Family Violence, Cyber Stalking and the Latest Cases and Developments

Paul Fildes

Accredited Family Law Specialist and Principal, Taussig Cherrie Fildes

and Carly Boekee

Associate, Taussig Cherrie Fildes

This paper will focus on cyber stalking as an emerging form of family violence, looking at how victims of cyber stalking can protect themselves, the changes to the law as a result of the recent metadata legislation and recent cases in the Family Courts where evidence of cyber stalking has been adduced.

Family Violence Legislation

There are three different Acts to which we need to have regard in matters of family violence and cyberstalking.

Section 4AB of the *Family Law Act 1975* (Cth) ("FLA") provides that the definition of family violence for the purposes of the Act is *"violent, threatening or other behaviour by a person that coerces or controls a member of the person's family (the family member), or causes the family member to be fearful."*

Examples of family violence are set out in the FLA and include, but are not limited to, an assault, sexual assault or sexually abusive behaviour, stalking, property damage, causing death or injury to an animal, economic abuse, preventing the family member from maintaining connections with family, friends or culture and unlawful deprivation of liberty.

Section 5 of the *Family Violence Protection Act 2008* (Vic) ("FVPA") provides the definition of family violence to which the Court will have regard to when considering an application either by Victoria Police or by an applicant for a family violence intervention order. The FVPA provides that family violence is:

(a) behaviour by a person towards a family member of that person if that behaviour

(i) is physically or sexually abusive; or

(ii) is emotionally or psychologically abusive; or

(iii) is economically abusive; or

(iv) is threatening; or

(v) is coercive; or

(vi) in any other way controls or dominates the family member and causes that family member to feel fear for the safety or wellbeing of that family member or another person; or

(b) behaviour by a person that causes a child to hear or witness, or otherwise be exposed to the effects of, behaviour referred to in paragraph (a).

Examples of a child being exposed to family violence are set out in subsection (1) of the Act and include overhearing threats of physical abuse, witnessing an assault, comforting and providing assistance to a family member who has been physically abused, cleaning up property damage and being present when police attend an incident of physical abuse.

Subsection (2) of the Act is similar to section 4AB(2) of the FLA as it provides specific examples of behaviour that constitute family violence which include an assault, sexual assault, property damage, causing or threatening to harm an animal and unlawful deprivation of liberty.

Stalking

Section 21A of the *Crimes Act 1968* (Vic) provides that stalking is a course of conduct which can include following the victim, contacting the victim, entering or loitering outside their home or workplace, interfering with the victim's property, offensive or abusive acts and keeping the victim under surveillance. The Crimes Act also specifically includes within the definition of stalking examples of behaviour which are generally regarded as "cyberstalking", such as:

- contacting the victim by email or other electronic means,
- publishing on the Internet or by email or other electronic means a statement or electronic material relating to the victim or purporting to relate to or originate from the victim,
- tracing the victim or another person's use of the Internet, or email or other electronic communications.

Stalking is punishable by up to 10 years imprisonment.

The *Personal Safety Intervention Orders Act 2010* provides that the Court may make a personal safety intervention order in respect of stalking.

Most instances of stalking and cyberstalking are also likely to fall well within the definition of family violence under the FLA and FVPA as behaviour that coerces or controls or causes a family member to be fearful.

Cyber Stalking

Cyber stalking is a form of family violence that has become increasingly prevalent with the development and widespread usage of technology including social media, smart phones and GPS.

Examples of cyber stalking typically include:

(a) denigration of the victim on social media;

(b) tracking the victim's internet use;

(c) hacking into the victim's email or social media accounts;

(d) impersonating the victim online or via email;

(e) spreading rumours about the victim;

(f) posting embarrassing, fake or intimate comments, photos or videos of the victim on social media;

(g) sending repeated Facebook messages, emails or text messages;

(h) harassment on social media sites or dating, chat or games sites;

(i) creating a fake account in another name and communicating with the victim without their knowledge of the person's true identity.

The purpose of cyber stalking and harassment is to scare, control or humiliate the victim.

Both victims and potential victims of family violence including stalking, and particularly those who remain separated under the one roof, should protect and preserve their private information and online presence.

Clients should be advised to remove their former partner as a Facebook friend and change their account to private so that only friends can access or post to their Facebook page. Passwords for both email and social media accounts should be changed and kept confidential. Clients should always sign out of email and social media accounts and uncheck the box "remember me on this computer". If clients are concerned about spyware and keylogging programs, which are commonly available and can track computer activities without the user's knowledge, they may wish to use a friend or family member's computer and have legal correspondence sent to a separate email address. Clients should also consider turning off their mobile phone when not in use, turn off the optional location service and change the settings so that a password or pin is required to unlock the keypad.

In the event you are acting for a client who is the respondent to a family violence intervention order, always ensure that you remind them that the order states that they are also prohibited from causing "another person to do anything the respondent must not do" under the order. They should advise their family and friends not to have any contact with the applicant on social media or post anything which could be construed as referring to them. It will not assist their case if the applicant produces at the hearing screen shots of social media posts, emails or text messages about them from the respondent's family members or friends and the respondent could be charged with contravening the intervention order.

Gathering evidence

Victims of stalking or cyberstalking should retain copies of abusive or threatening messages, posts or photos so that they can be used later as evidence either in support of an application for an intervention order or in family law proceedings if necessary. Most mobile phones and computers allow the user to take a screenshot and clients should be encouraged to do so immediately upon seeing a social media post which could later be taken down.

Victims can also download a copy of the information from their own Facebook account by logging into their Facebook account and clicking *"Download Your Information"*. It will include Timeline information, posts they have shared, messages and photos, but also ads

they have clicked on and data such as the IP addresses which are logged when logging into and out of Facebook. It will not include information or content that has been deleted by the user.

Unsurprisingly, Facebook will not provide another user's information upon request. It may be prudent to seek that the other party disclose their Facebook account, however remember to be alert to the fact that they may well delete any inappropriate posts, shared posts or photos prior to disclosure. Accordingly, it can prove difficult to obtain a print out of the other party's Facebook page if their page is private and mutual Facebook friends are unwilling to assist by providing screenshots.

Our experience has been that subpoenas to telecommunications companies ordinarily produce records of the dates and times phone calls and text messages have been sent and received and the phone numbers they were sent to, but not the content of the messages themselves. You may also encounter difficulties if the company you are seeking to subpoena is an overseas company and refuses to comply with a subpoena issued by an Australian court.

You may wish to consider utilising a Notice to Produce or a Notice to Admit Facts. Alternatively, consider filing an Application in a Case seeking an order that the other party produce copies of all comments posted on Facebook which refer to the victim or the children or either of them as well as copies of all private messages sent to the victim.

Metadata retention legislation

As a result of the amendments to the *Telecommunications (Interception and Access) Act 1979* brought about by the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* from 13 October 2015 all Australian telecommunications companies have been required to retain metadata logs for their customers' email, internet, mobile and landline usage for a two year period. Previously, largely as a result of the cost of storage, telecommunication companies frequently discarded this type of information.

The obligations of the service provider is set out at section 187A of the Act and the types of information to be retained are set out at in a table at section 187AA. Section 172 provides that the substance or contents of communications are not to be disclosed.

Metadata includes:

- phone numbers of people you have called or sent an SMS;
- missed numbers;
- 1800 numbers;
- duration of the call;
- time and date of calls and SMS;
- approximate location of the person making the call and the person receiving the call;
- email addresses of the recipients of your emails;
- time and date of email and volume of attachments;

- your IP address;
- time and duration of your web connections;
- volume of your uploads and downloads.

Metadata does not include:

- the contents or substance of the conversation, text message or email;
- internet browsing history;
- subject line or content of emails.

Google has already been keeping records of the location history for those individuals with a Google account for several years. Unless it has been actively disabled, Google records and time stamps the coordinates of the individual's mobile phone every 45 seconds. Whilst an individual could previously opt out of Google's tracking and delete their history, this information must now be stored for two years under the Metadata legislation.

The purpose of the legislation was to provide access to metadata to a limited set of entities and agencies, primarily for the purpose of law enforcement. However, as a result of public protest prior to passage of the bill, the bill was amended so that account holders can not only access their own metadata information, but also of anyone else who uses their account.

Critics of the legislation have expressed their concerns that many perpetrators of family violence hold the accounts for computers, phones and the like to which the metadata applies and can now access the victim's information retrospectively over a two year period. Potentially, the metadata information from a mobile phone will allow a perpetrator access to information with respect to:

- whom they connect to and the frequency and length of those connections;
- where they go and patterns of behaviour, including how long they remained in a particular location and frequency of trips.

It is alarming to consider that a victim of family violence who has left the relationship can still have their information and data accessed by the perpetrator for a two year period without their consent, putting them at serious risk of harm. Perpetrators can potentially find out where they are living, the identity and location of their friends and any new partners, the services they accessed in leaving the relationship, the location of their new workplace or their children's new school and the fact that they have sought legal advice.

One avenue for legislative reform is that it become an offence for the respondent to a current family violence intervention order to access the applicant or affected family member's metadata information. Of course, the difficulty would be one of enforcement as the victim may not be aware of the respondent's attempts to access their information from the telecommunications company.

Another option is that the account holder be required to provide evidence of the consent of other users to the account holder accessing their information. Whilst this would be easier to enforce the obvious concern is that the victim's consent will be extracted by threats or coercion.

Family violence victims who are concerned about metadata should use a messaging service operated by an overseas company such as Google, Twitter, Facebook or Whatsapp. The metadata stored will include the fact that they are using these services. The recipients of the messages will not be stored. Overseas based email service, such as Gmail, Hotmail or Yahoo, will also only store the identity of the individual using the services and not who they are emailing as information to and from offshore email service providers is generally encrypted, including the source and destination email address.

Malcolm Turnbull has previously suggested the use of Wickr, a messaging service which sends the message to a server and delivers it to the recipient when they log in. The metadata captured for this service will show that there has been communication with the Wickr server but will not directly link the sender and the recipient.

Another option is to use a virtual private network (VPN) which will encrypt communications between the sender and the VPN server. Similar to Wickr, the only metadata that can be collected will show that the recipient's data came from the VPN server but will not identify the sender.

Tor is primarily used to encrypt your web browsing history to protect it from surveillance and can be downloaded for free.

Recent Cases in the Family Courts

Whilst most cases of cyber stalking are played out in the criminal courts, there have been some recent examples in the Family Law Courts which demonstrate the varied types and means of cyberstalking and how the evidence may be taken into account by the Court.

Ahmed & Jeret [2016] FamCA 442

In parenting proceedings in the Family Court, the mother alleged a history of family violence by the father and that the father had stalked her on Facebook and also physically followed her. The mother's evidence as to the family violence perpetrated by the father was largely accepted by Justice Rees.

The father conceded during cross-examination that he had created the "Ms V" Facebook page in order to find out information about the mother. He conceded that he may have created other identities for the same purpose but alleged he couldn't remember. He conceded that his denials of the mother's allegations in his previous affidavits were false and that he knew that he had stalked the mother on Facebook both when the intervention order proceedings were on foot and when he was charged with using telecommunications to menace the mother.

Justice Rees took the cyberstalking into consideration under section 60CC(3(i) as relevant to the attitude of the father to the responsibilities of parenthood. Her Honour stated that she

was unconvinced that the father really understood why his behaviour was unacceptable. Her Honour stated that the father had received counselling from Dr G for several years and understood the language of family violence, including the expression "coercive and controlling", however was unable to identify any examples of behaviour by him which fell into that definition and had continued in his evidence to attempt to justify his own behaviour by referring to the mother's alleged failures.

Janssen & Janssen [2015] FamCA 942

Justice McClelland took into consideration at an interim hearing of the father's application to commence spending supervised time with the children evidence presented by the mother of Facebook print outs which included communication between the father and his new partner, Ms D. In January 2015 the father had posted a Facebook message referring to a child who was being treated in the hospital where the father worked. The message read:

> *The father was there for him looking after him after his surgery. The little boy needed his Dad and his Dad was there for him. At 6:15am sometimes all a child wants is his father to be there for him...*

Ms D had replied:

> *At least nobody will take away your daughter, unlike those cruel idiots have, I cant believe the stupidity and cruelty! She calls herself a mother, what a JOKE!!!!*

The reference to the father's daughter was understood as a reference to the daughter of the father and Ms D. The father had then responded *"Well said"* with a smiley face.

The father had also posted:

- in response to a Facebook message opposing the culling of sharks in Western Australia:

  > *"Mother shark must know without daddy shark her offspring will grow up screwed up. Her enemies with cc problems must be glad everything is going to plan"*

- a reference to a petition website titled *"Stop False Allegations of Domestic Violence"*;
- a message which read as follows:

  > *When a friend of mine notices at 4pm a really old lady (hunched and all) struggle with 3 young kids at a Northern Beaches Mall, it makes her wonder where the mum and dad are? Poor kids suffering for someone else's mess up is her thought. I try not to judge. After all Christ does not judge those without guilt... - feeling amused*

- another Facebook message which stated:

  > *My father has a piece of Padre Pio and the majority of the Australian Catholics would agree if he was here now he wouldn't be a fan of Catholics who fake domestic violence to cover up an extra-marital affair with a work colleague which is documented - just saying!!!!*

- a Facebook message in response to a message from White Ribbon Australia congratulating Ms Rosie Batty on being named Australian of the year. The father's message read:

  "Domestic violence is a serious issue my Australia Day wish is that all those that fake domestic violence for their own selfish and sinister motive be accountable by the legal system. Rosie may be sad to see her hard work be for nothing, due to the actions of a few horrible individuals."

His Honour declined to alter the existing arrangements whereby the children spent no time with the father pending the final hearing and an updated single expert report and noted that the father's Facebook entries would be a matter for the final hearing.

Delucca & Decarlo [2016] FamCA 497

At the final hearing the mother alleged controlling behaviour by the father, including that he had placed a tracking device on her car. The mother had received an anonymous text message a few weeks after an incident at changeover which had lead to police charging the father with intimidation and while an interim intervention order was in place. The text message stated that there was a *"tracker"* in her car and that *"he has been following your every move…no visual phone calls and is currently working on a plan with his mate to discredit you at work"*. The mother located the tracking device in her car and took it to the police who informed her that the sim card was registered to the father.

There was also evidence before the Court of Facebook entries between the father and Ms L in which he advised Ms L that he had placed a tracking device on the mother's car and had been tracking the mother's movements for *"months"*.

The father conceded having placed the device on the mother's car. His evidence was that he was keen to know where the mother was after separation and was interested in what she was doing and the men she was seeing. He claimed to have informed the mother prior to installing it and said that he disconnected it after receiving advice from his solicitor that he should do so.

Justice Hannam largely rejected the father's evidence about the tracking device. Her Honour was satisfied that the father had engaged in stalking and had shown controlling tendencies following separation in both his interactions with the mother and the child.

Condon-Nixon & Rivers [2012] FamCA 7

In final parenting and property proceedings, Justice Young expressed his concerns about the mother's evidence that she had been *"exposed on Facebook and described as a liar, manipulator, dad hater, child neglecter, child abuser and stalker"*. The comments accompanied a photograph of the mother, her address, current mobile telephone number and a cross reference to her business interests.

The father and his new wife, Ms L Rivers, denied any involvement, however the mother also tendered Ms L Rivers' Facebook page and her contact address and nickname was similar to the Facebook page which had been created about the mother. Justice Young concluded that

the similarity was *"obvious but not conclusive"*. His Honour expressed his concern that it took approximately three to four weeks of daily reporting by the mother to have the offensive site removed. Counsel for the father and the Independent Children's Lawyer cross-examined the mother in an attempt to establish that she set up the page herself, however his Honour remained unconvinced.

Justice Young expressed his surprise that neither a subpoena nor written requests had not been issued to the website controller for the disclosure of information such as the date the site was created and any personal or identifying information. His Honour ultimately accepted Ms L Rivers' denials of any responsibility in creating or organising the Facebook page. There was insufficient evidence for his Honour to make any findings as to who was responsible for creating the page.

Vincent & Reeves [2015] FCCA 616

In an interim hearing of the father's application to spend time with the child, the mother asserted that she had been stalked by the father, including that he had arrived unannounced and unbidden at her home, repeatedly driven past her home in his car and arrived at her home with gifts on the child's birthday as a result of which police were called.

There was also evidence about Facebook posts from each of the parties. It appeared that a message posted by the father about the mother had likely been obtained as a result of the mother or someone else accessing the father's account without his consent. The mother sought an order restraining both parties from posting anything on Facebook or other social media sites.

His Honour stated when delivering his ex tempore reasons:

> *If there are any more inflammatory postings on Facebook, I will have no alternative but to stop any interaction between X and her father. Facebook is a fairly contemporary and recent phenomenon, the societal effect of which continue to play out.*
>
> *I do not know what anybody is thinking at any one time. Nobody does. We only know what somebody is thinking if they say something or behave in a particular way. One of the consequences, I think, of Facebook is that people are inclined to share their spontaneous and unfiltered thoughts with the world, at large, instantly through media such as facebook. They do not necessarily consider that such thoughts have the potential to be frozen forever on the internet for all to see.*
>
> *The process has a spontaneity about it but, unlike thoughts which appear in the mind and then disappear and do not go anywhere else and are forgotten, what is put on Facebook does not disappear. It stays there forever.*
>
> *Both parties, I think, would be wise to think about that. They may want to share their frustration with this process, their antipathy about the other party with their friends, associates, and even with the world in general but they are not, I think, free to do so.*

Judge Brown granted an injunction in the terms proposed by the mother.

Beyond physical harm: threats, property damage, economic abuse, emotional and psychological abuse

As is apparent from the case law, stalking and cyberstalking are just one of the many types of behaviour which may be used by perpetrators of family violence in an effort to control or intimidate the victim. Stalking is a form of emotional and psychological abuse in itself and is now fortunately recognised as such and encompassed within the wider definition of family violence.

Stalking behaviour may or may not also be accompanied by other forms of non-physical harm, such as verbal threats or denigration to the victim directly or via children, damage to property and economic abuse. All forms of family violence should be taken seriously and the risk of harm to the victim assessed on an ongoing basis. Precautions should be put in place to protect clients' private information and legal professional privilege, particularly in circumstances where the parties are separated under the one roof. Evidence of threatening, stalking or other behaviour falling within the definition of family violence should be gathered and retained on the file for use in support of an application for an intervention order for the protection of the victim and/or the children or in support of an application in the family courts as is appropriate.

Appendix A

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015

172 No disclosure of the contents or substance of a communication

Divisions 3, 4 and 4A do not permit the disclosure of:

(a) information that is the contents or substance of a communication; or

(b) a document to the extent that the document contains the contents or substance of a communication.

…

Division 1—Obligation to keep information and documents

187A Service providers must keep certain information and documents

(1) A person (a ***service provider***) who operates a service to which this Part applies (a ***relevant service***) must keep, or cause to be kept, in accordance with section 187BA and for the period specified in section 187C:

(a) information of a kind specified in or under section 187AA; or

(b) documents containing information of that kind;

relating to any communication carried by means of the service.

Note 1: Subsection (3) sets out the services to which this Part applies.

Note 2: Section 187B removes some service providers from the scope of this obligation, either completely or in relation to some services they operate.

Note 3: Division 3 provides for exemptions from a service provider's obligations under this Part.

(3) This Part applies to a service if:

(a) it is a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both; and

(b) it is a service:

(i) operated by a carrier; or

(ii) operated by an internet service provider (within the meaning of Schedule 5 to the *Broadcasting Services Act 1992*); or

(iii) of a kind for which a declaration under subsection (3A) is in force; and

(c) the person operating the service owns or operates, in Australia, infrastructure that enables the provision of any of its relevant services;

but does not apply to a broadcasting service (within the meaning of the *Broadcasting Services Act 1992*).

…

(4) This section does not require a service provider to keep, or cause to be kept:

(a) information that is the contents or substance of a communication; or

Note: This paragraph puts beyond doubt that service providers are not required to keep information about telecommunications content.

(b) information that:

(i) states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider; and

(ii) was obtained by the service provider only as a result of providing the service; or

Note: This paragraph puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history.

(c) information to the extent that it relates to a communication that is being carried by means of another service:

(i) that is of a kind referred to in paragraph (3)(a); and

(ii) that is operated by another person using the relevant service operated by the service provider;

or a document to the extent that the document contains such information; or

Note: This paragraph puts beyond doubt that service providers are not required to keep information or documents about communications that pass "over the top" of the underlying service they provide, and that are being carried by means of other services operated by other service providers.

(d) information that the service provider is required to delete because of a determination made under section 99 of the *Telecommunications Act 1997*, or a document to the extent that the document contains such information; or

(e) information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected.

(5) Without limiting subsection (1), for the purposes of this section:

(a) an attempt to send a communication by means of a relevant service is taken to be the sending of a communication by means of the service, if the attempt results in:

(i) a connection between the telecommunications device used in the attempt and another telecommunications device; or

(ii) an attempted connection between the telecommunications device used in the attempt and another telecommunications device; or

(iii) a conclusion being drawn, through the operation of the service, that a connection cannot be made between the telecommunications device used in the attempt and another telecommunications device; and

(b) an untariffed communication by means of a relevant service is taken to be a communication by means of the service.

(6) To avoid doubt, if information that subsection (1) requires a service provider to keep in relation to a communication is not created by the operation of a relevant service, subsection (1) requires the service provider to use other means to create the information, or a document containing the information.

187AA Information to be kept

(1) The following table sets out the kinds of information that a service provider must keep, or cause to be kept, under subsection 187A(1):

Kinds of information to be kept		
Item	**Topic** **Column 1**	**Description of information** **Column 2**
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: (i) any name or address information; (ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being

Kinds of information to be kept		
Item	**Topic** **Column 1**	**Description of information** **Column 2**
		information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service, or any related account, service or device.
2	The source of a communication	Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.
3	The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.
4	The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.
5	The type of a communication or of a relevant service used in connection with a communication	The following: (a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. (b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. Examples: Call waiting, call forwarding, data volume usage. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).
6	The location of equipment, or a line, used in connection with a	The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the

Kinds of information to be kept		
Item	**Topic** **Column 1**	**Description of information** **Column 2**
	communication	start of the communication; (b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.