

**This document is downloaded from CityU Institutional Repository,
Run Run Shaw Library, City University of Hong Kong.**

Title	Stalking the cyberstalkers in Hong Kong
Author(s)	Jay, Anita Ka Yan (謝家茵)
Citation	Jay, A. K. Y. (2013). Stalking the cyberstalkers in Hong Kong (Outstanding Academic Papers by Students (OAPS)). Retrieved from City University of Hong Kong, CityU Institutional Repository.
Issue Date	2013
URL	http://hdl.handle.net/2031/7178
Rights	This work is protected by copyright. Reproduction or distribution of the work in any format is prohibited without written permission of the copyright owner. Access is unrestricted.

Stalking the Cyberstalkers in Hong Kong

Anita Ka-Yan Jay*

Hong Kong, the world's top international financial centre, has nurtured a complex and constantly evolving information technology infrastructure. However, with better and greater use of technology come greater risks of cybercrimes. Cyberstalking is an example of cybercrime, which often places the victims in fear and may be a precursor to assault, rape or even murder. Nevertheless, there is currently no specific legislation in Hong Kong to regulate such deviant behaviour. As such, this article aims to critically examine the scope of the proposed anti-stalking legislation to determine whether cyberstalking is covered.

I. INTRODUCTION

A. Technological Advancement and Setbacks

Technology is an attribute of Hong Kong's (HK's) economic growth and success.¹ More specifically, the Internet has increasingly and significantly contributed to our everyday lives.² It, *inter alia*, provides endless amounts of (often free) information and entertainment, serves as a communication platform and facilitates business transactions. Such contribution enhances convenience and save costs that would otherwise be expended offline. Simultaneously, there is an unfortunate risk of (serious) abuse.³ In other words, there are both positive and negative aspects of the Internet. Moreover, with

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 statics and mobile forms of electronic and digital forms and channels of communication ... there is a greater likelihood

* LLB Year 4, School of Law, City University of Hong Kong; Editor-in-Chief, *CityULR*.

¹ Information Services Department, 'Innovation and Technology' *GovHK* (April 2013) <www.gov.hk/en/about/abouthk/factsheets/docs/technology.pdf> accessed 22 April 2013.

² R Broadhurst and P Grabosky, 'Computer-Related Crime in Asia: Emergent Issues' in R Broadhurst and P Grabosky (eds), *Cyber-Crime: The Challenge in Asia* (HK University Press, HK 2005) 1; P Grabosky and R Broadhurst, 'The Future of Cyber-Crime in Asia' in *Ibid* 347, the 'levels of connectivity area among the highest in the world' in HK.

³ Inter-Departmental Working Group on Computer Related Crime, *Report* (HK 2000) <www.info.gov.hk/archive/consult/2001/crime-e.pdf> accessed 12 February 2013, 1-2; Y Wang, 'Cybercrime on the Rise in Hong Kong' *Ecns* (30 January 2013) <www.ecns.cn/cns-wire/2013/01-30/47976.shtml> accessed 24 February 2013; KH Pun et al, 'Computer Crimes: What Everyone Should Know About Them' in Broadhurst and Grabosky (n 2) 200-1.

of, and a conducive IT infrastructure and computing environment for [cybercrimes] to perpetuate.⁴

As in other countries, cybercrimes in HK exist in various forms, ranging from illegal interference with computers through hacking and cracking to harassment. Other cybercrimes include, *inter alia*, fraud, theft, money laundering, publication of offensive material and more extreme cases of cyber terrorism and warfare. In particular, the existence and prevalence of cyberstalking have been highlighted in the Report on Stalking in 2000 (2000 Report)⁵ and in recent cases.⁶ Moreover, many people have also expressed disturbances through the media and the Consultation Paper on Stalking in December 2011 (Consultation Paper) issued by the Constitutional and Mainland Affairs Bureau (CMAB).⁷ In *Ko Kam Fai's case*, the defendant hacked into the victims' email accounts and obtained their personal information.⁸ He then bombarded them with unwanted mails, including obscene materials and threats, over a period of time. These amount to cyberstalking, which is abhorred by society because it 'demonstrate[s] sheer disrespect for human dignity and disregard of personal feelings of the victims'.⁹ Despite that, the defendant was sentenced for criminal intimidation and criminal damage, as (cyber)stalking is not a crime yet.

B. Cyberstalking Definition and Effects

Cyberstalking is a form of cybercrime, which usually refers to repetitive, harassing behaviour directed at another person using the Internet and other forms of electronic technology, including computers, phones, fax machines and global positioning systems (GPS).¹⁰

⁴ W Chik, 'Harassment Through the Digital Medium: A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking' (2008) 3:1 *Journal of International Commercial Law & Technology* 13, 14.

⁵ The Law Reform Commission of HK (LRC), *Report on Stalking* (HK 2000) <www.hkreform.gov.hk/en/docs/rstalk-e.pdf> accessed 13 February 2013, 35-46.

⁶ For stalking related cases, see K Foo, 'Lack of English Fails to Stop Park Stalker: A Jobless Man was Yesterday Given 12 Months' Probation for Stalking an American Woman in Tai Po' *The Standard – China's Business Newspaper* (HK 21 March 2012) <www.thestandard.com.hk/news_print.asp?art_id=120869&sid=>> accessed 19 February 2013. See also *HKSAR v Cheung Kwok Yip Peter* [2010] HKEC 268 (CA); *Ng Yiu Ki v Chan Yuk Fung* [2010] HKCU 1072 (DC); *HKSAR v Lo Kwok Wai* [2010] HKCU 2539 (CFI); *WLK v TMC* [2009] 5 HKC 438 (CA); *K v C (Ancillary Relief)* [2008] HKFLR 395 (DC); *SEB v ZX (Custody)* [2007] HKFLR 165 (DC); *HKSAR v Tsui Chu Tin John (No 2)* [2007] 3 HKC 478 (CA); *HKSAR v Tsui Chu Tin John* [2001] 3 HKC 378 (CA).

⁷ Constitutional and Mainland Affairs Bureau (CMAB), *Consultation Paper on Stalking (Consultation Paper)* (HK 2011) <www.cmab.gov.hk/en/upload/Consultation_Paper_on_Stalking_E.pdf> accessed 12 February 2013, 15-6.

⁸ *HKSAR v Ko Kam Fai* [2001] 3 HKC 181 (CA).

⁹ *Ibid* 184.

¹⁰ Chik (n 4) 16.

Cyberstalkers may obtain the victims' personal information¹¹ and then send unwelcome (possibly obscene and threatening) emails, mail bombs and/or virus. They may also harass victims in live chats, post (false) information of the victims on websites, bulletin boards, chat rooms, discussion forums and newsgroups as well as impersonate victims to solicit unwanted contacts from third parties.¹²

Cyberstalking has far-reaching and potentially devastating effects on the victims.¹³ Many well-known psychologists, including Mullen and Pathé have found that fearful victims (and possibly their close relatives) are often forced to change their lifestyle to avoid the stalkers, including moving homes, changing their numbers and jobs.¹⁴ According to psychologist Mary Lee, such fear often escalates to severe psychological distress, including the development of post-traumatic stress disorder.¹⁵ The change of lifestyle and emotional distress also frequently cause physical deterioration.¹⁶ Moreover, cyberstalking is likely to be a precursor to physical stalking and violence, including assault, rape or even murder.¹⁷ Accordingly, it is crucial to remember that cyberstalking is as serious as offline stalking, thus should be criminalised and regulated as much as stalking.

C. Cyberstalking Features

Despite being a species of stalking, it is worth noting that cyberstalking has its own unique features. Unlike stalking, cyberstalking does not involve any personal contact, which may in

¹¹ Includes name, email, telephone number, residential address and more. These may be obtained through simple web search, directories and hacks.

¹² TM Gregorie, 'Cyberstalking: Dangers on the Information Superhighway' *NCVC* (2001) <www.victimsofcrime.org/docs/src/cyberstalking---dangers-on-the-information-superhighway.pdf?sfvrsn=2> accessed 13 February 2013, 1.

¹³ *Consultation Paper* (n 7) 14.

¹⁴ P Li, 'The Criminalization of Stalking in Hong Kong' *HK Lawyer* (2012) <www.hk-lawyer.com/InnerPages_features/0/3756/2012/5> accessed 4 October 2012; AW Burgess and T Baker, 'Cyberstalking' in J Boon and L Sheridan (eds), *Stalking and Psychosexual Obsession: Psychological Perspectives for Prevention, Policing and Treatment* (John Wiley & Sons Ltd, West Sussex 2002) 205.

¹⁵ Lee Wing Ming Mary, 'S0243: My Response to the Consultation Paper on Stalking' (23 March 2012) <www.cmab.gov.hk/en/upload/stalking_submissions_volume2_en.pdf> accessed 13 February 2013.

¹⁶ 'Stalking Consultation Invites Views' *News.gov.hk* (19 December 2011) <www.news.gov.hk/en/categories/admin/html/2011/12/20111219_145328.shtml> accessed 13 February 2013; JR Meloy, 'When Stalkers Become Violent: the Threat to Public Figures and Private Lives' (2005) 156 *Criminal Lawyer* 3, 7; Burgess and Baker (n 14); Gregorie (n 12) 3.

¹⁷ ML Pittaro, 'Cyber Stalking: Typology, Etiology, and Victims' in K Jaishankar (ed), *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (CRC Press, Boca Raton Florida 2011) 283; J Clough, *Principles of Cybercrime* (Cambridge University Press, New York 2010) 366.

turn ‘encourage the projection of fantasy’ and escalation of detrimental effects.¹⁸ Cyberstalkers generally find it easier and less risky to stalk online, due to anonymity and lack of cross-border restrictions.

A portentous aspect of cyberstalking is the potential anonymity and stealth of cyberstalkers. Pseudonymity ‘can cause a loss of social inhibitions and constraints’, thus ‘facilitate[s], or even encourage[s]’ stalking behaviour.¹⁹ Besides spoofed email or IP addresses and untraceable proxy servers, cybercriminals use the ‘increasingly sophisticated and more readily available’ encryption tools to ‘avoid detection and ... impede evidence-gathering’.²⁰ As such, it is ‘difficult to ... identify, confront and arrest [the cyberstalkers] before matters get worse’.²¹

Another ominous aspect of cyberstalking is that it has ‘no territorial borders’.²² Cyberstalkers may be present and cause harm anywhere, as long as there is Internet connection. Unlike Tasmania,²³ the Criminal Jurisdiction Ordinance (Cap 461) (HK) does not, even after proposed amendments,²⁴ address the jurisdictional issues of cross-border cybercrimes. As such, there are uncertainties as to HK’s jurisdictional powers over cross-border cybercrimes.

These unique features, on one hand, afford lesser impediments to such deviant behaviour. On the other, they create (investigatory and evidentiary) challenges that are unique to cyberstalking. As such, cyberstalking ‘should be seen as a unique form of deviant behaviour

¹⁸ M McGrath and E Casey, ‘Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace’ (2002) 30 *Journal of the American Academy of Psychiatry and the Law* 81, 86.

¹⁹ Clough (n 17) 367.

²⁰ M Jackson, ‘Law Enforcement in Cyberspace: The Hong Kong Approach’ in Broadhurst and Grabosky (n 2) 266. There are other ways of being anonymous, such as removing digital evidence.

²¹ N MacEwan, ‘The New Stalking Offences in English Law: Will They Provide Effective Protection from Cyberstalking?’ [2012] *Criminal Law Review* 767, 772.

²² Secretary for Justice, Elsie Leung, ‘Keynote Address at the Symposium on “Internet Law in Hong Kong”’ (Department of Justice, 26 September 2003) <www.doj.gov.hk/eng/archive/pdf/sj260903e.pdf> accessed 11 February 2013.

²³ Criminal Code Act 1924 (AUS TAS) Sch 1 s 192A stipulates that Tasmania courts will have jurisdiction over a person who (cyber)stalks outside Tasmania and ‘there is a real and substantial link between the action taken and Tasmania’. See also Crimes Act 1958 (AUS VIC) s 21A(6)-(7).

²⁴ Legislative Council (LegCo), ‘Motion on the Draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 to be Moved by the Secretary for Security’ (LC Paper no CB(3) 193/02-03, 2002) <www.legco.gov.hk/yr02-03/english/hc/sub_leg/sc53/papers/sc530108cb2-193-e.pdf> accessed 24 February 2013.

which is completely distinct to other forms of stalking’,²⁵ thus deserves (special) attention, both in law and society.

Accordingly, Part II will examine and assess the legal position in HK to determine whether cyberstalking is covered and to what extent. This includes the existing cybercrime related legislation and the proposed anti-stalking legislation. Part III will explore the anti-cyberstalking legislation in the United States (US), Australia and the United Kingdom (UK). These jurisdictions are ‘larger and more technologically-matured jurisdictions’, where ‘[c]yberstalking has become a concern that has translated into law’.²⁶ Despite the general trend in including the cyber element in anti-stalking legislation, they are still disparate – some include synonyms of cyberstalking, some incorporate the term cyberstalking and some have separate provisions on cyberstalking. A comparative analysis will illustrate how different jurisdictions have dealt with the problem and also provide guidance on how HK should proceed on this issue.

Taking into account HK’s and other jurisdictions’ existing legal position, Part IV will underline the future steps that should be taken to tackle cyberstalking in HK. This includes improvement of the proposed anti-stalking legislation, effective enforcement, heightened awareness as well as local and international collaborative effort.

II. CYBERCRIME AND PROPOSED ANTI-STALKING LEGISLATION IN HK

A. Cybercrime Related Legislation

In HK, there are several legislation which deal with cybercrimes. The main Computer Crimes Ordinance (Ord no 23 of 1993) comprises the Telecommunications Ordinance (TCO) (Cap 106), the Crimes Ordinance (CO) (Cap 200) and the Theft Ordinance (TO) (Cap 210).

²⁵ M Wykes, ‘Constructing Crime: Stalking, Celebrity, “Cyber” and Media’ in Y Jewkes (ed), *Crime Online* (Willan Publishing, Devon 2007) 137; Pittaro (n 17) 279.

²⁶ Chik (n 4).

1. Telecommunications Ordinance

Section 27A(1) TCO prohibits ‘unauthorised access to computer by telecommunications’ and imposes a maximum fine of \$20,000. Any interception or alteration of communication is also prohibited.²⁷ However, cyberstalking may not involve such acts of hacking, interception or alteration of communication, but simply (after obtaining the victims’ information from other means) sending emails, spreading rumours, impersonating the victims for other purposes or other forms of indirect means.²⁸ Even if cyberstalkers have accessed without authorisation, the amount of fine is not huge and there is no imprisonment. As such, cyberstalkers (especially those who acts out of emotional wants) are unlikely to be deterred.²⁹

2. Crimes Ordinance

Section 60 CO forbids ‘destroy[ing] or damag[ing] any property’ without lawful excuse. More specifically, Section 59(1A) extends such meaning of criminal damage to the ‘misuse of a computer’ program or data and imposes a maximum penalty of ten years imprisonment.³⁰ Despite the possibility of imprisonment, cyberstalkers will not be convicted under this provision if there is no criminal damage. Moreover, damage may be done not to computers, but to other electronic devices.

Section 161 CO disallows access to the computer with ‘criminal or dishonest intent’ and imposes a maximum penalty of five years imprisonment. Compared to the other cybercrime legislation, it seems that this provision is the most pertinent in capturing cyberstalkers. A cyberstalker may and often obtain access to a computer ‘with intent to commit an offence’,³¹ such as to threaten and intimidate the victims. Alternatively, cyberstalkers may use a computer ‘with a dishonest intent to deceive’,³² such as impersonating the victim to solicit unwanted contact. However, these provisions are limited in scope in that it only applies to computers; cyberstalkers may access other electronic devices with a specific intent. Moreover, the requirement of criminal and dishonest intent is a high threshold, which will not be met by cyberstalkers who are delusional and incapable of forming the necessary intent;

²⁷ TCO ss 24, 25 and 27.

²⁸ Chik (n 4) 15.

²⁹ Ibid 16.

³⁰ Except arson and aggravated criminal damage.

³¹ CO s 161(1)(a).

³² CO s 161(1)(b).

delusional cyberstalkers may be ‘acting out of “love” for the victim, or out of a belief that he was, or was meant to be, bonded to the victim’ and/or may ‘truly believe himself to be loved by the victim, and is incapable of realising that the victim is being harassed as a result’.³³

Arguably, cyberstalkers may have a ‘view of dishonest gain’ and/or ‘dishonest intent to cause loss to another’.³⁴ Examples include the gain of attention and the loss of psychological and physical comfort. Again, a major loophole is that it does not cover cases where the cyberstalkers did not have the required intent. For example, the intention of erotomaniac stalkers is to establish an intimate relationship with the victim, rather than a dishonest one.³⁵

3. Theft Ordinance

Similar to CO, Section 11(3A) TO extends the meaning of unlawful damage in burglary to ‘causing a computer ... to function’ other than it should as well as altering, erasing or adding any program or data in the computer. These offences attract a maximum penalty of 14 years imprisonment. As mentioned above, cyberstalking may not involve damage to the computer, but merely harassment with the use of a computer. Moreover, it is highly unlikely for cyberstalkers to cause damage in ‘burglary’ as most of them stalk online in order to remain anonymous, thus lower the risks of detection. Having said that, cyberstalkers’ behaviour may escalate to physical stalking involving such kind of damage.

It seems that the existing HK cyber-related laws catch certain deviant behaviours.³⁶ Unfortunately, these piecemeal legislation (even if combined) do not combat cyberstalking specifically and effectively.³⁷ The existing legislation are limited in scope, where they either focus on certain acts, do not cover other electronic devices and/or requires a specific intent. As a result, these legislation will not always be an available recourse in cyberstalking cases.

³³ *Consultation Paper* (n 7) 20-1.

³⁴ CO ss 161(1)(c), (d).

³⁵ See PE Mullen, M Pathé, R Purcell and GW Stuart, ‘A Study of Stalkers’ (1999) 156 *American Journal of Psychiatry* 1244.

³⁶ Other laws with a cyber element include the Control of Obscene and Indecent Articles Ordinance (Cap 390) (HK), where s 2(1) is wide enough to include computer files or e-data (*HKSAR v Cheung Kam Keung* [1998] 2 HKC 156 (CFI)); the Copyright Ordinance (Cap 528) (HK); the Gambling Ordinance (Cap 148) (HK); the Unsolicited Electronic Messages Ordinance (Cap 593) (HK), which governs commercial electronic messages, thus inapplicable here.

³⁷ HK may adopt a comprehensive approach to regulate cybercrime, however, the basic principles of cyberspace legislation should be kept in mind. See KC Wong, ‘Computer Crime and Control in Hong Kong’ (2005) 14:2 *Pacific Rim Law & Policy Journal Association* 337, 367.

It is also important to note that the element of ‘course of conduct’ is also absent in these legislation. As these legislation were not enacted to deal with cyberstalking specifically, it is understandable why such unique element is absent. This further justifies the need for a separate legislation to deal with cyberstalking. Moreover, existing laws do not provide anticipated remedies, including restraining orders and injunctions. In short, the cyber-related laws are of limited help to cyberstalking cases as they are limited in scope and remedies.

B. Proposed Anti-Stalking Legislation

Due to the rising prevalence and severity of (cyber)stalking, inadequate civil laws³⁸ and insufficient criminal laws,³⁹ especially inapplicable cyber-related legislation to cover its scope, the CMAB has responded by conducting a public consultation on the proposed anti-stalking law.⁴⁰ The proposed anti-stalking legislation stipulates that ‘a person who pursued a course of conduct which amounted to harassment of another, and which he knew or ought to have known amounted to harassment of the other, should be guilty of a criminal offence’.⁴¹ Such harassment should be ‘serious enough to cause that person alarm or distress’.⁴²

The pressing need for specific criminalisation of stalking revived subsequent to the 2000 Report and the 1998 Consultation Paper.⁴³ Out of 506 responses from organisations, individuals and anonymous parties from different sectors, 46% supported criminalisation, whilst 35% opposed.⁴⁴ The remaining either did not indicate or supported subject to revisions of the proposed legislation.⁴⁵

³⁸ See *Consultation Paper* (n 7) 9.

³⁹ See *Ibid* 10.

⁴⁰ *Ibid*.

⁴¹ CMAB, *Consultation Paper on Stalking Highlights (Consultation Paper Highlights)* (HK 2011) <www.cmab.gov.hk/en/upload/stalking_leaflet_en.pdf> accessed 12 February 2013, 19. The proposed offence of harassment will attract a maximum penalty of \$100,000 and two years imprisonment. The victim may also be granted restraining orders and/or injunctions.

⁴² *Consultation Paper Highlights* (n 41).

⁴³ LRC, Privacy Sub-Committee, *Stalking Consultation Paper* (HK 1998) <www.hkreform.gov.hk/en/publications/stalk.htm> accessed 13 February 2013.

⁴⁴ LegCo on Constitutional Affairs, ‘Consultation on Stalking – Summary of Views Received’ (CB(2) 196/12-13(04), 2012) <www.legco.gov.hk/yr12-13/english/panels/ca/papers/ca1119cb2-196-4-e.pdf> accessed 13 February 2013, 3-4. Most opposition came from the media and journalists groups, who raised concerns about the freedom of press and expression. Although this is not the focus of the article, I believe that the proposed ‘reasonable pursuit’ defence is sufficient to protect such freedom. For defence of ‘reasonable pursuit’, see *Consultation Paper* (n 7) 32.

⁴⁵ LegCo on Constitutional Affairs (n 44) 3.

Although cyberstalking is not specifically or explicitly included, Eric Lee, the Secretary for the CMAB, stated that

[s]ince there are many ways by which stalkers can harass their victims, the proposal ... does not specify the types of behaviour, or the means by which a person harassed another. The proposal ... would cover any behaviour that falls under the ... definition, regardless of the means by which a person harassed another.⁴⁶

In other words, '[t]he means by which a person harassed another was not the focus of the consultation'.⁴⁷ Accordingly, a purposive interpretation would suggest that cyberstalking, as a type or means of such behaviour, is impliedly included – 'a crime is a crime, no matter how it is perpetrated'.⁴⁸ The proposed law appears to be wide enough to encompass cyberstalking, as long as it falls under the definition and fulfills the criteria. If that is true, such proposed law will certainly be more effective in tackling cyberstalking than the piecemeal legislation analysed above, due to the expanded scope, inclusion of the element 'course of conduct' as well as comprehensive and appropriate punishment and/or remedies.

Having said that, in order to determine whether the proposed legislation actually includes cyberstalking, and if not, how it should be included, a comparative analysis of the technologically-matured jurisdictions' cyberstalking laws will be carried out. Moreover, HK's approach to cyberspace legislation will also be taken into account.

III. ANTI-CYBERSTALKING LEGISLATION IN THE US, AUSTRALIA AND THE UK

As major common law jurisdictions with developed economics and technologies, which have undergone significant reform of cybercrime laws, reference to the US, Australia and the UK ought to be made when considering HK's position. It should be noted that the countries (and states within) all have their own versions of anti-(cyber)stalking legislation.

⁴⁶ Email from Eric Lee to author (18 January 2013).

⁴⁷ Email from Eric Lee to author (9 January 2013).

⁴⁸ Wong (n 37).

A. US

The US is arguably the most established and advanced with regards to its anti-stalking and anti-cyberstalking laws. California was the first to criminalise stalking and then many other states followed suit.⁴⁹ As ‘original statutes ... failed to consider situations that involved high-technology devices’, subsequent legislation was passed or amended to criminalise cyberstalking.⁵⁰ Now, all fifty states with anti-stalking laws have included a cyber element – cyberstalking and/or cyberharassment.⁵¹ Recently, the state of Arizona changed its stalking law and it now specifically includes the ‘[use of] any electronic, digital or global positioning system device to surveil a specific person or a specific person’s internet or wireless activity continuously for 12 hours or more or on two or more occasions over a period of time’ in addition to communication as a ‘course of conduct’.⁵² Unlike HK, Arizona law is specific about what types of activity comprise the course of conduct, including surveillance.

In Florida, ‘[a] person who willfully, maliciously, and repeatedly follows, harasses, or *cyberstalks* another commits the offense of stalking’⁵³ (emphasis added). Cyberstalking ‘means to engage in a course of conduct to communicate ... by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose’.⁵⁴ Unlike HK, Florida has specifically included the term ‘cyberstalk’ and defined it. Washington DC, although not a state but a federal district, has a separate legislative provision for cyberstalking; cyberstalking involves ‘electronic communication’, meaning ‘the transmission of information by wire, radio, optical cable, electromagnetic, or other similar means [including] electronic mail, internet-based communications, pager service, and electronic text messaging’.⁵⁵ Furthermore, to deal with the jurisdictional issues unique to cyberstalking, it has provided that

⁴⁹ Pittaro (n 17) 293.

⁵⁰ R Moore, *Cybercrime: Investigating High-Technology Computer Crime* (2nd edn Elsevier Inc, Oxford 2011) 134.

⁵¹ ‘State Cyberstalking and Cyberharassment Laws’ *National Conference of State Legislatures* (16 November 2012) <www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx> accessed 26 February 2013.

⁵² Arizona Criminal Code (US) s 13.2923(C)(1)(a)(2) (2012).

⁵³ Florida Statutes (US) s 784.048(2)-(3) (2012).

⁵⁴ Florida Statutes (US) s 784.048(1)(d) (2012).

⁵⁵ Revised Code of Washington (US) s 9.61.260(5) (2012).

cyberstalking is ‘deemed to have been committed either at the place from which the communication was made or ... where the communication was received’.⁵⁶

B. Australia

Like the US, all Australian states have anti-stalking legislation. However, not all states have expressly included the cyber element.⁵⁷ Queensland, Australian Capital Territory, Tasmania, South Australia and Victoria have anti-stalking laws which cover ‘internet’, some form of ‘electronic communication’ or ‘technology’.⁵⁸ Compared to HK, these states are more specific and comprehensive, which listed out examples including contacting, communicating, publishing, tracing and surveiling by such means. It is worth noting that no Australian states have used the term ‘cyberstalk’ in their legislation or introduced separate cyberstalking provisions like some US states. The next part of this article will elaborate on whether the cyber element should be expressly included, whether the term ‘cyberstalk’ should be used and whether a separate provision is required.

C. UK

In the UK, on 25 November 2012, Section 111 of the Protection of Freedoms Act came into force and introduced two offences of stalking – ‘stalking’ and ‘[s]talking involving fear of violence or serious alarm or distress’.⁵⁹ HK’s proposed legislation is generally consistent with the latter offence. However, unlike HK, Section 2A(3) of the Protection from Harassment Act (also referred to in Section 4A(1)(a)) gives a list of ‘examples of acts or omissions ... associated with stalking’, which includes ‘monitoring the use by a person of the internet, email or any other form of electronic communication’⁶⁰ as well as following, contacting another by any means, publishing any material, loitering, interfering with property and watching or spying on another. In other words, the cyber element is explicitly included in the provision. Although the term ‘cyberstalk’ is not used, the inclusion of ‘any means’ and

⁵⁶ Revised Code of Washington (US) s 9.61.260(4) (2012).

⁵⁷ Such as Crimes (Domestic and Personal Violence) Act 2007 (AUS NSW) s 13, Criminal Code 1997 (AUS NT) s 189 and Criminal Code Act 1913 (AUS WA) s 338D-E.

⁵⁸ See Criminal Code 1899 (AUS QLD) s 359B(c)(ii); Crimes Act 1900 (AUS ACT) s 35(2)(f)-(h); Criminal Code Act 1924 (AUS TAS) Sch 1 s 192(1)(g)-(i); Criminal Law Consolidation Act 1935 (AUS SA) s 19AA(1)(a)(iv); and Crimes Act 1958 (AUS VIC) s 21A(2)(b).

⁵⁹ The Protection of Freedoms Act (PFA) 2012 (UK) s 111. See Protection from Harassment Act (PHA) 1997 (UK) ss 2A and 4A respectively.

⁶⁰ PHA ss 2A(3)(d) and 4A(1)(a).

‘monitoring ... of the internet, email or any other form of electronic communication’ indicates that cyberstalking is included. However, it is arguable that ‘some, but not all, forms of cyberstalking’ is included.⁶¹ For example, the conduct of covert surveillance is not covered, which, unlike monitoring, does not involve any intervention with the victims.

IV. CYBERSTALKING IN HK

A. Addition to the Proposed Anti-Stalking Legislation

The CMAB Secretary has advised that the broad language of the proposed anti-stalking legislation can be interpreted to include cyberstalking behaviour. In order to confirm that such legislation actually has the potential to do so, the abovementioned comparative analysis as well as HK’s approach to cybercrime legislation will be taken into account.

The US, Australia and the UK are all major common law, technologically-matured jurisdictions with history and experience in dealing with (cyber)stalking. As all states in the US, most states in Australia and the UK have all expressly included the cyber element (to different extents) in their anti-stalking laws, HK, with an evolving information technology infrastructure, should also align its position to explicitly include the cyber element in its proposed anti-stalking law. Regarding HK’s proposed anti-stalking legislation, Hema Khan has opined that it ‘the language ... could be modified to specify that the course of conduct would include technology’.⁶² Hema Khan is the Program Attorney for the Stalking Resource Center at the National Center for Victims of Crime (NCVC), who has ‘conduct[ed] legal research and analysis on stalking laws’.⁶³

The proposed legislation should address the virtual medium and be broadened to include ‘electronic communications (overt stalking)’ and ‘surveillance, monitoring and tracking (covert stalking)’, in view of the unique features of cyberstalking.⁶⁴ Otherwise, it will not address cyberstalking adequately. It should be remembered that (stand-alone) cyberstalking could cause equally serious harassment. The insertion of the cyber element to the proposed

⁶¹ MacEwan (n 21) 778.

⁶² Email from Hema Khan to author (6 March 2013).

⁶³ ‘2013 Speakers’ Conference on Crimes Against Women (2013) <http://conferencecaw.org/2013_Conference_Speakers.html> accessed 22 April 2013.

⁶⁴ Chik (n 4) 17.

anti-stalking law would be consistent with HK's basic principles of cyberspace legislation, which includes applying the current laws to cyberspace, avoiding undue legislation and introducing laws only when necessary as well as maintaining a 'predictable, consistent and minimal legislative regime'.⁶⁵ Accordingly, the proposed anti-stalking law should be applied to cyberspace, without creating a separate provision for cyberstalking; this is consistent with the existing HK cyber-related legislation and most of the abovementioned jurisdictions' legislation. In view of the practices of other jurisdictions and to ensure consistency in the proposed anti-stalking legislation which uses the term 'harassment', it is not necessary, and does not seem appropriate, to use the term 'cyberstalk'. Synonyms of 'cyber', such as Internet, electronic communications and technology, may be used instead to provide a better idea of what cyber constitutes.

HK currently adopts a general prohibition model, which generally prohibits the offence of stalking,⁶⁶ as compared to a list model, which specifically states the acts constituting stalking.⁶⁷ It is agreeable that 'a crime is a crime, no matter how it is perpetuated', hence a general prohibition model would *prima facie* be appropriate to cover all means of stalking. Having said that, the unique features of non-physical and non-proximate cyberstalking would mean that some forms will not be covered under the general provision, thus demands for special attention within the legislation. Accordingly, HK should, in addition to the general prohibition model, include a 'non-exhaustive illustrative list of common stalking and cyberstalking acts'.⁶⁸ More specifically, it should include both (direct and indirect) communications and surveillance, via traditional and technological methods – such as maintaining visual or physical proximity, physically or electronically following and tracking; making verbal or written communications; pursuing threatening conduct; impersonating and instigating a third party to further harass.

The inclusion of such list would give support and guidance to the courts as well as potential offenders and victims, in determining what falls under a 'course of conduct', thus constitute (cyber)stalking. In other words, it increases predictability and certainty of the regime, whilst maintaining flexibility, due to non-exhaustive nature of the list. Without such

⁶⁵ KC Wong (n 37).

⁶⁶ D Lamplugh and P Infield, 'Harmonising Anti-Stalking Laws' (2003) 34 *George Washington International Law Review* 853, 860-3.

⁶⁷ *Ibid* 863-5.

⁶⁸ Chik (n 4) 24.

an open-ended illustrative list, '[c]ourts will adjudicate each case afresh by reference to what it understands ... harassment to mean',⁶⁹ thus would create a great deal of uncertainty. Overall, this addition to the proposed anti-stalking legislation will 'strengthen the existing regulatory regime'⁷⁰ by aligning laws with the swift technological advances. Moreover, it would 'allow for easier investigation and prosecution of cyberstalking cases' and such cases would be taken 'more seriously'.⁷¹

Besides listing the common acts, it would be helpful and more comprehensive for the proposed anti-stalking legislation to also provide a definition of 'electronic communication' (like Washington DC) as well as to address 'the new challenges offered by cyberstalking'.⁷² For example, in order to remain anonymous, a person is likely to create false identities, thus would not technically be 'a person'.⁷³ In other words, 'a person' should be clarified to include false identities, which are in fact created by the same person. Like Tasmania, HK should stipulate its jurisdictional powers over cross-border (cyber)stalking cases. Furthermore, like the UK, additional powers should be given to the police to enter and search the premises, seize and retain as well as use reasonable force.⁷⁴ These powers will 'aid in investigation and evidential gathering in ... cyberstalking' and 'potentially strengthen the prosecution case'.⁷⁵

B. Effective Enforcement

A multi-faceted approach should be adopted for such a multi-faceted crime – aside from the implementation of law, enforcement agencies, the private sector and individual citizens themselves should work together to effectively control cyberstalking and tackle its unique challenges. They should also work hand-in-hand to raise awareness. Although not the focus of this article, it is noteworthy to point out that it is likely (cyber)stalkers will benefit from psychiatric or mental evaluation and treatment, since '[cyber]stalking often stems from a form of mental or social abnormality [with] unhealthy and uncontrollable obsession'.⁷⁶ In

⁶⁹ Lamplugh and Infield (n 66) 866-7.

⁷⁰ Jackson (n 20) 246.

⁷¹ Moore (n 50) 139; especially where many perceive stalking to be relatively harmless, see Pittaro (n 17) 280, 283.

⁷² Chik (n 4) 21.

⁷³ Ibid 22.

⁷⁴ PFA s 112 PFA; PHA s 2B.

⁷⁵ 'Stalking and Harassment' *The Crown Prosecution Service* <www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/#a03pi> accessed 22 April 2013.

⁷⁶ Chik (n 4) 42 fn 132.

absence of treatment, ‘the risk of recurrence of ... stalking behaviour [is] high’.⁷⁷ Whether such assessment and treatment should be essential is subject to further discussion.⁷⁸

1. Enforcement Agencies

The most notable enforcement agencies include the HK Police (HKP) and the Department of Justice’s Prosecutions Division. Currently, the HKP Commercial Crime Bureau’s Technology Crime Division (TCD) prevents and detects technology crime by ‘carrying out technology related investigations, collection of digital evidence [locally and overseas], forensic examinations of computer systems, and liaison with local and international agencies for timely and efficient intelligence and experience exchange’.⁷⁹ Moreover, the Technology and Crime Prevention Unit (branch of TCD) (TCPU) aims to raise awareness of cybercrime prevention amongst the public, through publishing materials, making talks and presentations, as well as formulating and implementing ‘crime prevention programs on computer security and technology crime related matters’.⁸⁰

More recently, the Cyber Security Centre was launched to tackle cyberattacks by monitoring the network data traffic.⁸¹ These agencies are certainly a cornerstone to regulating cyberspace. However, attention should be paid to cyberstalking as much as commercial crimes. Whilst technology is used to stalk, enforcement agencies should also take advantage of technology to develop better investigative and identification methods, such as ‘decrypted text or tools’.⁸² Moreover, agents should receive ‘advanced training on computer-based communications, updated computer forensic software, and drafting ... search warrants’ to prepare them for cyberstalking cases, especially when anonymous cyberstalkers are

⁷⁷ *Tsui Chu Tin John (No 2)* (n 6) 482.

⁷⁸ For HK’s position on this, see *Consultation Paper* (n 7) 56-7.

⁷⁹ ‘Technology Crime Division (TCD)’ *HK Police Force* (February 2013) <www.police.gov.hk/ppp_en/04_crime_matters/tcd/tcd.html> accessed 11 February 2013; ‘First INTERPOL Information Security Conference to Provide Global Platform for Preventing and Detecting High-tech Crimes’ *INTERPOL* (15 September 2010) <www.interpol.int/News-and-media/News-media-releases/2010/PR070> accessed 24 February 2013.

⁸⁰ ‘Technology Crime Division (TCD)’ (n 79), includes professional advice, ‘Clean PC Day’, ‘Fight IT Crime Ambassador Workshop’ and assisted by the Education Bureau.

⁸¹ Ellyne Phneah, ‘Hong Kong Launches Center to Curb Cybercrime’ *ZDNet* (10 December 2012) <www.zdnet.com/hong-kong-launches-center-to-curb-cybercrime-7000008526/> accessed 24 February 2013.

⁸² Jackson (n 20).

involved.⁸³ It is crucial for the enforcement agencies to collaborate with the private groups and industry regulators, discussed below.

2. Private Sector

Individual organisations and industry regulators should help tackle cyberstalking in HK. Individual interest groups, such as Working to Halt Online Abuse,⁸⁴ CyberAngels,⁸⁵ NCVC⁸⁶ and Network for Surviving Stalking,⁸⁷ generally aid the victims by providing advice and resources (such as the Use of Technology to Stalk online course),⁸⁸ whilst industry regulators, including Internet Service Providers (ISPs) and Network Solutions WHOIS,⁸⁹ work with the enforcement agencies to proactively prevent cyberstalking (by limiting or prohibiting access) as well as investigate, identify and gather evidence.⁹⁰ It should be noted 'ISPs must be protected from general liability for the acts of its users' in order 'for the Internet to continue as a medium for increased freedom of speech and expression, the exchange of ideas and limited censorship'.⁹¹ Having said that, the general position is that ISPs should provide assistance to identification and evidence collection where necessary, which would in turn benefit them, as users will continue to use their 'regulated' service.

3. Individual Citizens

Individuals, including both potential and actual victims, should be equipped with necessary knowledge to prevent and combat cyberstalking. Such knowledge on the nature of cyberstalking, self-protection and (legal) recourse may be gained from resources produced by the enforcement agencies and private groups. Although obvious, it is worth reminding that any identifying information (name, address, phone), passwords and credit card numbers should never be given to strangers or shared publicly. A routine check should be done regularly to ensure that personal details do not appear in the search engines, and if so, request

⁸³ Moore (n 50) 139.

⁸⁴ *Working to Halt Online Abuse* (2012) <www.haltabuse.org/> accessed 26 February 2013.

⁸⁵ *CyberAngels* <www.cyberangels.org/> accessed 26 February 2013.

⁸⁶ *NVCV* (2012) <www.victimsofcrime.org/> accessed 26 February 2013.

⁸⁷ *Network for Surviving Stalking* (2013) <www.nss.org.uk/> accessed 26 February 2013.

⁸⁸ 'The Use of Technology to Stalk' *Stalking Resource Center* (2012) <www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-information/the-use-of-technology-to-stalk> accessed 26 February 2013.

⁸⁹ *Network Solutions* (2013) <www.networksolutions.com/whois/index.jsp> accessed 26 February 2013.

⁹⁰ Jackson (n 20).

⁹¹ Chik (n 4) 24, the extent of assistance is beyond the scope of this article.

it to be removed. In order to aid prosecution, cybervictims should save a log of the harassing communications and/or postings.⁹²

4. Local and International Collaborative Effort

The criminalisation of cyberstalking will be a step forward, but it should not be the only step taken. Instead, there should be a concerted effort between the government, enforcement agencies, private organisations, industry regulators as well as individuals themselves, to effectively and efficiently, prevent, investigate, detect and prosecute cyberstalkers. There should be a ‘joint effort from various governing regimes and assistance from different legal jurisdictions ... international institutions and overseas regulators’⁹³ to address the unique challenges presented by cyberstalking, such as anonymity and jurisdictional issues.

Ideally, given the transborder nature of cybercrime and cyberstalking, common practices and standards should be adopted across (and within) jurisdictions. The Council of Europe Convention on Cybercrime (CCC) is illustrative of international cooperation and regulation, which also obligates signatories to criminalise certain cybercrimes, thus in turn harmonise different jurisdictions’ substantive laws.⁹⁴ The US, Australia and the UK are all parties to CCC.⁹⁵ Taking into account the progress made in cybercrime legislation, HK should also be a party⁹⁶ and then propose the inclusion of cyberstalking in the CCC.

V. CONCLUSION

Technology provides numerous benefits, but it should be regulated in order to prevent abuse. Cyberstalking, a form of cybercrime, is similar in effect to the traditional form of stalking, yet it has its own unique features. It is unfortunate that HK’s piecemeal computer crimes legislation do not deal with cyberstalking effectively. Auspiciously, the proposed anti-stalking legislation impliedly covers cyberstalking. However, after examining the unique features of cyberstalking, the US, Australian and the UK cyberstalking legislation as well as

⁹² S Plellusch and M Ryan, ‘Stalking: Know It, Name It, Stop It’ *Pentagram* (25 January 2013) <www.dcmilitary.com/article/20130125/NEWS10/130129863/stalking-know-it-name-it-stop-it> accessed 22 April 2013.

⁹³ Wong (n 37) 382.

⁹⁴ Council of Europe, Convention on Cybercrime, CETS no 185 (entered into force on 1 July 2004).

⁹⁵ Entered into force on 1 January 2007, 1 March 2013 and 1 September 2011 respectively.

⁹⁶ See JG Bullwinkel, ‘International Cooperation in Combating Cyber-Crime in Asia: Existing Mechanisms and New Approaches’ in Broadhurst and Grabosky (n 2) 301.

HK's basic principles of cyberspace legislation, it is strongly recommended that the proposed anti-stalking legislation should expressly include the cyber element through a non-exhaustive illustrative list of prohibited conducts. Moreover, the legislation should address the unique challenges posed by cyberstalking and provide additional powers to enforcement agencies. Not only will the inclusion of the cyber element, address of the unique challenges together with provision of additional powers will ensure that cyberstalking is covered, it will also ease investigation and prosecution as well as raise awareness on this issue. In short, cyberstalking will be tackled more effectively. This will also align HK's cyberstalking law with those of other major, technologically-matured jurisdictions.

The collective effort between the public and private sector, locally and globally, will challenge the challenges posed by anonymity of cyberstalkers and jurisdictional issues. As HK is in the forefront of technology, I anticipate this article to reflect the future position of cyberstalking in HK. Law and society should evolve with technology. With appropriate legislation, prevention and enforcement mechanisms, as well as local and international cooperation, the cyberstalkers will be stalked in HK.