A critical analysis of Queensland's cyberstalking legislation

Daniel Sullivan

Daniel Sullivan is admitted as a solicitor in Queensland and is currently undertaking LLM (Intellectual Property) studies at the University of Queensland.

1 Introduction

"Cyberstalking" is the term used to describe stalking behaviour undertaken by way of computer. The cyberstalker uses a computer to stalk or otherwise harass another computer user.

This paper examines and assesses the legislative response to cyberstalking undertaken in Queensland through the amendment of Chapter 33A of the *Queensland Criminal Code*.

It will provide a description of stalking[1] in general and the legislative strategies employed to address it in Australian States and Territories during the 1990s. The phenomenon of cyberstalking and the changes to legislation made in those same jurisdictions will also be examined.

2 What is stalking?

Stalking may be described as:

> *When one person causes another a degree of fear or trepidation by repeated or protracted behaviour which is on the surface innocent, but which, when taken in context, assumes a more threatening significance.*[2]

It is impossible to specify every kind of stalking behaviour.[3] A committed stalker will find ways around a specific prohibition. An apparently harmless act will not be seen as part of a stalking campaign until considered in its context of fear and trepidation. Stalking acts might include:

- telephoning the victim;
- sending gifts, letters, or notes to the victim;
- arranging delivery of unwanted flowers or taxis;
- conducting surveillance of the victim;
- waiting or loitering outside the victim's home; and
- following or approaching the victim at home or at work.

Many instances of stalking arise out of failed intimate relationships, although a stalker could also be a mere acquaintance of or a stranger to the victim. Often, the main motivation driving a stalker is to control the victim.[4]

Victims of stalking may suffer profound, long-term emotional injuries and lose time from work or be unable to return to work. Another serious consequence is that stalking behaviour often precedes more violent crimes.[5]

Anecdotal reports indicate that law enforcement agencies in many countries did not take action against stalking activity owing in part to the lack of an appropriate criminal offence which applied to stalking.[6] It is only in the last fifteen years that stalking has been identified as a social problem and the first stalking legislation in the world was passed in California as recently as 1990.[7]

3 Legislative responses to stalking

Legislators from most jurisdictions have avoided over-specifying stalking behaviour in stalking legislation. They have concentrated, with varying degrees of emphasis, on the intent behind the stalker's behaviour or the effect of the behaviour on the victim. Either way, the sense of fear and apprehension, as opposed to the actual physical acts, is the essence of the offence.

3.1 Queensland

In 1993, Queensland became the first Australian jurisdiction to enact legislation to prohibit stalking.[8] The legislation was substantially remodelled in 1999.[9]

Section 359B of the Queensland *Criminal Code* (as amended) defines unlawful stalking as conduct -

(a) intentionally directed at a person (the "stalked person"); and

(b) engaged in on any 1 occasion if the conduct is protracted or on more than 1 occasion; and

(c) consisting of 1 or more acts of the following, or a similar, type —

- *(i) following, loitering near, watching or approaching a person;*
- *(ii) contacting a person in any way, including, for example, by telephone, mail, fax, e-mail or through the use of any technology;*
- *(iii) loitering near, watching, approaching or entering a place where a person lives, works or visits;*
- *(iv) leaving offensive material where it will be found by, given to or brought to the attention of, a person;*
- *(v) giving offensive material to a person, directly or indirectly;*
- *(vi) an intimidating, harassing or threatening act against a person, whether or not involving violence or a threat of violence;*
- *(vii) an act of violence, or a threat of violence, against, or against property of, anyone, including the defendant; and*

(d) that —

- *(i) would cause the stalked person apprehension or fear, reasonably arising in all the circumstances, of violence to, or against property of, the stalked person or another person; or*
- *(ii) causes detriment, reasonably arising in all the circumstances, to the stalked person or another person.*

Complemented by expansive definitions in section 359A, the effects of stalking outlined in section 359B(d) (which must reasonably arise in all the circumstances) include:

- The victim would be caused to apprehend or fear violence (including deprivation of liberty) to the victim or another person. This apprehension or fear need not actually be caused. This definition of violence appears to be wide, including any sort of bodily injury and sexual assault.
- The victim would be caused to apprehend or fear violence to property (including damage, destruction, removal, use or interference of that property) belonging to the victim or another person. This apprehension or fear need not actually be caused.
- The victim is actually caused to apprehend or fear violence (including deprivation of liberty) to the victim or another person.
- The victim is actually caused to apprehend or fear violence to property (including damage, destruction, removal, use or interference of that property) belonging to the victim or another person.
- The victim or another person is actually caused serious mental, psychological or emotional harm.
- The victim or another person is actually prevented or hindered from doing an act that that person is lawfully entitled to do eg the victim no longer leaves home.
- The victim or another person is actually compelled to do an act that that person is lawfully entitled to abstain from doing eg selling a property that the victim would not otherwise sell.

Intentionally Directed at a Person (section 359B(a))

The requirement that the conduct be "intentionally directed at a person"[10] prevents prosecution for accidental stalking eg unknowingly following a person on more than one occasion.

Conduct (section 359B(b))

Section 359B(b) resembles most stalking statutes in that a single (but not protracted) act cannot support a charge of stalking. This recognises that stalking involves repeated or protracted intrusion into the life of the victim and eliminates the possibility that a person will be subject to criminal liability for stalking for a single act. That act may, however, offend another provision of the *Criminal Code*.[11]

Stalking Acts (section 359B(c))

The list of stalking acts in section 359B(c) is similar to lists in other Australian stalking statutes. Sections 359B(c)(vi) and (vii) serve as wide "sweeper" clauses.

Stalking Effects[12] (section 359B(d))

Section 359B(d) is the most controversial element of the offence. Whether the acts of the stalker constitute stalking is judged against the objective effect on the victim. The intention of the stalker is irrelevant[13], which is unusual for a criminal offence. Instead, consideration must be given to various matters including whether the reasonable victim would have suffered the relevant fear, apprehension or serious mental harm in the circumstances.

Before stalking became an offence, the *Criminal Code* was useful only where violence was threatened in specified circumstances[14] eg forcible entry[15], threatening violence[16], or written threats to murder.[17] The conduct that could constitute these offences was easily identifiable when compared to superficially innocuous acts of stalking. The gap between summary offences (with accompanying ineffective remedies such as restraining orders) and the indictable major offences in the *Criminal Code* was too wide.[18]

3.2 Comparison with other Australian jurisdictions

Although, every State and Territory has enacted legislation analogous to the stalking provisions in the *Criminal Code*, Queensland is unique among Australian States in that the intention of the stalker to cause a stalking effect on that person or another person is expressed to be immaterial to the offence.[19] This formulation is perhaps the most generous for the prosecution as specific intent can be difficult to prove.[20]

The Model Criminal Code Officers Committee (MCCOC)[21] criticises the constructive formulation used by Queensland and notes that it resembles the imposition of criminal liability for mere negligence, which ought not provide the basis for a criminal conviction attracting, in Queensland, a maximum term of five years imprisonment.[22]

In contrast, the most difficult provision for a prosecution is section 19AA of the South Australian *Criminal Law Consolidation Act* 1935. Under that provision, the stalker must intend "to cause serious [stalking effects]", ie, intent must actually be proved. Knowledge by the stalker of the likelihood of stalking effects occurring as a result of the conduct is not sufficient, although a finding of knowledge would tend to infer a finding of intention. Constructive knowledge is not sufficient either. This creates problems when prosecuting an "erotomaniac" stalker. An erotomaniac believes that he or she loves the victim and does not necessarily intend to harm the victim. This is not a major drawback, however, as the incidence of erotomania is very low.[23]

Nature of the stalking effect

Unlike Queensland, other State jurisdictions do not require that the harm threatened by the stalker be "serious".[24]

Provisions such as those in Western Australian, Northern Territory, South Australian, Tasmanian and Victorian legislation, are more loosely drafted than the Queensland provisions, in that they simply specify "apprehension or fear"; not apprehension or fear of violence, for example.[25]

Only Queensland and Western Australian legislation refers to the preventing or hindering of an act that the victim is entitled to do or the compelling of an act that the victim is entitled not to do.[26]

In summary, Queensland's stalking legislation is liberal in comparison to those of the other States and Territories because Queensland does not require proof of intent to cause a stalking effect or proof of actual harm. The apprehension or fear, however, must relate to "violence" and any mental, psychological or emotional harm suffered must be "serious".

4 The phenomenon of cyber-stalking

Cyberstalking shares attributes with traditional forms of stalking in that it incorporates persistent behaviours that instil apprehension and fear.[27] There is a perception that cyberstalking is not truly threatening because there is no direct personal contact, however, the unseen and unknown menace can be far more potent than the known danger, just as with real life stalking.[28]

There are three main types of cyberstalking: e-mail stalking, internet stalking and computer stalking and each will be considered in turn.

4.1 E-mail stalking

E-mail stalking constitutes direct communication from the stalker to the victim through e-mail. It resembles some traditional stalking behaviours. As a medium, e-mail incorporates the immediacy of a phone call and introduces the degree of separation entailed in a letter.[29]

E-mail stalking tactics include sending:

- unsolicited obscene or threatening e-mails;
- viruses;
- high volumes of electronic junk mail (spamming); and/or
- long e-mail messages that tie up the victim's system by consuming its computer memory (mail bombing).

An e-mail address is traceable but many stalkers use "anonymisers" and anonymous "remailers" to shield their identity. The stalker may also use different screen names and may provide bogus personal details to the ISP[30] when registering the e-mail address.[31]

SMS (Short Message Service) on mobile phones is yet another new avenue of e-mail-style stalking which may be used by a cyberstalker.

4.2 Internet stalking

Internet stalking is of a more public nature than e-mail stalking. It utilises the large number of computers connected to the network. Internet stalking can be used to slander and endanger victims and it often spills over into "real life" stalking.

Internet stalking practices include:

- impersonating the victim, disclosing the victim's personal details and inviting unwelcome personal attention, both through the internet and in real life. This may be done by posting an inflammatory message to a bulletin board so that the victim will be deluged with abusive messages from other computer users. The sending of the abusive messages is known as "flaming"; and
- creating a web page monitoring or defaming the victim.[32]

4.3 Computer stalking

Computer stalking is the unauthorised control of another person's computer.[33] The stalker exploits the workings of the internet and the Windows operating system in order to assume control over the victim's computer. This is a direct computer-to-computer link, not by way of an ISP.[34] The cyberstalker can communicate directly with the victim as soon as the victim's computer connects in any way to the internet.[35] Sophisticated cyberstalkers can carry out "keystroke logging" and real-time surveillance of the victim's use of the computer.[36] Electronic theft of stored information is also possible.

The qualities that have made e-mail and the internet so successful and accessible to millions also offer the cyberstalker many advantages over traditional stalking. These qualities include:

- anonymity;
- low cost;
- threats can be sent electronically from anywhere in the world[37];
- free e-mail and chat rooms provide a massive pool of potential victims[38];
- communication is very fast and can involve multiple recipients at any one time;
- third parties can be encouraged to harass or threaten a victim[39];
- programs can be written to send messages at regular or random intervals without the cyberstalker being physically present at the computer terminal;
- password and privacy safeguards are not infallible[40];
- communications can be intercepted[41]; and
- personal information such as silent phone numbers, photographs, and addresses can be tracked down at web sites designed for that purpose[42].

The decentralised nature of the internet makes statistical analysis of the prevalence of cyberstalking problematic. A comprehensive study has not yet been undertaken in Australia. The United States Department of Justice estimated as at January 2000 that there were over 60,000 cyberstalkers operating in the United States.[43] It is logical to expect that the incidence of cyberstalking will continue to rise in both the United States and Australia along with the use of computers and the internet.

5 Legislative responses to cyberstalking

Some commentators argue that internet-based technologies have created entirely new types of stalking requiring specific legislative responses.[44] Other commentators contend that existing stalking legislation can be adapted to remedy what is merely a modern form of commonplace criminal behaviour.[45] Most legislation already covers scattered aspects of cyberstalking based on a liberal interpretation of the relevant provisions. Nevertheless, there are educative and practical advantages in making the prohibition explicit.[46]

The argument for a separate cyberstalking offence implies that cyberstalking's reliance on computer technology makes it something very different to traditional stalking. It is true that cyberstalking bears little physical resemblance to traditional stalking methods such as following and loitering. All the same, the emphasis of a stalking offence is on conduct and the state of mind of the victim or stalker, not the technology used to carry out that conduct.

If existing stalking legislation is to be amended, the real challenge is to draft provisions encompassing incidents of stalking made possible by today's

technology, and, as far as possible, tomorrow's technology.

The best approach for Queensland is to enlarge upon the existing list of "stalking acts" in the *Criminal Code*. This was in fact done in 1999.[47] The 1999 amendments did not, however, make major practical changes to the offence of stalking as it was enacted in 1993. Victoria is the only other Australian jurisdiction to make similar amendments.[48]

6 Is Queensland's response to cyber stalking adequate?

The 1999 amendments to the *Criminal Code* attempted, amongst other things, to address cyberstalking. This part of this article examines the application of the amendments to cyberstalking and analyses their effectiveness.

6.1 "Intentionally Directed at a Person" (section 359B(a))

This element of the offence allays fears of indiscriminate use of the "reasonable victim" test. It should be retained as an effective defence against prosecution of "accidental stalking".

6.2 Conduct (section 359B(b))

Conduct consists of two or more stalking acts or a protracted stalking act. Complications arise regarding the ability of the cyberstalker to have agents, both human and mechanical, perform stalking acts on his or her behalf.

Consider the following scenarios:

Scenario 1: A stalker impersonates a victim in a chat room disclosing her residential address and stating that she fantasises about being raped. The victim is approached by men at her home on six different occasions seeking sexual activity. (an actual case)

Scenario 2: In late 1997, a stalker impersonates a victim on a bulletin board disclosing the victim's name and e-mail address, stating that "Princess Diana got what she deserved". The message is copied and e-mailed all over the world. The victim is "flamed" with thousands of messages including some detailed death threats.

Both of these scenarios are examples of internet stalking. They do not fall directly within section 359B(c)(ii) because the stalker has not contacted the victim by way of e-mail or through the use of any technology. The people incited to harass the victim can not be guilty of stalking if they only harass her once and their conduct is not protracted.

It is submitted that the stalker would still be liable through the counselling and procuring provisions of the *Criminal Code*[49], even if the flamers were innocent agents in regard to the stalking offence.[50] A conviction of counselling or procuring the commission of an offence entails the same consequences in all respects as a conviction of committing the offence.[51] The stalker's conduct may also fall within section 359B(c)(vi) as being an intimidating, harassing or threatening act.

Scenario 3: A stalker activates a computer program that sends random threatening messages to the victim. The victim receives an indefinite stream of threatening e-mails.

The issue in this scenario is whether the stalker can be guilty of stalking when only one act was performed personally. It is submitted that a wide interpretation should be taken of "conduct" and "contacting" so that each sending of a message is seen as a stalking act or one part of protracted conduct arising from the initial stalking act.

Also, there is no doubt that each message is intentionally directed at a person.

One stalking act under the West Australian legislation is "to repeatedly cause the person to receive unsolicited items"; such as pornographic magazines or gifts.[52] Queensland does not have an equivalent provision. A possible addition to the Queensland legislation to deal with this aspect of cyberstalking could be to add words to the effect of:

> *causing a person to repeatedly receive unsolicited communications, including for example, by telephone, mail, fax, e-mail or through the use of any technology.*

This provision would cover both the human and mechanical agency situations in scenarios 1, 2, and 3 and it is more direct than the counselling and procuring provisions.

An interesting question arises from the practice of flaming. If the flamers indulge in only one stalking act each, they can not be guilty of stalking, unless they are acting in concert with each other.[53] If ten flamers e-mailed each other and agreed to send one death threat each to a hapless victim, they could all be charged with stalking under the *Criminal Code's* collective liability provisions.[54] If, however, flamers are unaware or unsure of the activities of other flamers, it would be difficult to use the same provisions. Recourse could lie against the original stalker pursuant to the proposed provision on the previous page. Underlying all these possibilities is the practical difficulty of proving a common enterprise and identifying all the offenders.

6.3 Stalking Acts (section 359B(c))

In 1999, the "contact" paragraph from the stalking act list was changed from "telephoning or otherwise contacting another person" to:

> *contacting a person in any way, including, for example, by telephone, mail, fax, e-mail or through the use of any technology;*[55]

The reference to cyberstalking in this provision compels courts and police to take it seriously. It specifically names e-mail and is an effective response to e-mail stalking.

Gene Barton, an American commentator, has criticised this approach, stating that, "merely adding electronic communication provisions to anti-stalking statutes does not adequately address the scope of e-mail harassment. Such a construction would not proscribe single incidents of anonymous, obscene, or threatening e-mail, or such abuse as mass flaming or letter bombs. The very essence of anti-stalking statutes requires repeated contact".[56]

The views of this commentator should not be acted on for two reasons:

- A "harassment" provision covering single incidents of abuse would tend to involve less serious conduct than stalking and should be considered as an issue distinct from stalking.
- A tailored "e-mail harassment" statute should be avoided as the trend in Australia is towards technological neutrality.[57] The emphasis should be on the conduct rather than the means for carrying out that conduct.

Section 359B(c)(ii) does not apply to internet and computer stalking where direct contact does not occur. It is arguable that sections 359B(c)(vi) and 359B(c)(vii) could apply instead.

It has been suggested that terms such as "loitering", "watching", and "where a person visits" could be applicable to cyberspace.[58] It is submitted that the ordinary meanings of these words should not be stretched to cover cyberstalking thereby avoiding fruitless legal argument. A better option might be including language to the effect of:

Section 359B(ca):

> *(i) a reference to an "act" in subsection (c)(vi) or subsection (c)(vii) of this section includes an act carried out through the use of any technology*
>
> *(ii) a reference to "watching" in this section includes a reference to watching or surveillance carried out through the use of any technology.*

The use of the word "surveillance" would require consideration of whether auditory "bugging" should also be included in this paragraph.

6.4 Stalking Effects (section 359B(d))

Despite the concerns of the MCCOC report[59], it is submitted that the focus on the victim's state of mind is appropriate. Due to the highly contextual nature of the stalking acts, a consideration of the objective effect on the victim is warranted. Furthermore, considering the effect on the victim means that an erotomaniac will quite rightly be caught by the provision.

Appropriate results using the Queensland method depend upon a rational evaluation of the relevant circumstances and what the reasonable victim would have experienced in those circumstances. If the stalker appears to lack specific intent this may be relevant to sentencing or to an evaluation of the stalker's sanity.

It is commonly assumed that cyberstalking is not as serious or harmful as real world stalking. It is also believed that the anonymity and impersonality of computers causes people to be less inhibited. While people who fall into this category might become liable for doing something they would not do in real life, the focus should remain on the reasonable victim rather than the specific intent of the stalker. Expressly prohibiting cyberstalking through legislation will assist in raising awareness of its unacceptable nature.

An MCCOC report on Damage and Computer Offences[60] considers cyberstalking and whether liability should be extended beyond conduct intended to induce fear or injury so as to include harassment intended to induce fear of other kinds of harm such as annoyance, embarrassment, shame and resentment. The report dismisses this idea and criticises the breadth of the definition of "harassment" in the *Protection from Harassment Act* 1997 (UK).

Cyberstalking legislation should correspond with stalking legislation as closely as possible. It should not be taken as an opportunity to surreptitiously criminalise behaviour less serious than stalking. If legislation to criminalise other behaviour is needed, then it ought to be discussed as a separate issue and dealt with in an appropriately technology-neutral way.

6.5 "Detriment"

One of the terms comprising the definition of stalking effects is "detriment" that reasonably arises in all the circumstances to the victim or another person.[61]

"Detriment" is defined in section 359A:

> *"'detriment' includes the following -*
>
> *(a) apprehension or fear of violence to, or against property of, the stalked person or another person;*
>
> *(b) serious mental, psychological or emotional harm;*
>
> *(c) prevention or hindrance from doing an act a person is lawfully entitled to do;*
>
> *(d) compulsion to do an act a person is lawfully entitled to abstain from doing."*

The requirement for "serious" mental, psychological or emotional harm in paragraph (b) of the definition is appropriate. Harm which is less than serious, such as annoyance, should not be caught by the stalking provisions. The tort of nuisance would be a more appropriate avenue for this sort of harm.

6.6 "Prevention or hindrance from doing an act"

Detriment can consist of preventing or hindering the victim from doing an act that the person is lawfully entitled to do. Liability is very wide under this part of the definition. The act that the victim is prevented or hindered from doing could include real or virtual acts. For example, detriment could be constituted by the victim being prevented from sending an e-mail at a particular time.

6.7 "Violence to property"

"Violence" is defined in section 359A:

> *"'violence' -*
>
> *(a) does not include any force or impact within the limits of what is acceptable as incidental to social interaction or to life in the community; and*
>
> *(b) against a person includes an act depriving a person of liberty; and*
>
> *(c) against property includes an act of damaging, destroying, removing, using or interfering with the property."*

A fear or apprehension of violence to property includes a fear or apprehension of property being damaged, destroyed, removed, used or interfered with. A cyberstalker may be able to delete hard drive files of the

victim. If it is argued that the victim would apprehend that these files will be *destroyed*, it is necessary to prove that the information in the files constitutes property as that is what would be destroyed (unless the files were essential to the operation of the computer). It would be easier to argue that the victim would apprehend an *interference* with the computer itself, namely the alteration of the magnetic configuration of the hard drive. It is an open question whether copying of files or surveillance by keystroke logging could amount to interference. Such actions could breach section 408D (Computer Hacking and Misuse) of the *Queensland Criminal Code* and for that reason may be more likely to be an "intimidating, harassing, or threatening act".

A pending Texan case[62] against Yahoo! Inc. involves the use of "cookies" as a method of stalking. Chalkboardtalk.com alleges that it has been stalked by Yahoo!Inc through its use of cookies. Cookies are implanted by web servers onto personal computers in order to allow a company to build a personal profile of any particular user viewing that company's web page. Cookies use the processing power of the personal computer and result in the storing of information on that computer. If a victim is aware that cookies are being used by a particular company, he or she may apprehend that cookies will be used by the same company in the future. If the cookie is held to involve "use" of or "interference" with the victim's computer, this could support a charge of stalking under Queensland law. Issues of notice or implied consent would be relevant but it would seem illogical for this sort of activity to be categorised as "stalking" and for this reason, it may be prudent to amend the definition so that the damage, destruction, removal, use or interference must be of a "serious" nature.

6.8 Circumstances

The Queensland legislation requires that the fear, apprehension, or detriment of the victim must be "reasonable in all the circumstances". The definition of the circumstances that must be considered by the court under section 359A includes not only the circumstances surrounding the unlawful stalking but also the circumstances of the stalked person known, foreseen or reasonably forseeable by the alleged stalker.

This is a useful definition if the location of the stalker was unknown to the victim as it is reasonable to expect that the victim would have apprehended the possibility that the stalker was in close physical proximity. Therefore, even if the stalker were thousands of kilometres away, this fact should not detract from the victim's objective sense of fear as the victim simply did not know the truth.

Similarly, if the stalker pretends to be five different people or represents incorrectly that she is a man, the victim's reasonable perspective may be a circumstance lending weight to a finding of reasonable fear or apprehension.

No other Australian jurisdiction expresses these considerations in such a clear and concise way.

6.9 Immaterial Factors

Section 359C(1)(a) provides that it is immaterial whether the stalker intends that the victim be aware the conduct is directed at the victim. If the stalker deleted files on the victim's hard drive on two or more occasions and intended the victim to think it was a computer malfunction, the stalker would still have committed an offence. The stalker would have caused a detriment to the victim in that the victim is prevented from accessing the files. The examples given for "prevention or hindrance" in paragraph (c) of the definition of "detriment" involve acts consciously avoided by the victim in response to the stalking.[63] There is, however, no requirement that the act "prevented or hindered" be done with awareness of the stalker's conduct.

Section 359C(1)(b) provides that it is immaterial whether the stalker has a mistaken belief about the identity of the person at whom the conduct is intentionally directed. This might be a mistaken belief about the victim's gender or age. In the e-mail world, one can not see the recipient. It is often the case that the sender has no idea who, if anyone, will read the message sent or whether the address is functioning. If a person sends an e-mail to an e-mail address, it is difficult to argue that that is conduct intentionally directed at a person until that person has reason to believe that someone is reading the e-mail. On balance, though, the question must be asked why anyone would send an e-mail if it was not intended to be read. A mistaken belief that there was no identity would be unlikely to be believed.

Scenario 4: John has a robust relationship with his little brother. He sends brief messages to his little brother at *ashley123@yahoo.com such as "I'm going to enjoy punching your head in" which are not meant to be taken seriously and are not, in fact, taken seriously. John does not know that his brother's e-mail address is actually ashley122@yahoo.com and that he has been sending messages to a frightened elderly lady.*

John's e-mail is intentionally directed at a person of whom he has many mistaken beliefs. In this situation, the lack of a specific intent provision may lead to a harsh result. Possible negligence amounts to criminal liability. It is tempting to argue that a total mistaken belief of the recipient's identity should be material, but this could benefit the crank caller who calls the wrong person by mistake.

6.10 Exceptions to Unlawful Stalking

Section 359D(d) states that unlawful stalking does not include reasonable conduct engaged in by a person for the person's lawful trade, business or occupation. This exception provides important protection for sales people who market by way of e-mail - for example, a seller of lawful pornographic material.

Sections 359D(b) 359D(c) make an exception for acts done for the purposes of genuine industrial disputes and genuine political or public disputes carried on in the public interest. The MCCOC report on Non Fatal Offences Against the Person[64] disparaged the fact that "the scope of operation of such a serious criminal offence should be limited only by such a vague exception". It also questioned whether investigative journalists, heritage protesters or anti-abortion

protesters would come within the public interest exception.

E-mail campaigns are a popular form of protest, encouraged by organisations such as Amnesty International and anyone with an "axe to grind" against the government. Should there be a point at which an act is so offensive that it cannot be said to be part of a genuine dispute? The meaning of the word "reasonable", if it were to be used, would be hotly debated in the context of picketing and environmental issues.

The main defence to harassment in the *Prevention from Harassment Act* 1997 (UK) is "reasonableness".[65] It has caused uncertainty in the application of the law. The exceptions in Queensland are only marginally better than reasonableness.

It is submitted that the exceptions should not be interpreted in a restrictive manner. Stalking legislation did not arise in order to halt such protests. Other offences in the *Criminal Code* may be of more assistance to the prosecution, such as section 408D (Computer Hacking and Misuse).

7 Other matters

Other legal avenues may be open to a victim of cyberstalking. These include criminal prosecutions for threats[66], threats of violence[67] written threats to murder[68], computer hacking and misuse[69] or extortion[70]. On the civil side, the torts of defamation and nuisance may be applicable.

A major issue in the general area of computer crime is determining jurisdiction for crimes involving multiple jurisdictions, both inter-state and international. This paper does not deal with this complex issue.[71]

8 Conclusion

Cyberstalking is a serious social problem requiring an adequate legislative response. The amendments to the *Queensland Criminal Code* in 1999 made significant changes to the stalking offence and directly addressed cyberstalking for the first time. It is believed that amendment of the stalking provisions was the correct action to take and that technology-specific legislation applying beyond the bounds of stalking behaviour should not be pursued. The focus on the reasonable victim as opposed to the intent of the stalker is commendable and practical, however, harsh results may arise in some circumstances.

The amendments deal effectively with e-mail stalking. The application of the provisions to internet stalking and computer stalking, however, is not as successful and while the sweeper clauses are widely drafted, specific reference should be made to acts carried out with new technology.

In summary, Queensland's stalking provisions are better equipped to protect against cyberstalking than the corresponding provisions of the UK and other Australian States and Territories although improvements taking into account the nature of computers and the internet are desirable.

---

1 The term "stalker" is used as a general term to cover a person carrying out stalking-style behaviour regardless of whether that person has been charged or convicted of a criminal offence. The use of the term "victim" denotes a recipient of stalking-style behaviour regardless of the effect on that person.

2 M Goode, "Stalking: Crime of the Nineties?" (1995) 19 Criminal Law Journal 21 at 24 (the words "repeated or protracted" have been added for the purpose of this paper)

3 Stalking behaviours as identified by legislation shall be known collectively as "stalking acts" for the purpose of this paper.

4 US Attorney-General, Report on Cyberstalking: A New Challenge For Law Enforcement and Industry (1999) at 3, <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm> (10 July 2001)

5 A Radosevich, "Thwarting the Stalker: Are Anti-Stalking Measures Keeping Pace With Today's Stalker?" (2000) University of Illinois Law Review 1371 at 1372

6 R Lee, "Romantic and Electronic Stalking in a College Context" (1998) 4 William and Mary Journal of Women and Law 373 at 393 (relevant existing offences usually required an explicit threat)

7 Californian Civil Code section 1708.7

8 Criminal Law Amendment Act 1993 (Qld) inserted Chapter 33A in the Queensland Criminal Code

9 Criminal Code (Stalking) Amendment Act (Qld) 1999

10 section 359B(a) Queensland Criminal Code

11 eg threats: section 359 Queensland Criminal Code

12 The term "stalking effects" is used to cover a multitude of terms from various stalking statutes including fear, apprehension, harm, injury and detriment.

13 except for the intention to direct the conduct at a person

14 R Swanwick, "Stalkees Strike Back - the Stalkers are Stalked: A Review of the First Two Years of Stalking Legislation in Queensland" (1996) 19 University of Queensland Law Journal 26 at 27

15 section 70 Queensland Criminal Code

16 section 75 Queensland Criminal Code

17 section 308 Queensland Criminal Code

18 note 14 at 40

19 section 359C(4) Queensland Criminal Code

20 section 338E Criminal Code Act 1913 (WA)
section 189 Criminal Code Act 1997 (NT)
section 562AB Crimes Act 1900 (NSW)
section 192 Criminal Code Act 1924 (TAS)
section 34A Crimes Act 1900 (ACT)
section 21A Crimes Act 1958 (VIC)
section 19AA Criminal Law Consolidation Act 1935 (SA)

21 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General Model Criminal Code, Report: Chapter 5, Non Fatal Offences Against the Person (1998) at 55

22 The maximum term of imprisonment is seven years if certain aggravating circumstances are found to exist: section 359E(3) Queensland Criminal Code

23 J Merschman, "The Dark Side of the Web: Cyberstalking and the Need For Contemporary Legislation" 24 Harvard Women's Law Journal 255 at 263

24 section 338E Criminal Code Act 1913 (WA)
section 189 Criminal Code Act 1997 (NT)
section 562AB Crimes Act 1900 (NSW)
section 192 Criminal Code Act 1924 (TAS)
section 34A Crimes Act 1900 (ACT)
section 21A Crimes Act 1958 (VIC)

25 section 338E Criminal Code Act 1913 (WA)
section 189 Criminal Code Act 1997 (NT)
section 19AA Criminal Law Consolidation Act (SA) 1935
section 192 Criminal Code Act 1924 (TAS)
section 21A Crimes Act 1958 (VIC)

26 section 359A Queensland Criminal Code
section 338D Criminal Code Act 1913 (WA)

27 E Ogilvie, "Cyberstalking" (2000) *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice* at 1

28 note 14 at 36

29 note 27 at 2

30 Internet Service Provider

31 note 5 at 1380

32 A Seymour, M Murray et al, *National Victim Assistance Academy Text* (2000) at 3,<http://www.ojp.usdoj.gov/ovc/assist/nvaa2000/academy/welcome.html> (30 July 2001)

33 note 27 at 2

34 note 27 at 3

35 note 27 at 4

36 note 27 at 4

37 note 4 at 3

38 note 27 at 2

39 note 4 at 3

40 A Davidson, "Stalking in Cyberspace" (2000) 20(4) *Proctor* 31

41 note 40 at 31

42 note 40 at 31; note 7 at 395:There is even a stalkers' home page at http://www.glr.com/stalk.html,

43 note 32 at 2

44 G Barton, "Taking a Byte Out of Crime: E-mail Harassment and the Inefficacy of Existing Law" (1995) 70 *Washington Law Review* 465 at 469
45 note 27 at 1 and 4; E Ross, "E-mail Stalking: Is Adequate Legal Protection Available?" (1995) 13 *John Marshall Journal of Computer and Information Law* 405 at 413
46 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Model Criminal Code, Report: Chapter 4, Damage and Computer Offences* (2001) at 99
47 note 9
48 This can be seen in section 21A(2)(b) of the Crimes Act 1958 (VIC)
49 section 7(1)(d) and section 7(2) *Queensland Criminal Code*
50 see section 7(4) *Queensland Criminal Code*
51 section 7(3) *Queensland Criminal Code*
52 section 338E *Criminal Code Act* 1913 (WA)
53 note 44 at 467
54 note 46 at 99; section 7 (aiding a principal offender), section 8 (Offences committed in prosecution of a common purpose) *Queensland Criminal Code*
55 section 359B(c)(ii) *Queensland Criminal Code*
56 note 44 at 469
57 as exemplified by the *Copyright Amendment (Digital Agenda) Act* 2000 (Cth) and the *Electronic Transactions Act* 1999 (Cth).
58 note 23 at 267
59 note 21
60 note 46 at 98
61 section 359A *Queensland Criminal Code*
62 *Stewart v Yahoo! Inc.* Case No. 0001045I, 162nd Civil District Court, Dallas, Texas; discussed in J Selby, "Yahoo! accused of stalking" (2000) 41 *Computers & Law* 28
63 "a person no longer walks outside the person's place of residence or employment"; "a person significantly changes the route or form of transport the person would ordinarily use to travel to work or other places": section 359A *Queensland Criminal Code*
64 note 21
65 section 4(3) *Protection from Harassment Act* 1997 (UK)
66 section 359 *Queensland Criminal Code*
67 section 75 *Queensland Criminal Code*
68 section 308 *Queensland Criminal Code*
69 section 408D *Queensland Criminal Code*
70 section 416 *Queensland Criminal Code*
71 see Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Model Criminal Code, Discussion Paper: Chapter 4, Damage and Computer Offences* (2000)

New domain name policy for Open 2LDs (Australia)

auDA, the Australian domain name administrator, has approved new Domain Name Eligibility and Allocation Policy Rules for Open Second Level Domains (**2LDs**) which are expected to come into force on 1 July this year.

The new domain name policy has been drafted by auDA to reflect the recommendations of the report published by its Name Policy Advisory Panel in April 2001 called *Review of Policies in .au Second Level Domains: Recommended Changes to Domain Name Eligibility and Allocation Policies in the .au Domain Space.*

Open 2LDs include com.au, net.au, asn.au, org.au, id.au. Open 2LDs are basically open to all users, subject to some eligibility criteria. The new policy rules do not cover closed 2LDs which are those with a defined community of interest, such as edu.au and gov.au.

The current domain name policy for the registration of com.au and net.au names allows registrants with a company, business, partnership, trading, incorporated association or commercial statutory body name to register that exact name, or an acronym or abbreviation of that name. A registrant can currently only register one domain name per business name, company name etc. Under the new policy, registrants will also be eligible to register a domain name based on their Australian registered trade mark (or on a trade mark application). Further, a registrant will be able to register a domain name which is 'closely and substantially connected' to themselves. For example, it may be possible to register a domain name which refers to:

- a product that the registrant manufactures or sells;
- a service that the registrant provides;
- an event that the registrant organises or sponsors;
- a teaching, training or facilitation activity by the registrant;
- a venue that the registrant operates; or
- a profession in which their employees are engaged.

The new policy provides that there will be no hierarchy of rights in the new domain name system. For example, a registered trade mark will not confer any better entitlement to a domain name than a registered business name. Provided the relevant eligibility rules are satisfied, the first registrant to apply for a particular domain name will be permitted to license it.

The new policy also affects the org.au domain (used for non-profit and other organisations, statutory authorities and other entities that can reasonably be considered to be organisations) and the asn.au domain (used for incorporated associations, some unincorporated bodies, political parties, trade unions, industry bodies and sporting or special interest groups). The eligibility criteria for these domains have been widened to include not only domain names which exactly match the name of the organisation, but also names which are 'closely and substantially connected' to the registrant.

More details can be found on the auDA website, http://www.auda.org.au/about/news/2002061102.html.

Belinda Justice, Editor and solicitor in Freehills' Corporate and Technology Group.