehow ended up as a Friend, you would still probably not get full access to the page – you certainly would not be able to access the page's inbox. The only way to obtain full access would be to either obtain it from the Facebook user themselves or via subpoena to Facebook.

How to subpoena Facebook etc?

Facebook, Twitter and YouTube have their data centres based in California. Hence, a subpoena to the Australian office will not achieve the result of obtaining the material. Britain has successfully subpoenaed documents from Twitter by going directly to the Californian courts[74]. However, I am not so sure that Australia would have the same success.

There are Australian authorities which make it clear that even if there is authority to grant leave to serve a subpoena out of the jurisdiction, the court will be very slow to exercise its discretion: *Arhill Pty Ltd v General Terminal Co Pty Ltd* (1990) 23 NSWLR 545; *Stemcor (A/Sia) Pty Ltd v Oceanwave Line SA* [2004] FCA 391. See also *Ives v Lim* [2010] WASC 136 where the plaintiff unsuccessfully appealed to the Western Australian Supreme Court against a decision rejecting his application to issue a subpoena to Russia to discover the identity of chat room users (eg fnkymnky, so_deranged) who had allegedly partook in cyberbullying/defaming him.

Facebook states that the contents of a user's account are protected from disclosure by the Stored Communications Act. It also states that it is not able to provide content that has been deleted. To this end, Facebook says "If a Facebook user deleted content from their account, Facebook will not be able to provide that content. Effectively, Facebook and the applicable Facebook user have acess to the same content. To the extent a user claims it does not have access to content (eg the user terminated their account), Facebook will restore access to allow that user to collect and produce the information to the extent possible"[75].

Noting the above, "Facebook urges parties to civil litigation to resolve their discovery issues without involving Facebook"[76]. This would appear to be the case for criminal defence lawyers too. In

[74] Brown, Mark, *UK Councillors go to California to unmask anonymous tweeter*, Wired UK, 31 May 2011.
[75] Molder Legal Group Professional Association, "Obtaining user content from Facebook may not be as easy as you think", 11 November 2010: see http://molderlegal.com/content/obtaining-user-information-from facebook-may-not-be-as-easy-as -you-think.
[76] Ibid.

response to my questions about how an Australian criminal defence lawyer could subpoena Facebook 's Law Enforcement Response Team responded:

> Federal law prohibits service providers such as Facebook from disclosing the contents of communications (e.g. messages, Wall posts, photos, etc.) in response to requests from and/or process issued on behalf of private parties. This includes defendants in criminal cases and parties to civil litigation. Specifically, the Stored Communications Act, 18 U.S.C. §§ 2701 et seq., prohibits Facebook from disclosing the contents of an account to any non-governmental entity.
>
> Requests for contents should be sent directly to the Facebook user at issue who may satisfy any discovery obligations relating to their Facebook account by preserving, producing and authenticating that data. The user may log into their account and collect the contents thereof. Facebook also provides a "Download Your Information" tool, which is accessible to the user through the "Account Settings" drop down menu.
>
> If a user cannot access content because he or she disabled or deleted his or her account, Facebook will, to the extent possible, provide reasonably available data to the user.
>
> For additional information please see http://www.facebook.com/help/?page=1057 and http://www.facebook.com/help/?page=849

Asides from the forensic disadvantage of putting the witness on notice, a subpoena to the witness user to produce documents may encounter problems in relation to the logistics of the user accessing and printing out facebook pages and in relation to whether you trust that the witness will fully comply with the subpoena and not leave out relevant bits or even delete material. If you do choose to subpoena the user, you might consider issuing a subpoena to produce documents and a subpoena to attend to give evidence. Once in court, a laptop could be set up with internet access and a projector screen. The witness could then be directed to navigate their Facebook page whilst in the witness box.

If you still wish to subpoena Facebook itself, the subpoena will have to be in a Californian court. Facebook requires the Facebook users ID of the specific account from which information is being sought, or the email address associated with that account. Other information such as names, birthdays and locations are insufficient. Facebook also charges a mandatory non refundable processing fee of $500 per user account. Payment must be included with the subpoena. Although a "custodian declaration" is included, there is an additional $100 fee for it to be notarized. Turnaround time is a minimum of 30 days. Facebook will accept a request for the subpoena to be expedited if an additional $200 fee is include with the subpoena[77]. It may be possible to get an agent in California to issue the subpoena and then remit the material to Australia.

Apparently though, the cheapest and easiest way to obtain information from Facebook is to convince the Australian police (NSW police/AFP) that they should ask the Attorney General for assistance. The Attorney General (on behalf of a government department) can then ask the US for mutual assistance. If the police are unwilling to assist, you can go to the NSW Supreme Court and

---

[77] See Molder Legal, supra.

seek a certificate that the evidence is exculpatory???. Once that certificate is issued the Attorney general can then ask for mutual assistance from the US. The US can then issue a search warrant on Facebook to obtain the evidence. The turn around time for the US to issue and carry out a search warrant is approximately 6 months.

Of interest, see also *Charmyne Palavi v Radio 2UE Sydney Pty Ltd* [2010] NSWDC 332 in relation to failure by a party to comply with orders for discovery of mobile phone and Facebook material.

CONCLUSION

During the riots in England in August 2011, early criticism was made of the alleged role of social media in exacerbating rioting and corralling rioters. However, a number of British police agencies used Facebook, Twitter, Flickr and YouTube to communicate to rioters and the public alike in appeasing public fears, calling for information and publishing photographs and descriptions of alleged suspects[78].

Nowadays, regular conferences and seminars are being held to bring experts from around the world to discuss the efficacy of social media to policing agencies. For example, the "Social Media, the Internet and Law Enforcement" conference (SMILE) has been developed to facilitate the discussion of the application of social media to law enforcement and the investigation of crime and crime prevention[79]. Legislation is also being passed[80] and policies formed to facilitate cooperation and information sharing between law enforcement agencies and social media providers.

Hence, we can expect to see more and more use of social media evidence by police

The Australian Government Department of Communications has also recently announced the establishment of a Children's e Safety Commissioner and released a discussion paper seeking comment on enhancing online safety for children[81].

Technology continues to advance. Though there appears to be a bit more judicial consideration of social media evidence since the last time I presented this paper in 2011, Australian law still does not seem to have kept pace with the quantum of American cases. I hope therefore that this paper assists you in being pioneers in both seeking to use and objecting to the use of social media and mobile phone evidence.

[78] Alyce McGovern and Murray Lee, 'Police Communications in the Social Media Age', in Keyzer, P, Johnston, J and Pearson M., *The Courts and the Media: Challenges in the era of digital and social Media*, Halstead Press, 2007, p 166

[79] Ibid. p 167.

[80] See the Cybercrime Act 2001 (Cth) and the Cybercrime Legislation Amendment Bill 2011 (Cth) referred to in Middletons, Dudley, *New Bill changing how cybercrime is regulated in Australia*, Internet Law Bulletin 2011, Vol 14 No 4 July 2011.

[81] Submissions were due 7 March 2014.

Aaron Tang

12 March 2014

Acknowledgments

Thanks to the following people who provided assistance with the original 2011 paper and/or for this update: Legal Aid Library, Andrea Hadaway, Tim Khoo, Matt Dimech, Erica Lai, Kirsty Harrison, Carey Hulme, Julianne Elliott, Tony Lynch, Richard Leary, Vaughan Roles, Mark Dennis, Matthew Johnson, Peter McGhee. Apologies to anyone else who I may have inadvertently missed.