Harassment through the Digital Medium
A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking

Warren Chik
Assistant Professor of Law
Singapore Management University School of Law
LLB (Hons) NUS, LLM (IBL) University College London, LLM (ICL) Tulane University
Advocate & Solicitor (Singapore), Solicitor (England & Wales), Attorney & Counsellor at Law (New York)

Abstract. The cyber world is an extension of the real world. It is another dimension where we can work, study and play. But people also tend to lose their inhibitions on the Internet, often while keeping their anonymity. Because of the perceived and real freedoms in the digital environment, people are emboldened to act in ways that they may not normally do in the real world. One recent phenomenon that is steadily becoming a problem in every country with a high level of electronic connectivity is the act of cyberstalking. The electronic medium is an important factor due to its very nature such as low cost and ease of use, potential anonymity and stealth as well as the insignificance of physical distance to the act of cyberstalking. Hence, cyberspace affords lesser impediments to aggressive behaviour. The borderless nature of electronic communications medium, concomitant jurisdictional concerns and the unique challenges posed to computer forensics such as the collection of evidence and investigations also arise as relevant issues in this context. Cyberstalking has become a concern that has translated into law in larger and more technologically-matured jurisdictions such as the United States, the United Kingdom, Canada, Australia, Japan and even in a small country like Singapore. Existing laws relating to harassment or intimidation are often fact- or relationship- specific and are inadequate to meet the needs of modern society, while nascent cyberstalking laws are substantively disparate. I will first use Singapore as a case study and backdrop by presenting the factual experience and judicial developments in Singapore relating to cyberstalking and identify some of the usual problems in its treatment under law. I will then analyse and compare the cyberstalking laws of several key jurisdictions to determine the common elements and treatment amongst them with a view to the formulation of a proposed statutory solution that will take into consideration the different rights and interests of members of society in the use of digital media for social interaction. I will also briefly consider the issues of prescriptive, adjudicatory and enforcement jurisdiction and the need for greater international cooperation to deal with the problem through the harmonisation of substantive laws, the coordination in procedural investigative measures and complementary recognition and enforcement laws.

1. Introduction: Issues in Cyberstalking

Every breath you take, Every move you make,
Every bond you break, Every step you take, I'll be watching you.
Every single day, Every word you say,
Every game you play, Every night you stay, I'll be watching you.

The Police
Every Breath You Take

The cyber world is an extension of the real world. It is another dimension where we can work, study and play. The benefits are tremendous; in particular advances in information technology have enabled a whole new medium of electronic messaging without the hurdles of cost, time and effort that we face in the physical realm. On the Internet, people also tend to lose their inhibitions.[1] They create avatars for online gaming and online personas. Sometimes identities are revealed, but sometimes anonymity is kept. Particularly in the latter case, it emboldens people to act as they may not normally do offline.[2] That is where problems emerge in the virtual realm that has real world consequences.

Why is online stalking more of a problem than offline stalking? Before proceeding to consider the issue, it must be emphasized that whether it is performed online, offline or both, the acts that amount to stalking behaviour are the primary concern. However, the medium is also important for its many implications. First, the ease of use and hence lesser impediments to aggressive behaviour;[3] second, the borderless nature of electronic communications medium and concomitant jurisdictional concerns; third, the type of evidence and means of its collection; fourth, the lack of educative and deterrent effect of current laws; and fifth, the lack of effective laws, or of any law at all, to deal with the problem in some countries and in the international fora.[4]

Cyberstalking has become a concern that has translated into law in larger jurisdictions with more matured technological infrastructure such as the United States, the United Kingdom, Canada, Australia and Japan.[5] Although Singapore is geographically small, its 'virtual geography' is borderless. This is due to the high density in electronic and telecommunications connectivity, increasingly sophisticated and technologically savvy users, and the low cost of subscription to the Internet, cellular and other static and mobile forms of electronic and digital forms and channels of communication. Although this may not necessarily translate into a greater number of stalking behaviour within the country, and even though there are no official statistics to show that there has been such an increase, the fact remains that there is a greater likelihood of, and a conducive IT infrastructure and computing environment for, such anti-social harassing behaviour to perpetrate.

There is already evidence of such acts in recent cases that have gone to the local courts, although they have been resolved on other bases of law such as through computer misuse legislation or common law such as the tort of harassment. Although they may have indirectly provided some temporary solution to the problem, it will be demonstrated how they are neither comprehensive nor definitive or unambiguous enough in their application. They are also indirect and the criminal punishments or civil redress as the case may be may not be appropriate. Other existing laws relating to harassment or intimidation are fact- or relationship- specific, and are thus also inadequate to meet the needs of modern society.[6]

In Part 2 of this paper, I will consider the current coverage under Singapore law and show why and how it is inadequate to meet the needs of every victim of stalking, and in particular, cyberstalking. In Part 3, I will make a comparative analysis of the laws in various jurisdictions to see how other countries have dealt with the problem in order to draw lessons from them and also to highlight the rights and interests that have to be considered and balanced in formulating a legislative provision to deal with it. Suggestions will be made as to the appropriate approach in both form and substance to cyberstalking legislation. In Part 4, I will examine what is required in relation to the laws on digital evidence and computer forensics. In Part 5, I will consider the appropriate measures and punishments or redress to deal with stalkers. In Part 6, I will highlight the need for public education in technology and in the gathering and preservation of evidence, and the need to develop technological expertise in law enforcement agents. I will also briefly highlight the issue of prescriptive, adjudicatory and enforcement jurisdiction and the need for international cooperation through the harmonization of laws, in the coordination of procedural investigative efforts, and in recognition and enforcement laws.

2. Cyberstalking in Singapore: Emerging Problems in a Rapidly Digitised Society, the Search for a Solution and the Limitations of Current Laws

2.1. Lack of Comprehensive Coverage

Faced with problems of threatening or unwanted electronic communications, the question arises as to whether cyberstalking as a phenomenon is adequately addressed under the law. Harassment laws to an extent provide for some recourse, but it is not sufficient to address the needs of the individual in a digital environment, not least because such laws are piecemeal and too specific. Current harassment laws can be divided into three categories: Harassment and/or intimidation laws, which are often relationship specific or situational/contextual and those that are generally applicable.

2.2. General

In Singapore, sections 13A and 13B of the Miscellaneous Offences (Public Order and Nuisance) Act (Cap. 184) (MOA),[7] make it an offence for a person to use "threatening, abusive or insulting" words and behaviour with the intent to cause harassment, alarm or distress. However, based on legislative history, they appear only to cover *inter-praesentes* behaviour and not to electronic communications where the parties are physically removed.[8] They also do not cover other forms of behaviour which should also constitute harassment and which are typical to stalking behaviour such as sending messages or gifts, following or tailing someone and conducting electronic or physical surveillance on someone. Moreover, they do not take into account the fact that even without bad intentions,such conduct can have a negative effect on the victim and even on society. There are social concerns

relating to the act of stalking, particularly in the virtual context, which are not addressed by this legislation, which include the infringement of privacy (i.e. the right to be left alone or right to solitude) and peace.

At the turn of the millennium, the case of *Malcomson Nicholas Hugh Bertram & Anor v. Naresh Kumar Mehta*[9] was brought before the Singapore High Court. It involved an ex-employee harassing his ex-employer and company staff *via* electronic mail, SMS messages, telephone calls and postal mail. It was in this case that the then Judicial Commissioner Lee Seiu Kin first recognized the tort of harassment in Singapore by defining it as "a course of conduct by a person, whether by words or action, directly or through third parties, sufficiently repetitive in nature as would cause, and which he ought reasonably to know would cause, worry, emotional distress or annoyance to another person".[10] However, he gave the caveat that the definition is not meant to be exhaustive but was valid to the extent that it "sufficiently encompasses the facts of the present case in order to proceed with a consideration of the law".[11] An injunction was given to restrain the ex-employee from continuing his acts on the basis of harassment as well as on the basis of trespass and nuisance.[12]

Malcomson v. Mehta itself is inadequate to address stalking cases, in particular cyberstalking, for several reasons. First, Lee JC postulates only a general rule which is sufficient for the case in question; hence it suffers from ambiguity, being the only case so far on the subject. Second, victims take civil action only as a last resort because of the time, cost and effort involved in collecting evidence and mounting such cases.[13] Third, the remedies involved do not address the root cause of most cases of stalking and cyberstalking that involves people with psychological problems and for whom other measures, such as mental assessment, treatment and counseling, may be more appropriate.

However, it is to be noted that the tort of harassment as enunciated by Lee JC is established on the basis of the foreseeability of the effect of acts or words on the mental state of the victim, even if it were an just an annoyance. This will be important later when we look at the legislative approaches in other countries and in my recommended definition and scope of the cyberstalking law.

A case which illustrates how a form of stalking is dealt with under an existing criminal legislation that may not always be an available recourse, and that is not enacted to deal with such problems specifically, is if the acts in question involves the unauthorized use or interception of computer services, or the obstruction of the use of a computer, which can constitute an offences under the Computer Misuse Act (Cap. 50A) (CMA). In the case of *PP v. Lim Siong Khee*,[14] the stalker and the victim were in a short relationship and had gone on a European vacation before the victim called off the relationship. The stalker, in a classic case of the vengeful "former intimate" gained access to the victim's e-mail account without her consent to send messages to her friends detailing their intimate relationship in an attempt to embarrass her. An offence was made out under sections 3, 6 and 7 of the CMA.[15] However, these provisions will not apply in the usual cases of the stalker sending e-mails or other forms of electronic messages to the victim directly or to third parties with the purpose of affecting the victim through indirect means. Also, again the punishment may not adequately address the problem, for example, in the case of obsessive and psychologically disturbed stalkers.

2.3. Relationship

The Women's Charter (Cap. 353) has provisions relating to harassment in the context of domestic or relationship-based violence, specifically for the protection of persons from family members. Section 64 includes the act of harassment with intent to cause or knowing that it is likely to cause "anguish".[16] Sections 65 to 66 then provide for the issuance of protection orders (PO) and expedited orders (EO) to restrain a person from inflicting "family violence".[17] However, these provisions are only protective measures available to "family members".[18] They do not, for example, cater to non-marital or non-family-related relationships.

Similarly, the Moneylenders Act (Cap. 188) (MA) has specific provisions dealing with the harassment or intimidation of a debtor by his or her creditor in the context of a financial loan relationship. Section 33(1) of the Act makes it an offence for any creditor to, directly or indirectly, harass or intimidate his debtor and members of the latter's family or any other person in connection with the loan.[19] In *Chua Keem Long v Public Prosecutor*,[20] the then Chief Justice Yong Pung How noted that the word "harassment" under the MA was undefined and proceeded to look up its definition in a non-legal dictionary. Yong CJ referred to the definition under the New Shorter Oxford dictionary, which defined "harassment" as "[to] trouble by repeated attacks…subject to constant molesting or persecution." Yong CJ was of the view that a series of continuous or repetitious conduct is generally required for harassment, which can be contrasted to the act of intimidation, which can be a single incident. But he then gave the view that a single visit or encounter can still constitute harassment if it is so intense as to amount to a *persistent* attack or persecution.[21]

Under the Miscellaneous Offences (Public Order and Nuisance) Act (Cap. 184), it is an offence to harass public servants in the course of their duty under section 13D.[22]

These legislative provisions were clearly not intended, and are inadequate, to protect other victims of stalkers and of dealing with perpetrators with the profile that we are concerned with. So, for example, cohabitors, ex-partners, ex-boyfriends or girlfriends, neighbours, and secret admirers or other strangers do not qualify. The

behaviour of stalkers can be rational or irrational, they cannot be compartmentalized according to relation or context and is irrespective of race, language, religion, education, age, gender or sexual orientation.[23]

2.4. Situational/Contextual

Sections 13A[24] and 13B[25] of the MOA deals with both intentional and non-intentional words or acts of "harassment, alarm or distress" by a person against another within physical or geographical proximity of that other person. Section 13C deals with acts of harassment where violence is likely to result,[26] while section 14A makes it an offence to make harassing calls to emergency numbers specifically.[27]

These provisions are of limited help specifically to stalking cases as they are limited in scope. For instance, they require face-to-face communications or physical proximity. They also require a heightened level of threat due to the physical closeness of the parties. The words or behaviour have to be "threatening, abusive or insulting" which does not take into account the type of conduct that can be perpetrated in stalking cases, including those that are active such as gift giving[28] and electronic communications, or passive acts such as physical or electronic surveillance. They also relate to direct rather than indirect means of harassment. Section 13A requires specific intent "to cause harassment, alarm or distress to another person", which a delusional or mentally unstable stalker may not possess. Finally, the penalty of a fine of a maximum of $5.000 is hardly adequate deterrence or punishment to stalkers, most of whom are motivated by other than pecuniary goals or act out of emotional wants rather than for rational reasons or by logic.

These provisions may be amended to address the phenomenon of stalking in general, and cyberstalking in particular. However, there are some reasons which counsels against using the MOA as the vehicle for dealing with stalking. First, the provision will end up unwieldy and long, as it already has with the alphabetisation of the current provisions. Second, stalking comprises a range of action (not just present threats or phone calls under sections a3A-C and 14A) that the stalker may engage in over a period of time rather than in an instance (such as that in the current sections 13A-C). Stalking is really concerned with a course of conduct rather than a particular incident which may fall under one of the above offences. The real problem to be addressed is this persistency of conduct as it is this which has such devastating effects on the lives of victims and that also needs to be reflected in the sentencing options. Third, it may not fit in with the objective of the MOA, as the title implies, which generally deals with 'lighter' offences relating to public order and nuisance rather than a serious offence to the person like stalking. Even the current sections 13A-C appears a little out of place in the Act. The better option will be to create new provisions under existing criminal legislation, such as the Penal Code, or even to enact new legislation.

Finally, other offences relating to the effects of stalking are also generally non-preventative and inadequate,[29] except perhaps to some extent for the offences, if proven, of "attempt" and "conspiracy" for instance.

For an overview of the current treatment of harassment laws in Singapore, see Appendix: Table 1.

3. Comparative Analysis of the Laws in Other Jurisdictions: Lessons for a Comprehensive and Effective Solution to Cyberstalking

3.1. Definition and Scope

Cyberstalking can loosely be defined as threatening behavior or unwanted advances directed at another using the Internet and other forms of modern online electronic communications technology.[30] It is a new method of stalking, which in turn is a form of harassment. Cyberstalkers use computers, cell phones, fax machines and other electronic or digital devices to track and pursue their victims.[31] Cyberstalkers are also increasingly sophisticated and can use such diverse technology as global positioning systems (GPS), hidden cameras and malware or spyware.[32] Their motives are just as diverse.[33]

In the American Heritage dictionary, to "stalk" means "[t]o pursue by tracking stealthily" or "[t]o follow or observe (a person) persistently, especially out of obsession or derangement"; and to "harass" means "[t]o irritate or torment persistently" or "[t]o wear out, exhaust".[34] Whatever the factual definition of the words, the legal definition is what counts if recourse to legally enforceable civil and criminal recourse and protective measures are to be available to victims.

For a comparative table of harassment, stalking and cyberstalking, see Appendix: Table 2.

To come up with the definition, and hence the scope of legally actionable stalking (incorporating elements of cyberstalking), we first have to identify the *modus operandi* and decipher the profile of stalkers, paying particular attention to the digital context. Then we have to decide what balance should be achieved between right to privacy and personal space on the one hand and the benefits of social interaction, information flow and freedom of expression and physical movement on the other.[35] Following from that, we have to consider what legislative approach to adopt - a list or general prohibition model. Finally, we have to come up with the most effective solution to the problem.[36]

3.2. *Modus Operandi* of Cyberstalkers

The stalker may know the victim personally or interact with the latter anonymously through an alias on the Internet before starting to cyberstalk, or the parties may be have had a pre-established relationship that have broken down. The stalker may not even have had any contact with the victim at all, such as in the case of a secret admirer (usually in such a case the victim is popular, such as a celebrity or politician). The permutations are endless.

Online users are can be targeted by cyberstalkers in various ways, such as through chat rooms like live chat or Internet Relay Chat (IRC), where a user talks live with other users; message boards, discussion forums and newsgroups, where a user interacts with others by posting and replying to messages; e-mail, where a user can write and attach files to be sent to the victim and even spam the victim; and online impersonation by the theft of the victim's electronic identity or persona.

There are also many different types of stalking involving various actors including third parties. Stalking can be direct or indirect, such as by sending false information or vicious information about the victim to others. It can also be a threat or an actual attack on the victim's computer (e.g. electronic sabotage by sending viruses and worms). It can come in the form of threats made to the victim's person or property or family, friends or loved ones.

See Appendix: Table 3 for an analysis of the various permutations of actors in cyberstalking.

Stalkers can find ways and means to discover or trade a victim's contact information including e-mail address, phone number and even the residential or office address, whether through conventional means such as through a simple web search, the telephone directory or online directory listings for open source information; or they can discovering such information by, for example, deciphering an identity name and password. If the stalker is particularly sophisticated or an expert in computers and digital technology, the stalker can also hack or use other techniques to access the victim's computer and the information stored therein.

Similar to off-line stalking, online stalking can be a difficult experience for victims, placing them at risk of psychological trauma, and possibly even physical harm. Many cyberstalking situations do evolve into off-line stalking, and a victim may experience abusive and excessive phone calls, vandalism, threatening or obscene mail, trespassing, and physical assault.

The modus operandi will be useful in formulating the elements of the offence and finding a reasonable balance to interests as well as when deciding on the appropriate powers to give to the courts, such as sentencing options in criminal cases and civil remedies such as injunctions.

3.3. Policy Considerations Affecting Scope of Cyberstalking

To adequately address the specific problems relating to cyberstalking, the following points must be taken into consideration when tailoring a policy response in law:

1. "Stalking" should address the virtual medium. There is a need to broaden the definition of "stalking" to include electronic communications (overt stalking) and surveillance, monitoring and tracking (covert stalking). The best way to do this is possibly not to even address any one medium, method or form; or to do it illustratively and on a non-exhaustive manner.
2. Motive should be irrelevant. The offensiveness of stalking is unique in that it is the course of action and how it may affect another, rather than the aim, goal or motive that is the problem.[37] Hence, intention should be in relation to the acts that contribute to what is, or is reasonably or likely to affect the victim. The stalker can act based on such diverse motives as love ("borderline/delusional erotomania"), sex ("sex addicts" / "serial rapists"), fame ("celebrity stalker" / "paparazzi"), vengeance ("former intimate" / "enemy"), control ("ego/power tripper"), or other deviance ("sociopaths" / "serial killers").[38]
3. Victim should be identifiable. The threats or attentions must be proven to be directed at the victim as an identifiable individual or individuals rather than in a non-personal manner such as an indistinguishable member of a group, company or organization. The individual need not be the one that is the direct focus of an act of harassment or stalking as long as it is evidentially clear that the act was intended to have an effect on him or her. Hence stalking can be direct or indirect, although the latter behaviour will be more difficult to prove.
4. Behaviour should be unreasonable. The reasonableness or otherwise of the perpetrator's act *in relation to* its potential effect on the victim should be a key element of the offence or tort.[39] Hence, it should cover violent behaviour and the actual infliction of harm or threat of harm, whether to the person or property or family, friends or loved ones. Whether it could extend to more 'neutral acts' is less clear and will have to depend on the foreseeable effects on the recipient to be objectively determine. What is reasonable can be measured by a combination of factors including cumulative course of conduct and the perpetrator's reaction to the victim's response, which must be applied to the facts and circumstances of each case.

5. Foreseeable effect should be weighted. As mentioned, to establish a fair balance of interests, a "reasonable man test" with an objective analysis should be applied, but to the victim instead.[40] Such a test will also balance the want of certainty against the need for flexibility.[41] Such a balance is measured by what are the reasonable and foreseeable effects in relation to the reasonable victim.
6. Series of Action should be the norm. There is a need for repetitiveness or persistency of conduct. Repetition is a key feature of online stalking. A one-off attack online, while it may cause the recipient distress, could not be described as cyberstalking. Cyberstalking is a course of conduct that takes place over a period of time and involves repeated attempts to cause a person distress. Some laws define it as involving two or more incidents following a repetitive pattern. Even if the one and only threat is the intended execution of an act of violence, it should not constitute stalking although it can constitute some other tort or offence under civil or criminal law respectively. However, a case can be under made for access to preventative measures even without resort to a trial if there is strong evidence that an act will be repeated or followed-up or that there will be an escalation of a threat. Because it is the course of behaviour that we want to prevent and offer protection from, both the threat and actual institution of the ends sought to be attained could constitute the offence.
7. Public policy defences should be included in criminal stalking provisions. Countries with more advanced laws in this area have established defences to acts that come within the legal definition of stalking (e.g. U.K. and Australian legislation) or exceptions for legitimate purposes for sound policy reasons. This is to ensure that actions that should not constitute an offence would not fall under it.

3.4. Comparing Jurisdictional Legislative Initiatives

Stalking law is more complicated than general harassment law.[42] It involves more subtleties because the victim's perspective as well as the stalker's has to be considered. Moreover, the profile of the stalker is more peculiar and may not be susceptible to normal treatment. For example, acts that may not constitute harassment such as surveillance and even gift-giving and other non-threatening but unwanted attention such as constant calls, e-mails and SMS or IM messaging can cross the threshold of what is considered socially normal or even tolerable interaction to constitute stalking. Actions that may be acceptable or even encouraged in the context of a mutual loving relationship becomes sinister stalking behaviour in another context when there is no reciprocity of interest.

Stalking legislation varies in scope across jurisdictions.[43] For example, it tends to be more expansive in some States in the United States and the United Kingdom, but is given narrower treatment in other States in the U.S., Canada, Australia and Japan that may legally define stalking through a list of prohibited activities, require a credible threat assessment, and make the apprehension or fear of harm, violence or injury a prerequisite.

3.4.1. United States

All the individual States in the United States, has enacted some form of stalking legislation,[44] and most have or are in the course of addressing cyberstalking in these provisions or separate legislation.[45] The types of stalking legislation fall generally into, and in between, two categories according to the elements constituting the offence:[46]

1. The Higher Threshold category that generally consists of (a) a credible threat, and (b) the intent and (apparent) ability (to carry it out),[47] which (c) causes fear (to the victim for his or her own safety or that of his or her immediate family).[48]

2. The Lower Threshold category which largely consists of (a) behaviour directed at a victim that is performed by stalker,[49] that is (b) knowingly, purposefully and repeatedly carried out, which (c) causes alarm, annoyance, (etc.) and/or will cause a reasonable person to suffer fear and emotional distress (etc.).[50]

The 1993 Model Anti-Stalking Code for States (Model Code)[51] requires both *actus reus* and *mens rea*, which is the norm for criminal offences.[52] Most States require the following three elements to be satisfied: A threshold of threatening behavior such as a series or course of conduct;[53] the intention to perform those acts in relation to another; and the knowledge that it will cause a reasonable person to fear harm or suffer emotional distress (although that may not be the motive).[54]

The hodgepodge of state laws and the piecemeal way in which they are 'updated' in varying degrees and at different rates to specifically address problems peculiar to cyberstalking, where existing legislation are found lacking, is unsatisfactory.[55] There is no comprehensive federal statute on cyberstalking,[56] although serious study has gone into it by the government.[57] The existing federal laws that can partially cover cyberstalking still falls short of addressing all of its problems because they either still require a high threshold "credible threat"

requirement,[58] have other requirements that are a throwback to the original purpose of the legislation,[59] or do not address problems specific to the use of electronic communications.[60]

3.4.2. United Kingdom

In England and Wales, the emphasis is on protection and prevention of harassment in general.[61] Hence section 1(1) of the Protection from Harassment Act of 1997 (Cap. 40) (PHA)[62] provides for the prohibition of harassment (which includes alarming or causing distress)[63] in that "[a] person must not pursue a course of conduct which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other; or "[a] person must not pursue a course of conduct which involves harassment of two or more persons, and which he knows or ought to know involves harassment of those persons, and by which he intends to persuade any person…not to do something that he is entitled or required to do, or to do something that he is not under any obligation to do."[64] What he "ought to know" is determined using the "reasonable man test" in context, that is, "a reasonable person in possession of the same information".[65] Exceptions are made to the rule.[66] The powers of the court to punish and prevent are at sections 2-5 and range from criminal to civil powers (including monetary damages, injunctions and restraining orders).[67] There is no specific reference to the use of new technologies although the Malicious Communications Act of 1998 (MCA)[68] does refer to electronic communications.[69]

Prior to the Act,[70] the tort of nuisance,[71] and the tort of public nuisance, were used to deal with a case of stalking despite the uneasy relationship between these torts and the subject matter of harassment.[72] The tort of harassment has also been invoked, albeit on a limited basis.[73]

Sections 8 to 11 of the PHA make corresponding provisions for Scotland.[74] The Protection from Harassment (Northern Ireland) Order 1997 in Northern Ireland is substantially the same as the PHA except for a difference in numbering.[75] Similar replicas of the PHA have also been passed in the Isle of Man and the States of Guernsey in 2000 and 2005 respectively.

3.4.3. Canada

Canada deals with stalking under section 264 of Canada's Criminal Code on criminal harassment.[76] Section 264(1) states that: "No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in [prohibited] conduct…that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them."[77] The list of "prohibited conduct" is found at section 264(2) and consists of:

a. repeatedly following from place to place the other person or anyone known to them;
b. repeatedly communicating with, either directly or indirectly, the other person or anyone known to them;
c. besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or
d. engaging in threatening conduct directed at the other person or any member of their family.78

The maximum punishment for stalking is a five year jail term.[79]

3.4.4. Australia[80]

Like in the U.S., Australian stalking laws are state-centric,[81] and there is no consistent nationwide law against stalking. Some of its laws have been updated in response to the digital age. For example, under section 359B of the Queensland Criminal Code (Stalking) Amendment Act of 1999,[82] "unlawful stalking" (i.e. actionable stalking) is defined as "conduct intentionally directed at a person (the "stalked person"); and engaged in on any 1 occasion if the conduct is protracted or on more than 1 occasion; and consisting of 1 or more acts of the following, or a similar, type:[83]

a. following, loitering near, watching or approaching a person;
b. *contacting a person in any way, including, for example, by telephone, mail, fax, e-mail or through the use of any technology*;
c. loitering near, watching, approaching or entering a place where a person lives, works or visits;[84]
d. leaving offensive material where it will be found by, given to or brought to the attention of, a person;
e. giving offensive material to a person, directly or indirectly;
f. an intimidating, harassing or threatening act against a person, whether or not involving violence or a threat of violence;
g. an act of violence, or a threat of violence, against, or against property of, anyone, including the defendant; and

h. that 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 causes detriment,[85] reasonably arising in all the circumstances,[86] to the stalked person or another person."[87] [emphasis mine]

Section 359C renders irrelevant the personal awareness or mistaken identification of the stalked person, the use of a third party, similarity in action, intention to cause apprehension or fear or that it is actually caused, or motive. Section 359D lists exceptions to section 359B. Sections 359E-F provides for the powers of the court to punish or prevent stalking behaviour.88

In Victoria under the Crimes Act of 1958,89 stalking is defined as "engaging in a course of conduct with the intention to cause physical or mental harm, apprehension or fear." That conduct includes some of the usual physical acts similar to the Queensland Act including keeping the victim under surveillance and engaging other parties to do any of the acts. The offender's action must achieve the result (e.g. apprehension or fear) intended by the offender. The penalty is up to 10 years imprisonment. The legislation was updated by the Crimes (Stalking) Act 2003,90 which extended the definition of stalking to include acts performed through the use of the electronic medium such as:

a. contacting the victim or any other person by post, telephone, fax, text message, e-mail or other electronic communication or by any other means whatsoever;
b. publishing on the Internet or by an e-mail or other electronic communication to any person a statement or other material relating to the victim or any other person or purporting to relate to, or to originate from, the victim or any other person;
c. causing an unauthorised computer function in a computer owned or used by the victim or any other person; and
d. tracing the victim's or any other person's use of the Internet or of e-mail or other electronic communications.

3.4.5. Japan

In Japan, "stalking" is defined as "repeated acts of harassment of a specific person, motivated by an emotional attachment or a grudge borne because of unrequited love".[91] This is quite limited in scope and confines the offence to the motive of the perpetrator, and only one motive at that. A person who engages in any of the following eight activities relating to the abovementioned acts can be charged with stalking:[92]

1. Following and waiting near or visiting the victim's home, office, school or other places the victim frequents without a previous appointment.
2. Placing the victim under relentless surveillance and informing the victim that he or she is being closely watched.[93]
3. Demanding to meet or go out with the victim when he or she has no wish to do so.
4. Speaking or acting rudely toward the victim.
5. *Making silent or constant telephone calls or sending repeated fax messages to the victim.*
6. Sending repugnant items that will cause discomfort to the victim such as excrement or dead animals.
7. Telling the victim that the stalker knows secrets that could ruin the victim's reputation.
8. Telling the victim things that will make him or her feel sexually debased or sending documents or pictures that will sexually embarrass the victim. [emphasis mine]

The penalty for anyone found guilty of violating the law is up to six months in jail or a maximum fine of Yen 500,000.

3.4.6. Inchoate Developments in Other Countries

Many other countries all over the world have either enacted specific anti-stalking legislation or provisions, or are studying the feasibility of doing so and the models to be considered for adoption. They include:

The Law Reform Commission of Hong Kong issued a Report on Stalking Law,[94] which identified the concept of "harassment" in such a situation as descriptive of both "the activities engaged in by stalkers" and "the impact which such behaviour would have on victims of stalking". Thus it acknowledges both perspectives in relation to the problem.[95]

The Singapore experience has been examined in the earlier part of this paper. The rising problem of cyberstalking has since been raised in the Singapore Parliament,[96] the Singapore Law Reform Committee has produced a report on the feasibility of anti-stalking legislation in 2005, but it has yet to be translated or materialise into law.

Finally, it is to be noted that some stalking laws require the additional element of an effect on the lifestyle of the reasonable victim and significant disruption to their daily life and functioning. For example freedom of movement, right to solitude or privacy and to live in one's home, or use one's phone or computer without fear.

3.5. Recommendations for Cyberstalking Legislation

From the above evaluation of the unique problems relating to cyberstalking and assessment of the changes and shortcomings of existing cyberstalking laws, we have identified some of the needs that have to be addressed in order for legal protection against cyberstalking (in addition to existing harassment and 'offline' stalking laws) to be effective. In short, any enactment or amendment of such laws must address the social and policy angle (and the balance of interests), and the unique issues to cyberstalker based on their profile and the problems peculiar to electronic stalking (perpetuated by the increasingly novel ways of stalking offered by the benefits of technology), taking into account existing related legislation.

It must also address the challenges to enforcement such as in detection, identification, evidence gathering, attribution and jurisdiction.[97] This will require a more multi-faceted approach than the law itself can provide such as the participation of potential victim, others in society and communications intermediaries such as Internet Service Providers (ISPs).[98] Hence, beyond the prescriptive, the investigation and enforcement arms of the law must also be rendered effective to meet the special demands and challenges of cyberstalking.

3.5.1. Substance

The recourse should be a criminal action with the public resources and tools that it offers, such as police investigation and protection, various forms of criminal sanctions. Some civil redress should also be available to the courts, particularly to take anticipatory actions to prevent initial or continuing anti-social stalking behaviour, such as through the proactive use of restraining orders and the like.

Taking into account the policy considerations and legislative prototypes that have been canvassed, I come to the following conclusions. For an anti-cyberstalking law to be effective, it should:

1. Constitute a criminal offence but the courts should be given the power to use impose both criminal and civil measures as appropriate. As a specie of stalking, anti-cyberstalking should be part of an updated stalking or harassment legislation, albeit an integral part; and the new challenges offered by cyberstalking must be addressed.
2. Address both actual behaviour and the threat thereof in whatever form, including through electronic and other information and communication devices. Hence, there should be online and offline consistency of treatment,99 and the provision should be technologically neutral. Any physical proximity or a credible threat requirement will not be practical and can be ineffective in prosecuting certain cyberstalkers depending on the modus operandi.
3. The method of directing acts at the victim and at persons close to the victim which are meant to have an effect on the victim, must take into account and include new and innovative methods of stalking in cyberspace such as the use of automatic non-human agents or third party action through the use of computer software, impersonation and instigation of third parties.
4. Require a sufficiently anti-social behaviour directed at the victim by the perpetrator.100 The motive or ability to carry out a threat or follow up on behaviour directed at the victim are not prerequisites as we are dealing with the effects on, and seeking to protect, the reasonable victim's state of mind based on a factual determination of what is socially acceptable behaviour directed at him.
5. Put into the legal equation the actual and potential effects on the victim by requiring the actual or constructive knowledge of the alleged stalker (i.e. "knows or should reasonably know") that his or her words or actions will cause (serious) annoyance, alarm, fear or mental distress (based on an objective assessment).101
6. Require that the acts either did cause the victim harm, injury or death; or will cause a reasonable person (serious) annoyance, alarm, fear or mental distress (based on the same objective test) under the facts and circumstances of the case (which is the subjective context).102 This is an objective test based on and applied to the subjective facts and circumstances of each case, which will have to be sensitively applied in order to adequately balance the needs of the individual to freedom of speech, expression and movement on the one hand, and the right of the individual to privacy, safety and security on the other.103
7. To further establish a fair balance of rights, a gradation model for remedies and punishment should also be adopted. Also, public policy exceptions can be made for legitimate functions such as police investigations and money collection not amounting to harassment or intimidation.

8. Hence, the elements of an offence of stalking that has to be satisfied before sanction can be imposed should be as follows:

3.5.1.1. Identifying the Main Elements of a "Stalking" Offence

As with most crimes, stalking has both *mens rea* and *actus reus* requirements. Stalking as an offence should consist of: A ***course of conduct*** caused by a person (the stalker) that is ***directed at or towards*** another person (the victim) that the stalker ***knows or should reasonably know*** will cause ***annoyance, alarm, fear or mental distress*** to the victim.

3.5.1.2. Defining "Course of Conduct" and Illustrating the Type of Conduct

"Course of conduct" can be defined as the repeated or persistent surveillance of a person and the repeated or persistent making of communications to a person or a combination of both whether directly or indirectly by whatever means. The following constitutes a course of conduct for the purposes of this Act if one or more of them are performed more than once:[104]

a. engaging in threatening conduct towards a person;
b. maintaining a visual or physical proximity to a person, his place of residence or work;
c. following a person from place to place including tracking a person's words and actions on the computer through electronic or physical means;
d. making or conveying verbal or written communications to a person;
e. instigating others to do any of the above acts that the stalker knows or should reasonably know will lead to repeated or persistent words or actions made towards the victim.

The actual course of conduct need not be performed by the same person or instrument.[105] As noted before, acts also include words, and they can constitute other forms in the digital context that were not as common or that were even unknown in the physical realm, such as impersonation of the victim to elicit or invite reaction from third parties or the use of third parties to harass the victim. The course of conduct need not be perpetrated directly by the stalker or by just one person. It can be the cumulative effect of the words or actions of several persons or even non-human agents, such as the automatic and repeat sending of messages by software programming. Persistency, especially in the face of rejection, distinguishes a genuine stalker from, for instance, a one-off incident such as the actions of an over-eager suitor.

It should be made clear that the list is not exhaustive and is meant only as a guidance of the type of behaviour that amounts to a course of conduct. The above list serves merely as examples of the more common forms of stalking and can and should be expanded. It should primarily address the words or actions rather than the means (i.e. medium and technology neutral) although the possible mediums used, that is, physical or electronic, can be highlighted as illustrative of the trend. The words or actions need not be the same in order for them to have the cumulative effect of a course of conduct.

3.5.1.3. "Directed at or Towards" Another can be Direct or Indirect

Stalking as an offence is of a personal nature. This relates to the identifiability of the victim and of the targeted nature of the act. It must be made clear that the acts relate to the causing of negative mental and emotional effects on the victim and they can include indirect acts such as acts directed towards the victim's family, friends or loved ones.

3.5.1.4. Determining the Mental Element and its Relation to the Effect on the Victim

Cyberstalking and offline stalking should share the same mens rea requirement. To be effective, cyberstalking statutes should criminalise conduct that either causes a real effect or that a reasonable person will know will cause another one or more of the effects listed. What is reasonable, whether relating to the perpetrator or the victim, is to be objectively determined.

First, there must be an intentional mens rea requirement to engage in the abovementioned "course of conduct". Generally, a stalker must willfully or intentionally engage in repetitive conduct of a nature that relates to the next mental element, which is the mental state requirement tied to the effects on the victim. Hence, just like an 'offline stalker', a cyberstalker should have intentionally engaged in conduct that causes his target or a reasonable person to fear for her safety.

Second, there is another mens rea requirement that relates to the effects on the victim. Laws that focus solely on the perpetrator's conduct fall short in combating cyberstalking. On the other hand, laws with a "reasonable person" standard can better address cyberstalking because they accurately focus on the standards expected of the perpetrator in society as well as on the effect of the perpetrator's conduct on the victim.106

For the breakdown of the mens rea requirement and the list of effects, see Appendix: Table 4.

Countries that require constructive or actual knowledge include some states in the U.S. and Australia, the U.K., Canada, Ireland and New Zealand.

It is the unique nature of stalking and the profile of the stalker that explains the requirement for a series of conduct and why the mental element is based on basic/general intent, that is, the judgment of a reasonable person (unlike most criminal offences which require specific intention). Countries or states that require specific intent (usually to cause some form of injury) are confining it too narrowly and would not have taken into account the unique and diverse scenarios of cyberstalking.

To be fair, both the perpetrator and the victim are to be held up to the objective standards of the reasonable person. Hence, to "reasonably know" actually reflects both the test in relation to the perpetrator (the objective assessment) in the context of each case (the subjective context). The perspective of the 'reasonable victim' in the element of the offence and in the analysis of the mental state of the perpetrator should be a unique feature of this offence.

3.5.1.5. The Appropriate Degree of Effect or Level of 'Harm' Threshold

Arguably, the greatest challenge lies in determining the appropriate threshold for the degree of effect or the level of 'harm' that will provide the basis for legal action. Establishing a balance between what is 'social' and what is 'anti-social' behaviour in the ever-changing social context. There is a fine line between the two as we have seen due to the demands of society and close living, the requirement for compromise and in balancing personal peace with fruitful social activities.

Criminal statutes that are most useful and successful in prosecuting cyberstalkers and protecting victims are those which shift the focus from the perpetrator's behavior to the effect on the victim. The victim's state if mind is appropriate due to the highly contextual nature of the stalking acts and a consideration of the objective effects on the victim. That is, evaluating the facts and circumstances and what the reasonable victim will experience under them, but excluding from the analysis personal sensitivities and foibles. After all, one must remain mindful that criminal law deals with societal and public issues, not inter-personal ones.

Behaviour that "threatens", "harasses", "intimidates", "terrorizes" or "torments" are words that are commonly used in some legislation, but they may not be sufficient. A case can be made for sanctioned behaviour, in the digital age, to extend to conduct that alarms and even (seriously) annoys another although care must be taken in ensuring that there is a reasonable threshold that will not include negligible or 'minor' negative effects that is the cost of living in an urban society and inter-connected world.

3.5.1.6. Determining Defences

The following are some of the usual defences which can be exempted from the general offence:[107]

a. Acts done with the consent of the alleged victim. If the victim requests the alleged stalker to stop, such a request (if recorded) can function either as a rebuttable presumption that the contact is unwanted or as *prima facie* evidence that the stalker knew that he was causing annoyance, alarm, fear or mental distress, or both.
b. Acts performed in the course of police investigations or by law enforcement authorities for the purpose of the prevention of crimes.
c. Acts otherwise authorised or required by law, regulation,[108] or order of a court of competent jurisdiction.
d. Acts that for any other reason the court find is reasonable under the facts and circumstances of the case.[109]

Canada uses the general approach by incorporating the term "without lawful authority" to qualify the offence.[110] A more detailed policy study should be conducted by the government to determine the exemptions from the general criminal provision.

3.5.2. Form

Now that I have identified the essential elements of an effective anti-cyberstalking provision, let us revisit the Singapore case study. The reasons have already been canvassed as to why a stand-alone legislation or a separate provision under an existing legislation is more appropriate than an amendment to the current sections 13A-C of the Miscellaneous Offences Act (Cap. 148).[111]

The other format issue which has to be considered is whether to have a provision that generally prohibits the offence (i.e. a General Prohibition Model) such that those used in the U.K. and the U.S. Federal Statute and selected States;[112] or one that more specifically states the acts constituting an offence (i.e. a List Model) such as those in Canada, Australia, Japan and other State in the U.S.;[113] or a combination of both, and if so, what type of combination it should take.

It is proposed that a combination model is the best approach to take. I recommend a general prohibition provision with a non-exhaustive illustrative list of common stalking and cyberstalking acts.

A general prohibition will clearly and concisely inform as to the offence of stalking while a non-exhaustive list (serving as both evidence of "course of conduct" and as illustrative guidance on other similar activities) will give support and additional guidance to the courts. This approach provides flexibility without the expense of incurring more uncertainty.[114] The courts can then be trusted to apply the provision with purposeful objective and wisdom.[115]

While a simple and succinct general prohibition approach has the benefit of certainty, the usefulness of open-ended (i.e. non-exhaustive) illustrations is that it will guide the courts to confine actionable stalking to the types of behaviour that the legislation is meant to cover,[116] leaving other types disputes such as nuisance and neighbour disputes (very common in urban areas) to the more appropriate law, such as the tort of harassment and nuisance.

4. Computer Forensics: Challenges to Criminal Investigation and Evidence Gathering in the Digital World[117]

4.1. The Role of Law Enforcement and the Need for Expertise and Legislative Powers

Legislation is even more compelling in the electronic age as existing police powers and evidential provisions become antiquated and inadequate to the needs and unique challenges of the digital medium. For example, problems include presentation of computer-related evidence in court, identification and tracing of perpetrators using pseudonyms or fake identity, dealing with stalkers not within physical jurisdiction. All these require special powers and expertise for law enforcement agents.

With respect to the type of evidence, and in comparison to tangible evidence, evidence in electronic or digital form is very important but is generally more difficult to obtain and to admit as evidence, particularly if it involves passive behaviour such as surveillance, where it may be difficult to identify the stalker or to protect against a tech-savvy stalker who can spy on and keep track of the victim through the use of spyware.

4.2. The Collection of Electronic Evidence by the Victim

Victims should be educated and made aware of the procedures they can take to gather evidence that will serve them in a court of law to protect themselves from future stalking. They should refrain from communicating with the stalker, other than to warn the latter not to make further advances so as to supply the mental element for an offence if the latter does not discontinue his actions.[118] Other than informing the police by lodging police reports,[119] victims should save copies of e-mail, postings, or other communications in both electronic and hard copy form.[120] Victims can also file a complaint with the stalker's ISP as well as their own. Many ISPs offer tools that filter or block communications from specific individuals.[121]

The victim of cyberstalking faces somewhat of a Catch-22 situation. By avoiding or filtering out surveillance and communications, electronic evidence of stalking behaviour is lost. On the other hand, to collect such evidence against a stalker requires knowledge that it is happening in the first place and the victim may have to suffer continued abuse in order to accumulate sufficient evidence to launch a complaint to initiate police investigation.[122]

4.3. Electronic Forensics and the Role of Intermediaries

As noted, there are many issues relating to the challenges in cyber-investigations and the discovery of digital evidence. With assistance, often offensive e-mails or other forms of electronic messages and weblogs can be traced to the sender with the cooperation of ISPs. But the issue is not only one of technical expertise, but also to what extent and in what situation should such intermediaries be compelled to assist in investigations or to provide information on its users despite the breach of privacy. Hence, it is clear that with regards to investigations, the ISPs do have an important role to play. The balance that must be achieved is between the right to privacy and data protection on the one hand and the public interest in computer forensics and electronic investigations on the other.

The general position is that ISPs should not incur civil or criminal responsible or be held vicariously liable for the action of cyberstalkers.[123] The reasons are many and can be culled from both a public interest and private interest perspective. In order for the Internet to continue as a medium for increased freedom of speech and expression, the exchange of ideas and limited censorship, ISPs must be protected from general liability for the acts of its users and they should also not be imposed the role of a regulatory authority.

5. Civil and Criminal Legal Recourse and Redress

Cyberstalking is a social problem that requires a unique set of legal 'remedies' in order for the law to be effective in preventing and removing it. The most important reason for criminalising stalking is that it can provide appropriate sanctions and powers to deal with perpetrators, which are not available if we merely rely on civil action such as the tort of harassment or existing piecemeal and outdated statutory provisions, civil or criminal.

5.1. An Overview of Jurisdictional Sanctions

In England and Wales, courts can impose a fine or imprisonment, of up to five years in the case of putting the victim in fear of violence. United States, Canada, and Australia provide for similar penalties.

The English courts can additionally impose a "restraining order" on an offender, prohibiting the defendant from doing anything described in the order.[124] The order may prohibit the defendant from contacting the victim or from going to the target's home or place of work. The order may have effect for a specific period or until the court makes a further order. If a defendant breaches a restraining order, that breach is itself a criminal offense for which he can be imprisoned for up to five years, be fined, or both.[125] Similar orders appear to be available in other jurisdictions.

Australian courts has a canopy of orders at its disposal in stalking situations including the Apprehended Violence Orders or Intervention Orders, often referred to as Apprehended Domestic Violence Orders (ADVO), Apprehended Personal Violence Orders (APVO), Restraining Orders, Restraint Orders and Protection Orders.[126]

Such measures should not only be available on criminal conviction to prevent future incidents, they should also be available as a civil recourse to arrest or stop such acts that are in progress as interim or temporary measures and as a final or permanent solution when a case is resolved.[127] Other useful orders can be added to these measures including orders for counseling, mediation and psychiatric evaluation.

Japan has legislated for a less formal system that requires the issuance of police warnings or cautions before a perpetrator can be arrested.[128]

5.2. Recommendations for Types of Recourse and Redress

Both civil and criminal recourse and redress, like the type found in the U.K. statute, should be available to alleged victims.[129]

Punishment under criminal law serves several purposes. The main objectives are to deter and prevent offences generally, to incapacitate the offender from committing further offences, to rehabilitate the offender where appropriate, and to mete out retributive or restorative justice. These are all factors that should be taken into consideration in the development of the options recommended to be made available to the courts.

Upon criminal conviction,[130] the courts should also be given additional powers to order medical treatment or supervision such as psychiatric evaluation,[131] whether while the offender is in incarceration or otherwise.[132] If it is determined that the perpetrator is so mentally unsound that the *mens rea* is not made out or he cannot even make his defence, the courts or the authorities should also have the power to remand him for treatment in a mental facility or take any other action that will rehabilitate him and to prevent continued threat of stalking.[133] The stage of recourse, whether by request of the victim or by the court's initiative, to order a mental evaluation, should be legislatively addressed.[134]

Furthermore, the power to make other orders such as to disallow access to, or use of, instruments to perpetrate the offence should also be considered and legislated. For example, prohibiting electronic access such as prohibiting the use of the Internet for a period of time or regulated/limited usage. This will have an incapacitating effect.

The approach to punishment in general should be one that is graduated and preventative,[135] and with an early interventionist objective taking into account civil liberties implications.

Because stalking is also capable of early detection as it constitutes a cumulation of acts, its further development can be arrested and its continuation prevented through preemptive protection. In this case, civil remedies are also an important addendum to criminal sanctions, which generally come in 'after the fact' (i.e. after the acts have been committed, or at the very least attempted).

Civil remedies may serve to warn stalkers to stop, for example, by injunctions or protection orders, and to provide monetary remedies for victims if acts have led to damages such as for medical treatment or pain and

suffering. For those stalkers that are less likely to respond merely to warnings and to be deterred by the threat of pecuniary damages, other forms of deterrence or measures of prevention such as mandatory medical treatment or supervision, incapacitating measures and even incarceration, may be more appropriate, which are criminal sanctions.[136]

5.3. Recommendation for a Sliding Scale of Recourse and Redress

There should be a gradation or scale of remedies or punishment for offenders in a civil and criminal action respectively.[137] The remedies may include warning,[138] restraining or protection orders with consequences for violation, fine, imprisonment, caning, and mental assessment and/or treatment, with probation or confinement. This is to ensure that the most appropriate and effective remedy is given for the relevant offender.[139]

In the meantime, as noted earlier, the courts should also be given powers to grant interim relief, such as an interim injunction to restrain the behaviour complained of or the alleged stalker from approaching or contacting the complainant, pending the outcome of the case.

So that sentencing is rational and is based on the level of the offender's culpability, the severity of the remedy or punishment can be statutorily provided for. For instance, recurrent offences (i.e. recalcitrant offenders) and aggravated offences (e.g. flagrant disregard for protective orders, possession and use of weapons, causing actual harm, escalation of behaviour) should carry heavier penalties.

See Appendix: Table 5 for a proposed sliding scale continuum of civil and criminal recourse and redress.

Some other solutions can include Offender Registration,[140] which is useful for profiling, forewarning and police investigations; and the use of Anti-Social Behaviour Orders (ASBO) that serve as community warning or notification.[141] Electronic monitoring devices may also be considered in order to be able to monitor the movement of certain offenders and their proximity vis-à-vis the target.

It is envisioned that there will not be a problem with frivolous complaints or litigation. An alleged stalker can always reject a police stern warning or go to trial. Lack of evidence or merit can also prompt the public prosecutor not exercise prosecutorial discretion not to proceed with a case. As for private prosecutions and civil trials, they involve cost and effort on the part of the alleged victim. Moreover, as usual, false or frivolous complaints can come with legal consequences as well.

6. Education, Technological Defences and the Global Solution

6.1. Education and Technology as Non-Legal Complimentary Measures

Education should extend both to society and to law enforcement. In relation to the former, there are ample cyberstalking resources and help centers, both online and offline,[142] for individuals to learn how to deal with stalkers, to protect themselves, to gather electronic evidence and to seek victim support. The government can also embark on a sort of "Cybercitizen Awareness Program"[143] to educate the public on all aspects and forms of cybercrime, preventative or protective measures, and legal recourses.

Similarly, the investigatory authorities should have the requisite skills, training and experience to competently conduct computer forensic investigations.[144] Stalking through the electronic medium is quite different from traditional stalking. Thus law enforcement needs to better understand and explore this new medium for crime, and embrace new technologies and other appropriate investigatory tools.[145] Intermediaries such as ISPs also have a role to play, whether in support of crime enforcement or to proactively prevent stalking behaviour online.

The private sector, especially the technology and media industries, should also come up with products that can assist in blocking stalking surveillance or communications, assist in the identification of the source of such actions, and in the collection of evidence.[146]

6.2. The Need for a Global Solution to Cross-Jurisdictional Stalking

In the electronic frontier, the perpetrator requires no passport and do not pass through any checkpoints while navigating cyberspace and committing his acts. The problem of extra-territorial jurisdiction and enforcement extends to the problem of cross-jurisdictional stalking. The enforcement of national laws and procedures on a global scale is a challenge unless there is consistency of legal treatment worldwide and cooperative procedural arrangements. Like other types of cybercrime, a concerted effort is required to create an international regime for mutual co-operation and enforcement and to tailor a consistent legal and regulatory approach to cyberstalking behaviour worldwide. Dealing with it in an international forum and through the use of a harmonizing instrument such as the Cybercrime Convention will go some way in tackling the global problem.[147]

7. Conclusion

One must remember the social and policy reasons behind combating cyberstalking, which is the need to reign in the anti-social effects and inconveniences of negative types of electronic communications and to protect people from mental harm, not just to protect people from the potential manifestation of physical harm. In the same way that spam is a problem that requires a distinct treatment from junk mail, so too cyberstalking requires additional attention from harassment and stalking.

The uniqueness of stalking is that motive is irrelevant and the effect of a series of acts on the reasonable victim is key. More specifically, in the case of cyberstalking, increasing recognition must be given to the effects of non-physical, non-proximate and other methods of stalking that were not known or common in the past when stalking was largely linked to the physical form.

Anti-stalking legislation around the world generally follow two basic models: The "list model", which can consist of a 'closed' list of acts (e.g. some States in the U.S., Canada, Australia and Japan) which provides certainty. The other model is the "general prohibition model" (e.g. the U.K. and other U.S. States).[148]

The preference and the recommendation here is to adopt the latter model with an 'open' 'illustrative list' of examples, which can be updated, and that can serve as guidance to the courts. This will provide certainty while remaining flexible and responsive to change.

Substantively, criminal stalking can be defined as a course of conduct or behaviour (i.e. more than a single incident) that is perpetrated by one person upon another (i.e. individual-to-individual), and either the alleged stalker in fact knows that the conduct will cause annoyance, alarm, fear or mental distress to the victim; or a reasonable person will consider that the behaviour will cause annoyance, alarm, fear or mental distress to the victim (objectively tested) under the circumstances and in the context of the case (subjective context).

See Appendix: Table 6 for a comparision of the elements of the stalking offence in relation to the parties (i.e. from the perspective of the perpetrator/stalker and the target/victim). Finally, see Appendix: Annex 7 for a draft proposed criminal model provision for stalking, which includes cyberstalking, and a brief explanatory note.

Appendix

Table 1. Comparison: Current Treatment in Singapore

Criminal	Civil	
Legislative		***Tortious***
Sections 13A-D and 14A of the Miscellaneous Offences Act Various provisions of the Penal Code (esp. Offences Affecting the Human Body)	Domestic violence under the Women's Charter Harassment and Intimidation under the Moneylenders Act	Harassment Private Nuisance Assault Battery Trespass on Land Infliction of Emotional Distress

Table 2. Comparison: Permutations of Harassment

Harassment	**Stalking**	**Cyberstalking**
Genus	***Specie***	***Subspecie***
Generally less cross-border problems due to costs of perpetration and physical distance Generally less investigative, evidential and enforcement problems		More jurisdictional issues Investigative issues (tracing, identification, evidence gathering) Enforcement issues
Personal or Non-Personal e.g. purpose driven harassment; commercial harassment; other forms of nuisance; stalking; etc.	Personal e.g. Erotomania; Love Obsession; Simple Obsession; Sex; Vengeance; Control, Perversion or Deviance; etc.[149]	
Individual Group to Individual Individual to Group Group to Group	Individual to Individual	

Table 3. Combinations: Permutations of Actors

First Party Perpetrator Physical or cyber, through self or Internet persona, avatar, etc.	**First Party Victim** Includes threats and actual harm to self, property, family, friends or loved ones
Third Party Perpetrator E.g. instigating another to act against one in a negative manner, irrespective of the true knowledge or intentions of that other[150]	**Third Party Victim** If stalking one indirectly, e.g. through messages sent to another or conduct in relation to that other[151]

Table 4. Breakdown: The *Mens Rea* Requirement and the List of Effects

Mental Element **Basic/General Intent related to a List of Effects**	
Degrees of knowledge **(Objective/Reasonable Man Test)**	**Degrees of Effect/Type of 'Harm'** **(Subjective/Contextual Basis)**
Know (actual) Likely to know (*recklessness*) Ought reasonably to know (constructive/*negligence*)	In order of severity: (below threshold?) Nuisance[152] (*serious*) Annoyance[153] Worry[154] (above threshold) Mental Distress/Alarm Fear of harm to property Fear of harm to first person or another (with emotional connection) Actual compulsion/hindrance[155] Actual harm[156]
Deemed to know (e.g. after legal notice to cease and desist) Presumed to know (e.g. rebuff or non-reciprocation by victim)	

Table 5. Scale: Continuum of Civil and Criminal Recourse and Redress

Scale **(in order of severity)**	**Civil** **(balance of probability)**	**Criminal** **(beyond reasonable doubt)**	**Other** **Statutory** **Powers**
Level 1	Victim Protest putting Stalker on notice of unwanted attention (no trial or standard of proof required)	Police Stern Warning (no trial or standard of proof required) Cease and Desist Order?	
Level 2	Expedited Order[157] **/** Protection Order Temporary and Permanent Injunction	Prohibition Order / Restraining Order Sentencing Option or Power	Power to send the stalker for psychiatric evaluation to assess if he or she is suffering from mental problems; and Power to send the stalker for mandatory treatment, with probation or confinement, if necessary.
Level 3	Violation of Protection Order: Fine Breach of Civil Injunction: Damages[158]	Violation of Protection Sentence: Imprisonment/Fine Breach of Civil Injunction: Imprisonment?	
Level 4	Damages	Imprisonment and/or caning	

Table 6. Comparison: Elements of the Stalking Offence in Relation to the Parties

Stalker	Target
Threatening Behaviour or Unwanted Attention/Advances (operative element): The *actus reus* is in the acting out of the course of conduct,[159] which in most cases consists of repetitive but not necessarily similar acts [*unless a single act is especially serious*].[160]	Direct or indirect recipient of Threatening Behaviour or Unwanted Advances which can be in active (e.g. communications) or passive (e.g. surveillance) form (evidential).
The *mens rea* that the 'threatening' acts will cause annoyance, alarm, apprehension or fear in the victim to be objectively assessed based on actual knowledge or on a "reasonable man" test.	(*serious*) Annoyance, Alarm, Fear of harm or mental distress caused (operative element):[161] Objectively assessed based on a "reasonable man" test (objective) in the circumstances and context facing the victim (subjective).[162]

Annex

Draft Proposed Criminal Model Provision[163]

A person who pursues a persistent course of conduct in relation to another which he knows or ought reasonably to know will cause that person alarm, distress or fear of harm to himself or another shall be guilty of a criminal offence punishable with imprisonment of up to [ ] years or a fine of up to [ ] or both.

The act of stalking can include, but are not limited to, [any][one or more] of the following [examples][164] –
a. Sending of unwanted and unsolicited electronic messages of a personal nature;
b. Impersonating the victim and sending of electronic messages using his name; and
c. [other common examples of physical and cyber- stalking as they evolve].

The offence includes –
a. Instigating third parties to do any of the above acts; and
b. Directing any of the above actions to a family, relative or friend with an emotional connection to the victim that he knows [or ought (reasonably) to know] will affect the victim in the same way as if was directed at the victim himself.

The court have the power to require a defendant convicted of the offence to receive counseling, undergo medical, psychiatric or psychological evaluation or monitoring, and any other treatment as the court thinks fit. The court has the power to require a defendant to be subject to probation and police or electronic monitoring as an alternative to imprisonment.

The court shall also have the power to make Prohibition or Restraining Orders in addition to a sentence imposed on the defendant convicted of the offence of stalking to prevent further such offences as the court thinks fit. The Order shall have effect for a specified period of up to [ ] until review. An application may be made for variation or discharge. Failure to abide by such an Order shall be punishable by imprisonment of up to [ ] years.

Explanatory Note to Draft Proposed Criminal Model Provision

Stalking implies something done over a period of time, whether protracted or at intervals. Using electronic equipment, it can be more insidious and protracted rather than intervals (consider monitoring, which is more difficult to sustain for a continuous period physically than when conducted through a spycam).

A person must not pursue a persistent course of conduct directed at one or more identifiable person which he knows or ought reasonably to know [is unwanted/unsolicited and that] will cause [see scale and consider appropriate threshold]. Such conduct can include but are not limited to the following examples: [non-exhaustive list]

"Conduct" includes physical and electronic acts or words. It can include instigation of an outcome and it can also be vicarious in nature. Thus, "pursuing a course of conduct" can be direct or indirect, active or passive, or any combination.

"Persistent course of conduct" can involve conduct on at least two occasions whether protracted (uninterrupted over a period of time)[165] or with intervals (at separate occasions). These incidents do not have to bear any similarity to each other or be conducted through the same conduit, although a protracted conduct is likely to be so (e.g. use of a spycam). Acts constituting stalking are cumulative. A one-off incident that does not span a relatively long period of time such as a quarrel or fight at a scene, does not constitute a stalking offence although it may constitute the offences. Simlarly, a web posting or flaming will not, merely by virtue of its prolonged existence perhaps due to caching, constitute protracted conduct (hence, the use of "persistent").

"Ought reasonably to know" is an objective test (i.e. if any reasonable person in possession of the same information would be expected to know) but applied in a subjective setting (facts and circumstances of the case). In other words, a person ought to know that his course of conduct amounts to stalking of another if a reasonable person in possession of the same information would think that the course of conduct would result in the prohibited types of effect on the other. The effect on the victim is objectively determined, and actual proof of resulting harm or effects is not necessary. Hence the target need not be shown to actually have suffered those effects perhaps due to stronger constitution (although negative proof will not likely be complained of or litigated in the first placed, and can constitute proof of unreasonableness) or it is not relevant if the target is particularly sensitive (public policy and social reasons to sustain normal/ordinary human interaction).

Any persistent, unwanted behaviour can be considered stalking, but query whether "unwanted" or "unsolicited" are already an element of the effects (because surely those effects can only come from conduct of such a nature).

The stalker must know and be aware of his conduct (act) but need not specifically intend any of the effects (although proof of intent will of course be sufficient). This is because of the unique nature of stalking offences which are based precisely on the unreasonable conduct of the perpetrator, that can in ordinary circumstances consist of neutral or even what some may consider positive conduct, and on the negative effects on recipients of the attention that renders it anti-social even in the face of and in the context of modern urban society and the necessity and importance of human interactivity as a public social policy.

The *non-exhaustive* and *example-only* list approach will provide some certainty to would-be potential offenders (i.e. what not to do) and guidance to the courts.

Finally, the additional redress enunciated (i.e. injunctions, Orders, damages), above should be made available for the courts to impose unde the civil procedure code/rule if a civil action for a tort of harassment or stalking is made out on a balance of probabilities. This will complement the criminal recourse of the victim.

Notes

[1] The boon of anonymity can also be a bane. Even people that have perfectly ordinary profiles and lead ordinary lives offline can display a different personality in the digital realm - something more playful or open, but also sometimes something more sinister giving in to the temptation of deviant behaviour induced by the drug of anonymity. See, Anon., *Cyberstalking: A Real Life Problem* (Grafx-Specs, 1997), available at: http://www.safeteens101.org/cybstalker_prevention1.html.

[2] Pseudonymity allows people to act out their fantasies and to speak or express their innermost thoughts, which can be illegal, offensive or objectionable, that they may be proscribed from doing in real life. They do this under the impression that there are no social repercussions and that they cannot be traced. This stems from a false sense of security against both the detection of identity and the vigilance in enforcement of the law.

[3] There are also novel ways of stalking that have arisen in the context of the digital realm and through the workings of electronic media. This can include the enlistment of third parties to harass a victim irrespective of the intentions or knowledge of the third party in question. Harassment can also arise through victim impersonation to solicit unwanted advances or attention.

[4] See Kimberly Wingteung Seto, *How Should Legislation Deal With Children as the Victims and Perpetrators of Cyberstalking?*, 9 Cardozo Women's L.J. 67, 73-74 (2002), on the specific problems relate to identifying the stalker, effective deterrence, novel ways of stalking online and collection of evidence.

[5] For the rising statistics of stalking in the United States and in Japan, see Diana Lamplugh & Paul Infield, *Harmonising Anti-Stalking Laws*, 34 Geo. Wash. Int'l L. Rev. 853, 853-858 (US), 466-467 (Japan) (2003). On the

effects of stalking on victims, see Nga B. Tran, *A Comparative Look at Anti-Stalking Legislation in the United States and Japan*, 26 Hastings Int'l & Comp. L. Rev. 445, 448-9 (2003). There are currently no statistics on the number of stalking incidents or their effects in Singapore.

[6] Although stalking is a phenomenon that has existed for centuries, and cyberstalking has gained prominence in the media in recent years. There is a lack of the public knowledge and understanding of this and of their legal rights and obligations relating to such acts. The general impression seems to be that it is more of a problem in western countries than it is in an Asian one. Law and policy makers have also not focused on the specific issues relating to stalking as opposed to harassment as exemplified by the fact that a search of the word "stalk" in all its permutations yielded no cases under the Singapore Case Law Database, and only one short discussion under the Parliamentary Reports between Ms. Indranee Rajah and Assoc. Prof. Ho Peng Kee. See Parliamentary Debates Singapore Official Report: Tenth Parliament, Part I of First Session, Volume 74, 17 May 2002, available at: http://www.parliament.gov.sg.

[7] The Miscellaneous Offences (Public Order and Nuisance) Act (Cap. 184) (MOA) came into force on 9 June 1989, when the Minor Offences Act (Cap. 184, 1985 Rev Ed) was amended and renamed. Sections 13A and 13B of the MOA are largely modelled on sections 4A and 5 of the English Public Order Act of 1986 (c. 64). The objective was to extend the scope of the public order offences for which the MOA was meant to deal with while dealing with acts of nuisance and inappropriate behaviour in general. It is to be noted that there is a defence of "reasonable conduct" which acts as a limited safeguard for freedom of expression, speech and assembly.

[8] See *Malcomson v. Mehta*, Note 9 at para. 54, where the then Judicial Commissioner Lee Seiu Kin was also of this view. See also, *Chee Siok Chin and Others v. Minister for Home Affairs and Another* [2006] 1 SLR 582; [2005] SGHC 216 (High Court). "The manifest intent and purpose of ss 13A and 13B of the MOA were to promote good order in public places. It is the nature of the conduct and its [actual or likely] effect on "any person" that grounds the offence." *Ibid.* at 76. "The fact that Parliament did not define the word "harassment" in ss 13A and 13B of the MOA is a strong indication that this word, like the words "insult" and "abusive", is intended to be accorded a common-sense meaning. Harassment describes determined conduct which is directed at persons and is calculated to produce discomfort and/or unease and/or distress." *Ibid.* at 124, citing and following *Malcomson v. Mehta*.

[9] [2001] 4 SLR 454; [2001] SGHC 308 (High Court).

[10] *Ibid.* at 464, para. 31.

[11] *Ibid.*

[12] The latter bases have variously been used to deal with harassment or stalking cases with a certain degree of success. However, they are inadequate, unsatisfactory and simply not meant to deal with such cases. For example, trespass requires the threat or use of force or physical contact which will exclude causing *serious* annoyance, alarm or emotional or mental distress. Similarly, the tort or crime of intimidation or other relevant crimes, in particular, "offences affecting the human body" that relate to actual threats or acts of harm to the person, under the Penal Code (Cap. 224) or other specific provisions under existing legislation. On the other hand, private nuisance requires an interference with the use or enjoyment of land rather than anything to do with the person.

[13] I.e., making stalking and cyberstalking offences with criminal sanctions will serve as a stronger deterrent against such conduct, as they will provide additional deterrence than only the remedies that can be obtained *via* civil actions.

[14] [2001] SGDC 32 (District Court) [2001] 2 SLR 342; [2001] SGHC 69 (High Court).

[15] Section 3 makes it an offence to obtain unauthorised access to computer material, section 6 makes the unauthorised use or interception of computer services an offence, and under section 7, the unauthorised obstruction of the use of a computer is also an offence. Punishments are in the form of a fine, imprisonment or both.

[16] Under section 64(d), "family violence" includes "causing continual harassment with intent to cause or knowing that it is likely to cause anguish to a family member, but does not include any force lawfully used in self-defence, or by way of correction towards a child below 21 years of age". As in other legislative provisions, there is no legal definition of the word "harassment", which means that it is given only an ordinary meaning in the context of the case to describe the type of actions that evidences violence. This is especially clear when it is preceded with the adjective "continual", which is often part of the meaning of the word "harassment" in a legal definition.

[17] The willful violation or contravention of a PO or EO constitutes a criminal offence (section 64(8)),

[18] Under section 64, "family member" means: (a) a spouse or former spouse of the person; (b) a child of the person, including an adopted child and a step-child; (c) a father or mother of the person; (d) a father-in-law or mother-in-law of the person; (e) a brother or sister of the person; or (f) any other relative of the person or an incapacitated person who in the opinion of the court should, in the circumstances, in either case be regarded as a member of the family of the person".

[19] Section 33(1) states that: "Any moneylender who, personally or by any person acting on his behalf, harasses or intimidates his debtor, any member of the debtor's family or any other person in connection with the loan to the

debtor at, or watches or besets, the residence or place of business or employment of the debtor, the member of the debtor's family or that other person, or any place at which the debtor receives his wages or any other sum periodically due to him, shall be guilty of an offence". The punishment is fine, imprisonment or both.

[20] [1996] 1 SLR 510; [1996] SGHC 30.

[21] For more moneylending cases involving harassment or intimidation, see e.g., *Kan Chee Seng v. PP* MA 117/98/01; *PP v. Tee Choon Lian* MA 338/95/01; *Chan Kuan Swee v. PP* MA 219/95/01; *Ng Kum Kong v. PP* MA 132/2001/01; and *Lau Tian Heng v. PP* MA 229/2001/01.

[22] Section 13D(1) states that: "Any person who in a public place or in a private place…uses any indecent, threatening, abusive or insulting words or behaviour towards a public servant in the execution of his duty as such public servant; or distributes or displays to a public servant in the execution of his duty as such public servant any writing, sign or other visible representation which is indecent, threatening, abusive or insulting,
shall be guilty of an offence". Punishment is in the form of a fine or imprisonment.

[23] Although the most common profile of the stalker and the victim is male and female respectively. But see Evonne von Heussen, *The Law and 'Social Problems': The Case of Britain's Protection from Harassment Act 1997*, 1 Web JCLI (2000), available at: http://webjcli.ncl.ac.uk/2000/issue1/vonheussen1.html. The writer analyses the de-legitimising effect of legislation and the phenomenon of female stalking based on a variety of reasons not necessarily relational or even romantic. See also, B. Stanko, *Men Who Beat the Men Who Love Them - Battered Gay Men and Domestic Violence*, 33 *British Journal of Criminology* (1993), where it is made clear that domestic violence knows no gender or relational distinction.

[24] Section 13A states that: "Any person who in a public place or in a private place, with intent to cause harassment, alarm or distress to another person uses threatening, abusive or insulting words or behaviour; or displays any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that person or any other person harassment, alarm or distress, shall be guilty of an offence and shall be liable on conviction to a fine". Compare this provision to section 4 of the UK Public Order Act of 1986, which requires *proof of purpose* and expressive behaviour.

[25] Section 13B states that: "Any person who in a public place or in a private place uses threatening, abusive or insulting words or behaviour; or displays any writing, sign or other visible representation which is threatening, abusive or insulting, within the hearing or sight of any person likely to be caused harassment, alarm or distress thereby shall be guilty of an offence and shall be liable on conviction to a fine". Compare this to section 5 of the UK Public Order Act of 1986, which requires expressive behaviour and *physical proximity* (i.e. immediacy requirement); see also section 4A, inserted by section 154 of the U.K. Criminal Justice and Public Order Act of 1994.

[26] Section 13C states that: "Any person who in a public place or in a private place uses towards another person threatening, abusive or insulting words or behaviour; or distributes or displays to another person any writing, sign or other visible representation which is threatening, abusive or insulting, with intent to cause that person to believe that immediate unlawful violence will be used against him or another person by any person, or to provoke the immediate use of unlawful violence by that person or another person, or whereby that person is likely to believe that such violence will be used or it is likely that such violence will be provoked shall be guilty of an offence and shall be liable on conviction to a fine."

[27] Section 14A states that: "Any person who makes a telephone call to an emergency telephone number with intent to annoy, abuse, threaten or harass any person who answers the telephone call shall be guilty of an offence and, subject to subsection (3), shall be liable on conviction to a fine…or to imprisonment…or to both." This provision still does not fully address the concerns raised in Parliament by Dr. Kanwaljit Soin and Assoc. Prof. Ho Peng Kee of the failure under the then proposed sections 13A-B in dealing with phone harassment. See Singapore Parliamentary Reports Vol. 65 (1996) at 701-702.

[28] Ms. Indranee Rajah, MP for Tanjong Pagar, gave the example of silent phone calls in the night, unwanted flowers and gifts and calls from strangers instigated by the alleged stalker. See Parliamentary Debates Singapore Official Report: Tenth Parliament, Part I of First Session, Volume 74, 17 May 2002, available at: http://www.parliament.gov.sg.

[29] See e.g., *Allen i*n relation to such crimes as the infliction of "bodily harm" and "assault". Other forms of legal redress under Singapore law involve, for instance, a private summons or the application of the Criminal Procedure Code (Cap. 68), which addresses threats such as harm and trespass. These are incidental recourses only and are not specific to stalking, and they are also of limited use (i.e. only if the elements of the specific offence is made out). Other Penal Code offences that may be applicable depending on the circumstances includes criminal behaviour that can sometimes be displayed during a stalking such as assault (section 351), outrage of modesty (section 354), house trespass (section 442), defamation (section 499), criminal intimidation (section 504), and criminal intimidation by anonymous electronic mail (section 506).

[30] For our purposes "acts" can include "words". For another attempt at a definition, see the U.S. Department of Justice (DOJ), *Report on Cyberstalking: A New Challenge for Law Enforcement and Industry* (1999), available at:

http://www.usdoj.gov/criminal/cybercrime/cybertstalking.htm. The U.S. DOJ defines stalking as repetitive, threatening and/or harassing behavior by an individual generally as a means to control his or her victim. Stalking consists of a course of conduct that is directed at the victim in order to cause the victim fear, injury or death, and where a reasonable person would experience the same or similar fear, and where the perpetrator must know, or should know, that his behavior would cause the victim such fear. Cyberstalking refers to the use of the Internet, e-mail, or other electronic communication devices to stalk another person.

[31] See e.g., Jennifer Starr, *E-Mail Harassment - Available Remedies and Proposed Solution*, 39 Brandeis L.J. 317 (2001).

[32] Anon., *Who's Watching You - Spyware and Stalkers*, Newsletter of the Stalking Resource Center, Volume **5,** Number 1, Summer 2005, available at: http://www.ncvc.org/src/main.aspx?dbID=DB_WhosWatchingYou--SpywareandStalkers128.

[33] There are many different ways of compartmentalising stalkers, which goes to show how diverse the profiles can be and how varied the motives are. See further, *Cyber911 Emergency: Cyberstalker Profile* at: http://www.wiredsafety.org/cyberstalking_harassment/stalker.html, which categorizes stalkers into three basic types: Obsessional, Delusional and Vengeful.

[34] The American Heritage Dictionary of the English Language (4th ed., Houghton Mifflin Company, 2000).

[35] E.g., distinguish a reporter from a paparazzi. See Dan Whitcomb, *Schwarzenegger Signs Calif Anti-Paparazzi Law*, Reuters, 1 October 2005, available at: http://news.yahoo.com/news?tmpl=story&u=/nm/20051001/people_nm/paparazzi_dc_1; *Schwarzenegger Signs Law Aimed at Paparazzi Wallets*, Reuters, 2 October 2005, available at: http://www.nytimes.com/2005/10/02/national/02paparazzi.html; and *Calif Enacts Anti-Paparazzi Law*, Japan Today, 2 October 2005, available at: http://www.japantoday.com/e/?content=news&cat=8&id=350965. This is an example of an effective package of measures against a known category of offender.

[36] E.g. preventative and protective measures and even rehabilitative measures are more appropriate than, for instance, monetary remedy in terms of fines or compensation. Hence, the solution is prevention, by making it unlawful to stalk; and protection, if the stalking has in fact begun such as through the use of restraining orders (or if the stalker is irrational or mentally disturbed, then through court powers to order mental evaluation or treatment).

[37] To put it another way, the objectionable act in relation to stalking is the course of behaviour rather than the ends to be attained.

[38] K.G. McAnaney, L.A. Curliss and A.E. Abeyta-Price, *From Imprudence to Crime: Anti-Stalking Laws*, 68 *Notre Dame Law Review* 819, 821-823 (1993). The writers state that: "Stalkers can be obsessed fans, divorced or separated spouses, ex lovers, rejected suitors, neighbours, co-workers, classmates, gang members, former employees, disgruntled defendants, as well as complete strangers." See also, Amy C. Radosevich, *Thwarting the Stalker: Are Anti-Stalking Measures Keeping Pace With Today's Stalker?*, U. Ill. L. Rev. 1371, 1377-1380 (2000); and Rebecca K. Lee, *Romantic and Electronic Stalking in a College Context*, 4 Wm. & Mary J. of Women & L. 373 (1998). See further, Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, Stan. Tech. L. Rev. 2 (2004) at Part II; and Catherine E. Smith, *Intentional Infliction of Emotional Distress: An Old Arrow Targets the New Head of the Hate Hydra*, 80 Denv. U.L. Rev. 1 (2002), where the writer likens cyberstalking to a new head of the Hate Hydra.

[39] The act or behaviour itself is not enough because, as we have seen, there is a fine and blurry line between stalking behaviour on the one hand and excessive ardour or interest on the other.

[40] Subjectivity can come into the equation by applying the objective test to the facts and circumstances of the specific case. For example, if the perpetrator actually knew the effects his actions can cause to the victim or he knew the victim's character, weaknesses or susceptibility to the type of attention concerned.

[41] There may be problems of precision, coherence and consistency, particularly when the treatment is compared to that in other jurisdictions. For example, are spammers "stalkers"? Are romantic pursuers "stalkers"? Is continuing despite a "no" stalking or mere ardour? Where is the line to be drawn? The "reasonableness" test is inevitably influenced by the cultural and social context. This is partly due to cultural and societal differences. It involves the balancing of rights while remaining flexible to achieve fairness in protection. As it is an offence based on perception, sometimes it may not be clear-cut, especially in the ardent admirer scenario.

[42] Anti-stalking legislation is difficult to draft as its nature is imprecise and behaviour that is ordinarily normal can become sinister taken in context. "[T]he difficulty in defining stalking as a concept lies in its paradoxical status as an act that is ambiguously located somewhere between crime and conformity". See E. Ogilvie, *Stalking: Legislative, Policing and Prosecution Patterns in Australia* (Australian Institute of Criminology, 2000) at page 12. It is also difficult to determine the type of effect that merits any sort of legal sanction, after weighing the pros and cons to social interaction and contact to personal privacy and peace.

[43] See Lorraine Sheridan, *What is Stalking? The Match Between Legislation and Public Perception*, Paper presented at the Stalking: Criminal Justice Responses Conference convened by the Australian Institute of

Criminology and held in Sydney, 7-8 December 2000. The writer noted the major differences between the stalking laws of the U.S., U.K. and Australia. The U.S. Model Code requires the victim to fear bodily injury or death in order to be invoked, but provides no definition of stalking; the England and Wales Protection From Harassment Act is loosely framed and does not require evidence of intent or fear of physical harm; and most of the Australian legislation offers clear guidance in list form as to what constitutes stalking and has an intent requirement.

[44] The only Federal Legislation that addressing stalking is the Interstate Domestic Violence / Stalking provisions under 18 USC §2261 and §2261A respectively, which makes it a federal crime for a person to cross state lines to commit domestic violence on a spouse or intimate partner or to stalk another person ("intent to kill, injure, harass, or intimidate"). The effects are limited as, for instance, the victim of a stalker must be in reasonable fear of the death of, or serious bodily injury to, that person or a member of their immediate family, spouse or intimate partner. Punishment includes up to 5 years in prison for stalking, up to 10 years in prison for stalking with a dangerous weapon or if serious bodily injury occurs, up to 20 years if permanent disfigurement or a life-threatening injury occurs, and life in prison if death results from the stalking. The act also makes a restraining order issued in one State enforceable in other States. It is interesting to note the reference under §2261A to the use of "the mail or any facility of interstate or foreign commerce". Unfortunately, other than that ambiguous statement, there is no other reference to the communications or surveillance medium offered by modern technology. See also, 18 USC §875(c) (Interstate Communications), which makes it a federal crime, punishable by up to five years in prison, to transmit in interstate or foreign communications, any threat to kidnap or injure another person; and 47 USC §223(a)(1)(C) (Harassing Telephone Calls in Interstate Communications), which makes it a federal crime, punishable by up to two years in prison, to use a telephone or other telecommunications device to annoy, abuse, harass, or threaten another person at the called number. For an overview of U.S. State legislation, see Aaron Burstein, *Annual Review of Law and Technology: III. Cyber Law: B. Cybercrime: A Survey of Cybercrime in the United States*, 18 Berkeley Tech. L.J. 313, 319 (2003); Kimberly Wingteung Seto, *How Should Legislation Deal With Children As the Victims and Perpetrators of Cyberstalking?*, 9 Cardozo Women's L.J. 67, 80-91 (2002) ("Part V. Current Legislation On Cyberstalking"); and Joseph C. Merschman, *The Dark Side of the Web: Cyberstalking and the Need For Contemporary Legislation*, 24 Harv. Women's L.J. 255 (2001). See also, Lisa A. Karczewski, *Review of Selected 1998 California Legislation: Crimes: Stalking in Cyberspace: The Expansion of California's Current Anti-Stalking Laws in the Age of the Internet*, 30 McGeorge L. Rev. 517 (1999), for the California experience. California, which is the home of many celebrities, is at the forefront of anti-stalking, cyberstalking and paparazzi legislation.

[45] See the breakdown of State legislation at the Working to Halt Online Abuse (WHO@) Cyberstalking web site at: http://www.haltabuse.org/resources/laws/index.shtml. See also, The National Center for Victims of Crime's Stalking Resource Center web site at: http://www.ncvc.org/src/main.aspx?dbID=DB_State-byState_Statutes117 (for Criminal Stalking Laws by State); and http://www.ncvc.org/src/main.aspx?dbID=DB_CivilStalkingLaws188 (for Civil Stalking Laws by State). See also, Shonah Jefferson & Richard Shafritz, *A Survey of Cyberstalking Legislation*, 32 U. West. L.A. L. Rev. 323 (2001) 323, an article that gives a brief overview of the stalking legislation in the U.S. (327-9), cyberstalking legislation in the U.S. (329-334), and stalking laws in England and Wales (335-6), Scotland (336-7), and Canada (337) as of 2001. See further, Craig Lee and Patrick Lynch, *Cyberstalking - Is it Covered by Current Anti-Stalking Laws?*, available at: http://gsulaw.gsu.edu/lawand/papers/su98/cyberstalking/.

[46] See Shonah Jefferson and Richard Shafritz, *A Survey of Cyberstalking Legislation*, 32 U. West. L.A. L. Rev. 323, 328 (2001); and Keirsten L. Walsh, Comment, *Safe and Sound at Last?*
Federalized Anti-Stalking Legislation in the United States and Canada, 14 Dick. J. Int'l L. 373, 386 (1996). See also, the U.S. DOJ Report on Cyberstalking (1999) at Note 30; and the National Center for Victims of Crime, Infolink: Stalking and the Law, available at: http://www.ncvc.org/Infolink/Info71.htm.

[47] Often through a physical or visible proximity requirement.

[48] Note the requirement to prove the actual effect on the victim as well as the more severe effect required of the victim.

[49] There may be a problem here with instigation cases (i.e. cyber-harassment though third parties).

[50] Note the "reasonable person" test and the wider category of 'effects' criteria taken from the perspective of the victim.

[51] In 1992, the U.S. Congress enacted legislation which required the Attorney-General, through the National Institute of Justice, to conduct research on the issue of stalking and to develop and distribute among the states a constitutional and enforceable model anti-stalking code. (U.S. Departments of Commerce, Justice, State, the Judiciary and Related Agencies Appropriations Act for Fiscal Year 1993, Public Law 102 - 395, 109[b]). In October 1993, the final summary report of the *Project to Develop a Model Anti-Stalking Code for States* was presented to the National Institute of Justice. This was the end product of the 1992 legislation. The U.S. federal government's Anti-Stalking Code of 1993 legally defines the crime in the following manner: "[Stalking is] a knowing, purposeful course of conduct directed at a specific person that would cause a reasonable person to fear bodily injury or death to himself or herself or a member of his or her immediate family." The enactment of a

federal cyberstalking statute is complicated by Constitutional considerations, particularly First Amendment considerations. See, Ashley Packard, *Does Proposed Federal Cyberstalking Legislation Meet Constitutional Requirements?*, 5 Comm. L. & Pol'y 505 (2000).

[52] Section 2 of the Model Anti-Stalking Code for States (Model Code) defines a stalker as: "Any person who purposefully engages in a course of conduct directed at a specific person that would cause a reasonable person to fear bodily injury to himself or herself or a member of his or her immediate family or to fear the death of himself or herself or a member of his or her immediate family; and has knowledge or should have knowledge that the specific person will be placed in reasonable fear of bodily injury to himself or herself or a member of his or her immediate family or will be placed in reasonable fear of death of himself or herself or a member of his or her immediate family; and whose acts induce fear in the specific person of bodily injury to himself or herself or a member of his or her immediate family or induce fear in the specific person of the death of himself or herself or a member of his or her immediate family [i.e. a spouse, parent, child, sibling, or any other person who regularly resides in the household or who within the prior six months regularly resided in the household]…"

[53] "Course of conduct" is defined under section 1 of the Model Code as: "[R]epeatedly [i.e. on two or more occasions] maintaining a visual or physical proximity to a person or repeatedly conveying verbal or written threats or threats implied by conduct or a combination thereof directed at or toward a person…"

[54] Although the degree to which States have adopted the Model Anti-Stalking Code varies, most States define stalking as the "willful, malicious, and repeated following and harassing of another person." It involves a series of individual acts that accumulate and build on one another. Most States require the following three elements to be satisfied: threatening behavior, a course of conduct and intent to cause fear.

[55] See Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws* (4 September 2006), bepress Legal Series working paper 1689, available at: http://law.bepress.com/expresso/eps/1689/.

[56] At least one attempt had stalled. See the proposed Just Punishment for Cyberstalkers Act of 2000 ("Revises stalking provisions of the Federal criminal code to prohibit a person: (1) from traveling across a State line or within the special maritime or territorial jurisdiction of the United States with the intent to injure or harass another person and place that person in reasonable fear of death or serious bodily injury to the person or a member of his or her immediate family; or (2) with the intent to kill or injure a person in another State or to put such person in reasonable fear of death or serious bodily injury, from using or causing another to use the mail or any facility of interstate or foreign commerce to place that person in reasonable fear of death or serious bodily injury to the person, a member of his or her immediate family, or a spouse or intimate partner." Available at the Library of Congress (THOMAS) web site at: http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN02991:@@@L&summ2=m&.

[57] See e.g., Notes 30 and 54. See also, the *Stalking and Domestic Violence: Report to Congress* (2001), available at the National Conference of State Legislatures web site at: http://www.ncjrs.org/pdffiles1/ojp/186157.pdf. See further, the National Conference of State Legislatures web site resource on State Computer Harassment or "Cyberstalking" Laws, available at: http://www.ncsl.org/programs/lis/cip/stalk99.htm.

[58] Interstate Communications Act, 18 U.S.C. § 875(c). In 2006, the Violence Against Women and Department of Justice Reauthorization Act amended the Communications Act by prohibiting certain types of communications including anonymous annoying electronic messages. But again it is only a piecemeal solution and is not a comprehensive solution to the versatility of cyberstalking (i.e. its means and type).

[59] The Federal Telephone Harassment Statute, 47 U.S.C. § 223, which requires of anonymity and direct communication. The punishment is also one-dimensional (imprisonment) and arguable inadequate as a deterrence, or have any rehabilitative effect on stalkers (in appropriate cases).

[60] The Federal Interstate Stalking Punishment and Prevention Act, 18 U.S.C. § 2261A. Because the travel requirement is such an integral component of this law, it may not adequately address the situation where someone is stalked or threatened online without physical travel across state lines. The problem has led to calls for proposed legislation to amend the law in order to specifically proscribe cyberstalking. Also, *modus operandi* such as the instigation of third parties, impersonation of the victim and anonymous stalking are not addressed.

[61] The landmark case on stalking in the U.K. was the Court of Appeals case of *Burris v Azadani* [1995] 1 WLR 1372. It was that case that first recognised stalking as a tort, and an injunction was used to prevent further stalking by the perpetrator. In 1997, the House of Lords decided in the cases of *R v Burstow & R v Ireland* [1997] 3 WLR 534, that stalkers who cause psychological injury to their victims can be prosecuted for the criminal offences of causing actual bodily harm or grievous bodily harm even if they have not physically attacked their victim. See Deepa Bhabutta, *Anti-Stalking Legislation*, available at: http://www.lawgazette.com.sg/2002-2/Feb02-feature2.htm#f7. In the *Ireland* case, the perpetrator made repeated silent telephone calls to three women causing them to suffer from anxiety and depressive disorders. He was convicted of assault occasioning actual bodily harm contrary to section 47 of the Offences Against the Person Act of 1861 (OAPA) and was sentenced to three years of imprisonment. In the *Burstow* case, the perpetrator harassed a woman by making abusive telephone calls to her,

keeping watch at her house, stealing her cloths and scattered condoms in her garden. He was convicted of maliciously inflicting grievous bodily harm contrary to section 20 of the OAPA.

[62] The PHA came into force on 16 June 1997. It incorporates section 7(3A) added to the Act by section 44 of the Criminal Justice and Police Act 2001 and other amendments made by section 125 of the Serious and Organised Crime Act 2005. Subsections 3(3)-(9) came into force on 1 September 1998, section 7(3A) came into force on 1 August 2001, and sections 1(1A), 3A and 7(5) came into force on 1 July 2005. The full text of the Act is available on the HMSO web site at: http://www.opsi.gov.uk/acts/acts1997/1997040.htm. See also the Harassment Law web site at: http://www.harassmentlaw.co.uk/ for a useful resource.

[63] Section 7(2).

[64] "Course of conduct" is described under section 7(3) as involving, in the case of conduct in relation to a single person (section 1(1)), conduct on at least two occasions in relation to that person, or in the case of conduct in relation to two or more persons (section 1(1A)), conduct on at least one occasion in relation to each of those persons. Hence the requirement of repetitiveness (i.e. more than one incident) is preserved.

[65] Section 1(2).

[66] Sections 1(3) and 12. Although the Act deals with all kinds of harassment, it is the primary legislation that is used in stalking cases and it takes into account the unique problems of stalking.

[67] The PHA created two criminal offences and gave the civil courts the authority to award damages and issue injunctions in harassment cases. Section 3(1) of the Act provides for civil remedy and damages may be awarded for anxiety and financial loss caused by and resulting from harassment respectively (section 3(2)).

[68] As amended by section 43 Criminal Justice and Police Act 2001. It applies to offences committed from 11 May 2001 onwards. See also section 43 of the Telecommunications Act of 1984.

[69] Section 1(1) provides that: "Any person who sends to another person a letter, electronic communication or article of any description which conveys a message which is indecent or grossly offensive a threat or (iii) information which is false and known or believed to be false by the sender or any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature, is guilty of an offence if his purpose, or one of his purposes, in sending it is that it should…cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated." "Electronic communication" is described under section 1(2A) as including "any oral or other communication by means of a telecommunication system…*and any communication (however sent) that is in electronic form.*" [emphasis mine]. Finally, section 1(4) provides for a fine, imprisonment or both.

[70] See Michael J. Allen, *Look Who'stalking: Seeking a Solution to the Problem of Stalking*, 4 Web JCLI (1996), available at: http://webjcli.ncl.ac.uk/1996/issue4/allen4.html. The writer examined the phenomenon of stalking and the approaches being adopted to deal with it by victims, prosecutors and the courts in England and Wales. The article was written prior to the PHA and thus examined the civil remedies and criminal offences that were available prior to the statutory recourse as well as the government proposals that eventually led to the enactment of the PHA.

[71] See *Burnett* v *George* [1992] 1 FLR 525; *Pidduck* v *Molloy* [1992] 2 FLR 202); *Khorasandijan* v *Bush* [1993] 3 WLR 476; and *Burris* v *Azadani* [1995] 1 WLR 1372.

[72] See *R* v *Johnson (Anthony Thomas)*, The Times, May 14, 1996; but contrast it to *Madden* [1975] 3 All ER 155. See also *Allen*, Note 73 at Part IV.

[73] *Wilkinson v Downton* [1897] 2 QB 57 (harassment affecting health); *Burnett* v *George* [1992] 1 FLR 525; *Burris* v *Azadani* [1995] 1 WLR 1372. See also, T. Lawson-Cruttenden , *The Final Emergence of the Tort of Harassment?*, Family Law 625 (1995); and John Murphy, *The Emergence of Harassment as a Recognised Tort*, 143 New LJ 926 (1993).

[74] Equivalent to sections 1 to 7, which applies to England and Wales. Section 8 empower the Scottish civil courts to award damages or make Interdicts (Scottish Injunctions) and section 11 empowers Scottish criminal courts dealing with such cases to make preventative non-harassment orders. Breach of the interdict or order constitutes a criminal offence punishable with imprisonment of up to 5 years. See a Scottish government sanctioned research report on Stalking and Harassment in Scotland (research into the existing criminal and civil law procedures and practices in relation to stalking and harassment) (15 November 2002), available at:
http://www.scotland.gov.uk/library5/justice/sahs-00.asp
http://www.scotland.gov.uk/Publications/2002/11/15756/13113; and
http://www.scotland.gov.uk/library5/justice/sahs-04.asp or
http://www.scotland.gov.uk/Publications/2002/11/15756/13117.

[75] It came into force on 17 June 1997. For the full text of the Act, see the OPSI web site at:
http://www.opsi.gov.uk/si/si1997/19971180.htm.

[76] Found under "Part VIII: Offences Against the Person and Reputation" of the Code, available at: http://laws.justice.gc.ca/en/C-46/42644.html. For a detailed examination of the legislative history of section 264 of Canada's Criminal Code, see Bruce A. MacFarlane, *People Who Stalk People*, 31 UBC Law Review 37 (1997).

See also, Keirsten L Walsh, *Safe and Sound at Last? Federalized Anti-stalking Legislation in the United States and Canada*, 14 Dick. J. Int'l L. 373 (1996).

[77] The "reckless" standard is higher than that of a "reasonable man" standard. Note that fear for safety is probably equivalent to fear of violence or harm (e.g. it can encompass fear of sexual assault), but is not as narrow as fear of injury or death.

[78] The first two conducts appear to require more than one incident while the latter two do not, probably due to the uncertain and indefinite duration involved in the acts and the aggravated nature of the threat respectively. There is no reference to electronic forms of stalking, although it is possible to apply the existing provisions to the cyberspace context.

[79] Section 264(3).

[80] In New Zealand, stalking may be addressed to some extent by existing legislation such as the Harassment Act of 1997, the Domestic Violence Act of 1995, the Telecommunications Act of 2001 and the Crimes Act of 1961. There have not been any test cases on cyberstalking under these pieces of legislation.

[81] See the Harassment Law web site at: http://www.harassment-law.co.uk/australia.htm. See also, Caslon Analytics, *Cyberstalking*, December 2005, available at: http://www.caslon.com.au/stalkingnote2.htm#avos, for a brief summary of state enactments on stalking.

[82] No. 18 of 1999. Assented to on 30 April 1999. Queensland was the first Australian State to enact anti-stalking legislation, which it did in 1993. These consist of amendments under the new Chapter 33A on "Unlawful Stalking" which contains sections 359A-F. The old version was in the Queensland Criminal Code Act of 1899 (section 359A). Note, however, the restriction to apprehension or fear of violence. The other States also have stalking laws but they tend also to be conservative. For example, The Australian Capital Territory Crimes Act of 1900 (section 34a), the Northern Territory Criminal Code Act of 1997 (section 189), South Australia Criminal Law Consolidation Act 1935 (section 19AA), Victoria Crimes Act of 1958 (section 21A), the Western Australia Criminal Code Act of 1913 (sections 338D-E), and the Tasmania Criminal Code Act of 1924 (section 192) only restricts stalking to apprehension or fear of mental and physical harm, while the New South Wales Crimes Act of 1900 (section 562A-B) restricts stalking to fear of personal injury. Obviously, none of the earlier legislative provisions refer to the use of the electronic medium to stalk. Only recent subsequent amendments, such as those in Queensland and Victoria, refer to the "use of technology" or "electronic messages".

[83] These appear descriptive rather than mandatory and thus have more the effect of illustrations than as prerequisites. The list is not meant to be exhaustive.

[84] But no specific reference to surveillance technology.

[85] "Detriment" is defined under section 359A to include: "[A]pprehension or fear of violence to, or against property of, the stalked person or another person; serious mental, psychological or emotional harm; prevention or hindrance from doing an act a person is lawfully entitled to do; compulsion to do an act a person is lawfully entitled to abstain from doing."

[86] "Circumstances" is defined under section 359A to mean: "[T]he alleged stalker's circumstances; the circumstances of the stalked person known, foreseen or reasonably foreseeable by the alleged stalker; the circumstances surrounding the unlawful stalking; any other relevant circumstances."

[87] All State legislation requires a high effects threshold, often requiring fear, apprehension or mental/physical harm/injury. Queensland is unique in that the intention of the stalker to cause a stalking effect on the victim is immaterial to the offence and hence is "most generous for the prosecution", while other States require the specific intention to cause those effects. However, unlike other states, Queensland require the harm threatened to be "serious". See Daniel Sullivan, *A Critical Analysis of Queensland's Cyberstalking Legislation*, Computers and Law, June 2002, at page 7.

[88] For an examination of the changes that the Queensland Criminal Code (Stalking) Amendment Act of 1999 made to the original section 359A of the Queensland Criminal Code Act of 1899, see Sally Kift, *Stalking in Queensland: From the Nineties to Y2K*, 11 Bond L.R. 144 (1999).

[89] Section 21A of the Victorian Crimes Act of 1958 is available at the Austlii web site at: http://www.austlii.edu.au/au/legis/vic/consol_act/ca195882/s21a.html.

[90] The Victorian Parliament passed the Crimes (Stalking) Act of 2003 in December 2003 which supplement the 1994 stalking legislation. They address stalking through electronic means and amend the Victorian Crimes Act of 1958. *Ibid.*

[91] Japan's Law on Proscribing Stalking Behaviour and Assisting Victims of 2000. See *Nga at p. _*.

[92] This appears to be a set and exhaustive list; hence, at least one of those activities is required as a pre-requisite element to prove stalking.

[93] There is no reference to what type of surveillance, but it may be implied that it can transpire in any form or method, including through the use of modern technology.

[94] Report from the Law Reform Commission of Hong Kong, Privacy Sub-Committee, examining existing Hong Kong laws affecting privacy and making recommendations and proposals to provide protection against stalking. See Note 98, below.

[95] *Stalking*, The Law Reform Commission of Hong Kong Report (October 2000), at page 5, available at: http://www.worldlii.org/hk/other/hklrc/reports/2000/3/stalk-Chapter-6.html or http://www.worldlii.org/cgi-worldlii/disp.pl/hk/other/hklrc/reports/2000/3/stalk%2dChapter%2d6.html.

[96] See Parliamentary Debates Singapore Official Report: Tenth Parliament, Part I of First Session, Volume 74, 17 May 2002, available at: http://www.parliament.gov.sg.

[97] See Kimberly Wingteung Seto, *How Should Legislation Deal With Children as the Victims and Perpetrators of Cyberstalking?*, 9 Cardozo Women's L.J. 67, 73-74 (2002) . See also, Carol E. Jordan, Karen Quinn, Bradley Jordan and Celia R. Daileader, *Stalking: Cultural, Clinical and Legal Considerations*, 38 Brandeis L.J. 513 (2000), for a background on, and a multi-faceted view of, stalking and its problems as well as possible solutions.

[98] However, ISPs should not be liable for the mere transmission of data or the offer of such service that incidentally constitutes cyberstalking behaviour or that facilitates it. ISPs already generally enjoy statutory immunity from most criminal and civil offences with some exceptions, under most jurisdictions. See Joanna Lee Mishler, *Cyberstalking: Can Communication via the Internet Constitute a Credible Threat, and Should an Internet Service Provider Be Liable if it Does?*, 17 Santa Clara Computer & High Tech. L.J. 115, 115-118 (2000). However, ISPs can still play a significant role in education, law investigation (e.g. providing evidence), and enforcement (e.g. limiting or prohibiting access).

[99] See EFF, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet*, March 2000, available at the EFF web site at: http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#TECH; in particular "Part II: Policy Framework and Legal Analysis" at "B. A Framework for Evaluating Unlawful Conduct on the Internet".

[100] I.e. repeat behaviour or threat, although recurrence or the threat thereof are often, but may not necessarily always be, a prerequisite. Much will depend on the nature of the behaviour or threat in question.

[101] The objective test will ensure that irrational stalkers or stalkers with mental problems can still be caught by the legislation and subject to legal 'remedies'.

[102] This will sieve out the so-called extra-sensitive 'victims'.

[103] I.e. consideration of other societal interests. *Ibid.* A threshold has to be maintained so that not any type of activity, even if it may affect others, are prohibited. Hence, acts which cause "worry" or "anger" and the like fall below the threshold of actionability. Even for annoyance, which is a borderline element, perhaps requiring it to be "serious" or "aggravated" may be fairer albeit that it may contribute to a little more uncertainty. Assoc. Prof. Ho Peng Kee: In the Singapore context, we must be careful. Because of our close proximity, Police must be very satisfied that they can practically be able to implement any anti-stalking or anti-harassment law. Otherwise, somebody just lingering around in the void deck may fall foul of that law.

[104] An illustrative list such as this one should include references to both surveillance and communications as well as to traditional and technological methods. Type of effect on the victim can also be included but is not necessary. For example, the behaviour can affect a reasonable person's freedom of movement.

[105] As an extension of Internet anonymity, it is also a conducive environment not only for the assumption of created identities (i.e. alter ego or online persona) but also of false identity and impersonation (i.e. identity theft). Hence, for example, a stalker may make postings on the internet in the name of the victim provoking reaction against the latter whether through the same fora or even in the real world by listing the victim's contact information. See Joanna Lee Mishler, *Cyberstalking: Can Communication via the Internet Constitute a Credible Threat, and Should an Internet Service Provider Be Liable if it Does?*, 17 Santa Clara Computer & High Tech. L.J. 115, 115-118 (2000), for some real life examples of such cases and for an analysis of "public forum" stalking.

[106] See Joseph C. Merschman, *The Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation*, 24 Harv.Women's L.J. 255, 260 (2001).

[107] The Australian State statutes of Queensland and Victoria provide examples, mainly relating to law enforcement or other government-related official functions.

[108] For example, a (limited) exemption for the media functioning in its capacity as such. See Sebastien Maury, *Developments in Combating Cyberstalking in Australia*, Internet Law Bulletin Vol. 6 No. 10 (February 2004) at page 127 and n.14. Another example are acts done in the reasonable conduct of lawful trade, business or occupation perhaps including spam and junk mail, which are more appropriately dealt with elsewhere (see e.g., the Australian Queensland provision as amended, section 359D(d)). In any case this will fail under the criteria of directedness and identified individuals. Some exceptions do not appear necessary as they do not seem in any way as constituting stalking or cyberstalking behaviour or that can be directed to an individual or threatening as such (e.g. *Ibid.* sections 359D(b)(c) on industrial disputes and political/public disputes). In such cases, they may be redundant.

[109] See the reasonable defence under sections 13A(2)(b) and 13B(2)(b) of the MOA. The U.K. Act provides for a conclusive defence where the Secretary of State (executive branch) certifies, based on certain requirements. See section 12 of the U.K. Act.
[110] Section 359D of the Canada Criminal Code.
[111] Maybe this can be done under the MOA itself (perhaps under the second rubric), provided that it is suitable given that the act relates to public order and nuisance or as a new provision under the Penal Code (Cap. 224).
[112] *Diana Lamplugh, Paul Infield*, Note __ at 860-863.
[113] *Ibid.* at 863-865.
[114] "The "list method" has the advantage of certainty and makes it easy for the courts, the potential offender, and the victim to ascertain whether certain activities will violate the law. The disadvantage, however, is that its very certainty creates rigidity. It defines stalking and/or harassment by reference to what activities those phrases are understood to encompass by the legislators at the time of the passing of the law, and it does not have the flexibility to change. The law would not be able to take into account new methods, such as cyberstalking. The "general prohibition" method, on the other hand, trades certainty for flexibility. Courts will adjudicate each case afresh by reference to what it understands stalking and harassment to mean. It achieves this, however, at the expense of some amount of uncertainty." *Ibid.* at 866-867.
[115] This can then also be followed by a list of judicial powers for graduated forms of treatment and/or punishment for both recurrent and aggravated offences respectively (including sending a respondent or an accused for mental assessment/treatment). Considered below.
[116] What constitutes stalking should be left to the courts to decide by applying the offence provision to the facts of each case, but non-exhaustive illustrations of cyberstalking and examples as well as updates of new forms of technology and possible methods of cyberstalking will provide some guidance to the courts. For example, in relation to Global Positioning System (GPS) and devices, see Laura Silverstein, *The Double Edged Sword: An Examination of the Global Positioning System, Enhanced 911, and the Internet and Their Relationships to the Lives of Domestic Violence Victims and Their Abusers*, 13 Buff. Women's L.J. 97 (2004/5). The problem with legislation being non-technologically neutral is that they fast become outdated in the face of ever-evolving technology and require update 'patches', which are often delayed by the legislative process and which render the provision unwieldy and unnecessarily complicated See *ibid.* at 105. Hence, in the U.S. for instance, state legislatures are under pressure to re-evaluate and re-write harassment or stalking laws to accommodate technological advancements. So a good model anti-stalking and anti-cyberstalking provision should avoid confining the acts concerned to any one or more type.
[117] It is beyond the scope of this paper to consider in detail the issues relating to computer forensics. This Part is meant to highlight the problems relating to it and how it relates to cyberstalking..
[118] Experts suggest that in cases where the offender is known, victims should send the stalker a clear written warning. Specifically, victims should communicate that the contact is unwanted and ask the perpetrator to cease sending communications of any kind.
[119] Victims may want to file a report with local law enforcement or contact their local prosecutor's office to see what charges, if any, can be pursued. They should save copies of police reports and record all contact with law enforcement officials.
[120] They should also collect all other forms of evidence and document all contact made by the stalker (e.g. record the dates and times of any contact with the stalker). Victims should also consider logging each communication by keeping a diary explaining the situation and their feelings and responses in more detail.
[121] However, again note the problems of filtering or blocking to the gathering of evidence. Other forms of avoidance include changing e-mail addresses, ISPs, and other contact information, as well as the use of encryption software or privacy protection programs.
[122] The individual victim will have to personally gauge how much contact he or she can take with the stalker without having to suffer unnecessary abuse in order to prevent future contact.
[123] Hence, for example, under section 10 of the Singapore Electronic Transactions Act (CAP. 88), an ISP ("network service provider") is not subject to any civil or criminal liability in respect of third-party material in the form of electronic records to which he merely provides access provided that such liability is founded on the "making, publication, dissemination or distribution" of such materials or any statement made in it. See also, Joanna Lee Mishler, *Cyberstalking: Can Communication via the Internet Constitute a Credible Threat, and Should an Internet Service Provider Be Liable if it Does?*, 17 Santa Clara Computer & High Tech. L.J. 115, 129-137 (2000); and Kimberly Wingteung Seto, *How Should Legislation Deal With Children As the Victims and Perpetrators of Cyberstalking?*, 9 Cardozo Women's L.J. 67, 92 (2002).
[124] The power to make a restraining order is found in section 5 of the U.K. Protection from Harassment Act., which is a new sentencing power and only available after a conviction to prevent future harassment.
[125] The U.K. stalking regime is underpinned by the *Crime & Disorder Act 1998* and the *Anti-social Behaviour Act 2003*. Under their provisions, the police or local authorities may seek an Anti-Social Behaviour Order (ASBO)

against an individual who may be engaging in activities that cause or is likely to cause "harassment, alarm or distress to one or more persons not of the same household".

[126] See Caslon Analytics, *Cyberstalking* (December 2005), available at: http://www.caslon.com.au/stalkingnote2.htm#avos.

[127] E.g., the U.K. Act allows victims of actual or apprehended stalking to seek civil remedies of damages and an injunction through the creation of a statutory tort of harassment. See section 3 of the Act. The breach of such an injunction constitutes a criminal offence and is punishable as such. The procedure should be based on existing show cause procedures and the standard of proof for a temporary order should be based on a *prima facie* case while a permanent order should require proof on a balance of probability.

[128] *Diana Lamplugh, Paul Infield*, Note __ at 867.

[129] Carol E. Jordan, Karen Quinn, Bradley Jordan and Celia R. Daileader, *Stalking: Cultural, Clinical and Legal Considerations*, 38 Brandeis L.J. 513, 578-579 (2000) at paragraphs 7 to 9, supporting a civil right of action.

[130] This requirement is due to the civil rights implications of such actions. An order for mandatory treatment should require a criminal conviction as it involves taking away the liberty of the person.

[131] There is a need for the law to specifically address the special circumstances that often relate to stalking cases. Stalking often stems from a form of mental or social abnormality. For instance, it often involves an unhealthy and uncontrollable obsession. This is separate from the question of whether the stalker has the requisite *mens rea* from telling right from wrong or from knowing the consequences of his or her actions. The difference between a normal cyberharasser and a cyberstalker, is that a harasser can move on and is to some extent in control of his or her emotions, whereas a stalker will more likely than not be a repeat offender. Sociopaths, social deviants, and the like, all potential profiles of stalkers, also do not respond to reason or normal incentives or deterrent measures. In a sense, they are also 'victims' of their mental state.

[132] A clearly important solution will be to give statutory powers to the courts to order a mandate psychiatric or mental evaluation for an alleged stalker, and if necessary, treatment coupled with probation or confinement. Perhaps the assessment, supervision, consultation and evaluation can, additionally, be required to be performed by a medical practitioner from an approved panel.

[133] In Singapore, this is already possible under the Criminal Procedure Code (Cap. 68), see sections 308 and 315. See also, the Mental Disorders and treatment Act (Cap. 178).

[134] The ordering of an evaluation can be done in the course of a trial, whether civil or criminal. For example, perhaps as part of proof of specific intent, if relevant; or to assist the court in deciding on the need for, or effectiveness of, interlocutory or final relief such as injunctions and restraining orders as opposed to some form of confinement, whether for treatment or as punishment.

[135] In that case, then a gradated model of punishment comes into the picture to, for example, give notice to the stalker that his or her attentions are not appreciated and should cease (e.g. through a warning and restraining order or cease and desist order) before more serious punishments will be considered or imposed (e.g. fines and imprisonment, especially for repeat or recalcitrant offenders). Keeping in mind that perpetrators may also stalk out of mental or personality disorder, the possibility of mandatory psychological evaluation with a view to mandatory treatment should also always remain an option. There should also be more severe punishments available for more malevolent stalkers (e.g. those that threaten or perpetrate harm or violence, to person or property).

[136] When dealing with stalkers, we are looking generally at two demographics; that is, there are two categories or profiles of stalkers: The normal and ordinary person who has given in to his or her emotions in relation to another; and the person with mental or psychological problems who has delusions or obsessions with respect to another. Different approaches should be taken for either demographic.

[137] The model allows for the use of a continuum of measures and charges that can be used by law enforcement officers to intervene at different stages as well. This is important as stalkers' behavior is characterized by a series of acts.

[138] A part of the solution will be to have a gradated form of punishment so that the individual should have a general right to privacy and if that is conveyed to the interested (but perhaps socially inept person) party in a more 'gentle' approach first as a warning (e.g. in the form a warning, or a protection order), followed by harsher penalties if the first warning is not effective. On the other hand, there can be more severe punishment for recalcitrant offenders.

[139] As noted previously, under sections 13A-B of the current Miscellaneous Offences Act, the penalties are insufficient as deterrence as well as to meet the needs of the stalker profile as they only simply provide for a fine. Moreover, victims cannot recover damages or costs in criminal proceedings brought under these provisions.

[140] But that may have civil rights implications. For an overview of existing offender registration and ASBO regimes in some jurisdictions, see Caslon Analytics, *Offender Registers* (March 2006), available at: http://www.caslon.com.au/offendersnote3.htm and http://www.caslon.com.au/offendersnote4.htm respectively.

[141] But this may be even more objectionable to civil rights activists if the registrants need not be convicted of an offence for it to be made.

[142] For a list of online harassment resources including web sites to educate the public in the fight against stalking and cyberstalking, see the Sexual Assault and Harassment Resources web site at: http://www.karisable.com/sashres.htm; and Cyberstalking Information at: http://www.vaonline.org/cyberstalking.html. See also, the Stalking victims web site (U.S.) at: www.stalkingvictims.com; Bully on-line at: www.bullyonline.org; Metropolitan Police Stalking Guide (U.K.) at: www.met.police.uk; and Anti-Stalking web site (U.S.) at: www.antistalking.com. See further, the Cyber Criminals Most Wanted web site at: http://www.ccmostwanted.com/topics/cstalk.htm; Cyberstalking and Internet Safety F&Q at: http://www.sfwa.org/gateway/stalking.htm; the Stalking Resource Center of the National Center for Victims of Crime web site at: http://www.ncvc.org;; and Cyberstalking Information web site at: http://www.stalking-research.org.uk/index.php.

[143] See EFF, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet*, March 2000, available at: http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#TECH, at "Part IV: The Role of Public Education and Empowerment".

[144] See *Nga B. Tran*, Note __ at 467, 469-70, 473-6, for the Japanese experience in stalking insurance and police training and education as well as the establishment of a task force to deal with cyberstalkers.

[145] Increasing the funding for computer training and equipment for local law enforcement agencies is one important solution. Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. Pa. Rev. 1003 (2001) at Part II.

[146] See e.g. the following web sites: www.getnetwise.org; www.americalinksup.org; www.cyberangels.org; www.parentech.org; and www.safekids.com.

[147] The Council of Europe (CoE) Convention of Cybercrime of 23 November 2001 is available at the CoE web site at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[148] For a continental European example, see Lambèr Royakkers, *The Dutch Approach to Stalking Laws*, 3 Cal. Crim. L. Rev. 2 (2000); and Marijke Malsch, *Stalking in the Netherlands*, Paper presented at the Stalking: Criminal Justice Responses Conference convened by the Australian Institute of Criminology and held in Sydney (7-8 December 2000), available at: http://www.aic.gov.au/conferences/stalking/Malsch.pdf.

[149] See *Nga B. Tran*, Note __at 459-62.

[150] Instigated or procured stalking (through third party culpable or innocent agents).

[151] Vicarious stalking (of a family, relative or friend of the victim).

[152] The tort of nuisance or even a computer misuse criminal provision may capture some, if not most, electronic acts that can have this effect.

[153] Mere annoyances, such as flaming behaviour, which is anti-social but that is quite the norm on the WWW, may be excluded on a balance of interests analysis and a criteria of "seriousness" can serve that purpose.

[154] In Europe, where privacy principles are quite well settled, some Western European countries have placed emphasis the intrusion upon the victim's peace of mind as a basis of an action for stalking (e.g. Norway, Belgium and Denmark). See *Malsch*, Note __ at page 3.

[155] Some legislation provides that a stalking effect can constitute a form of detriment, such as compelling the victim to do acts or to refrain from acts that are legal (e.g. the Australian Queensland provision as amended, section 359B(d)(ii) read with the section 359A(c)(d) definition (under the term: "detriment")).

[156] Actual knowledge (amounting to specific intent) and actual harm will most certainly constitute other criminal offences such as assault, battery and causing hurt, depending on the appropriate criminal provisions of the jurisdiction concerned.

[157] Including the power to make exceptions or conditions.

[158] This may encounter problems of proof, particularly causation and remoteness. For example, proof of costs can come in the form of therapy, loss of job, emotional distress, etc., which have to be linked to the stalker's acts.

[159] Explicit (words or deeds) or implicit (conduct) or both; and direct or indirect (e.g. through instigating third parties).

[160] Passivity or not doing something is also a unique feature of cyberstalking and should be relevant in this analysis as well. For instance, setting an electronic device to automatically monitor or contact a person can constitute a continuing event. The solution is also relevant, and this is where specific performance and injunctions will be useful.

[161] The inclusion of *serious* annoyance and alarm is due to the "psychological menace" that stalking can cause, which is often left out of most stalling legislation (e.g. US and Australia) that confines actionable stalking to fear of harm or mental distress. Annoyance and alarm has some precedent, for example, in the State legislation of Missouri and New Jersey in the U.S., see the 1993 US Task Force Report on Stalking, at Note _ at 21. See also Carol E. Jordan, Karen Quinn, Bradley Jordan and Celia R. Daileader, *Stalking: Cultural, Clinical and Legal Considerations*, 38 Brandeis L.J. 513, 578 (2000), at para. 5 ("serious annoyance").

[162] I.e. Objective person under the circumstances and in the context of the victim (e.g. relationship to the offender, offender's history, status and reputation, etc.). This is *not* the same as a requirement of actual awareness on the

part of the victim. Some laws (e.g. some States in the U.S.), for example, refer to the credibility of the threats (i.e. "credible threats"); however that may be too stringent a definition and it will only address the effect of fear but not of the reasonableness of *serious* annoyance or alarm on the part of the victim and that the stalker knows or should reasonably be aware that he or she is causing. Adjectives like *credible* (threat) or *serious* (harm) only makes standards even higher to prove stalking, however they are meant to perform the same functions of, for example, the reasonableness test.

[163] The proposal only deals with the substantive offence and direct criminal punishment or outcome. Procedural provisions relating to stalking such as police powers of investigation and the law of evidence are not included in this proposal. Additional criminal and civil redress such as temporary/permanent orders and medically-related orders are also not included here.

[164] It may also be useful to include factors for the court to consider in determining whether the course of conduct will have the objective reasonable effect on the target such as the number of occasions it was carried out, the frequency and duration and manner of the acts, the diversity and combination of the acts, circumstances under which they are carried out, and so on.

[165] This "protracted" element is unique to the Queensland legislation. "The gravamen of the offence is now that conduct on one protracted occasion is sufficient. All that is required is that 'conduct' be 'engaged in on any one occasion if the conduct is protracted [or particularly egregious in terms of time/intensity] or on more than one [separate] occasion. The provenance of this phrase is presumably the interpretation given to 'course of conduct' under section 21A of the Victoria *Crimes Act* 1958 by McDonald J in *Gunes v Pearson and Tunc v Pearson* (1996) 89 A. Crim. R. 297, where he stated that: "[A] 'course of conduct' which includes keeping the victim under surveillance, may comprise conduct which includes keeping the victim under surveillance for a single protracted period of time or on repeated separate occasions." See *Sally Kift, Stalking in Queensland: From the Nineties To Y2K* at page 151. In actuality, whether a conduct is protracted or whether it can actually be split up into, and considered as, separate actions on separate occasions constituting a course of conduct may be mere semantics.