Copyright © 2013 International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891
January – June 2013, Vol 7 (1): 18–27

Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's four Modalities of Constraint[1]

Hee Jhee Jiow[2]
National University of Singapore, Singapore

Abstract

Singapore is ranked as one of the most wired nations in the world; it is internationally ranked fourth highest in cyber crime rate and this is expected to increase. The establishment of INTERPOL's Global Complex in Singapore signals the nation's interest and readiness in playing a greater role in regulating Internet usage. As such, there is great significance in exploring Singapore's glocalized approach towards regulation of Internet behaviors. Adopting Lessig's four modalities of constraint, this paper will examine Singapore's approaches and efforts in its regulation of cyber crime, and will conclude by highlighting Singapore's challenges in regulating users' behaviors in cyberspace.

Keywords: Cyber crime, Regulation, Law, Social Norms, Technology, Cyberwellness Education.

Introduction

The usage of the Internet has proliferated and affected the lives of many people (Keyser, 2003), especially so in Singapore, which boasts a high Internet penetration rate, with 160.2% of its population having broadband access (Infocomm Development Authority of Singapore [IDA], 2012). With a mobile penetration rate of 151.4% (IDA, 2012), and access to wireless, location based, cloud computing and always-on technologies, the usage of Internet-connected devices is becoming pervasive in daily life (Symantec Corporation, 2011). As such, the Internet has evolved into a space – usually termed 'cyberspace' – that Singaporeans 'live' in (Lessig, 2006). Moreover, the government has, since 2006, been actively promoting the usage of the Internet via its Intelligent Nation 2015 Masterplan (IDA, n.d.-a).

However, with increased Internet usage and penetration, a corresponding increase in the incidence of cyber crimes has been observed (Symantec Corporation, 2011). The Internet is increasingly becoming the domain and conduit of harmful activities and

[1] A short version (non-peer-reviewed) of this paper has been presented at the International Conference on e-Democracy and Open Government-Asia 2012 (CeDEM-Asia-2012) held during 14-15, November 2012, at Singapore.

[2] PhD Candidate, Department of Communications and New Media, Faculty of Arts and Social Sciences, National University of Singapore, AS6 Level 3, 11 Computing Drive, Singapore 117416. E-mail: jhee@nus.edu.sg

criminal behaviors (Grabosky, Smith, & Dempsey, 2001; Jewkes, 2003). As such, governments have been enacting international laws, using technological means, market forces, and education to regulate Internet usage, albeit not always successfully (Jewkes, 2003; Lessig, 1999). Singapore is not spared either; it has one of the highest cyber crime rates in the world, which is expected to increase significantly (Ministry of Home Affairs, 2010). Latest figures show that 80% of Internet users in Singapore have experienced cyber crime, the fourth highest rate in the world (Symantec Corporation, 2011). In addition, with INTERPOL stepping up its efforts in regulating the global Internet, by establishing its Global Complex in Singapore (Ministry of Home Affairs, 2010), it would be pertinent to explore Singapore's commitment and contribution to the regulation of the global Internet locally – via the glocalized approach.

This paper will adopt Lessig's four modalities of constraint to discuss Singapore's approach to Internet regulation and conclude by discussing Singapore's Internet regulatory approaches, in terms of preventing its citizens from being either victims or perpetrators of cyber crimes. It will also consider future challenges.

Singapore's Cyber Crime Scene

Hacking cases in Singapore mirror those commonly found around the world. Defacement of websites, hacking into schools' computer files to view other students' grades and riding on neighbors' wireless networks are examples found locally (Jin-Cheon et al., 2009). However, in a rare case of global perpetration by a Singaporean, a 17-year-old student was convicted of hacking into foreign servers; he claimed it was done out of curiosity (Urbas, 2008). More recent incidents of hacking, virus or Trojan attacks in Singapore have been products or results of scamming. Viruses and Trojans have been used to deceive victims into revealing personal information to access banking transactions (Weizhen, 2009). This information was then marketed and published on hackers' forums. In another incident, the perpetrator hacked into a Singaporean's email account to scam the victim's friends into transferring money to him (Luo, 2009). There was also another recent case in which a virus infiltrated the victim's computer system via the social networking site, Facebook (Luo, 2009). The intent was to gain information from the user's friends, which would eventually translate to financial gains for the perpetrator. Fraud cases online are also common in Singapore (Jin-Cheon et al., 2009). A couple was charged with extorting money from a 22-year-old man, by threatening to upload the victim's nude video online (Ho, 2012). A recent survey on Internet fraud identified human behavior as the key weakness in Singapore's Internet security framework; that is, victims lack understanding on how these frauds are conducted (KPMG, 2011).

Internet harassment activities or threats to Singapore's social fabric have been rampant lately. In a multi-racial and religious society such as Singapore, racist or anti-religion remarks are taken seriously. A 27-year-old man was arrested for inciting violence through his Facebook posting (Chen, 2010). Besides him, there have been many others taken to tasks by the police and the Internal Security Department of Singapore for making racist or anti-religion remarks, though they were not formally arrested (Hou, 2010c). As such, many netizens have taken to shaming as a means to discourage negative or racist comments from flourishing in cyber space (Wong, 2012). However, some vigilantes have taken this approach to extremes. A young person was wrongly identified as the one who caused noise disturbance in his neighborhood, resulting in his personal details being published online. Another victim's personal details, such as his residential and work addresses, email address and mobile phone number, were published online by some netizens who did not agree with his views about government policies, which he had aired online. These cases can be considered as cyber bullying, in the vein of those occurring in schools (Osada, 2011). In some cases, the harassment was sexual in nature (Ho, 2012). It is no surprise that Singapore is only second to the United States in the number of cyber bullying cases per capita (Gwee, 2008).

With more than half of all installed computer programs being pirated copies, Singapore's intellectual property (IP) figures are lower than for its Asia-Pacific counterparts, but on par with the global average (Tham, 2012). The fear of getting caught is commonly touted as a deterrent for most users, and a powerful one, as Singapore continues to see a decline in its software piracy rate.

Lessig's Four Modalities of Constraint

Lessig (2006) claims that Internet behaviors in general can be regulated by four constraints: "the law, social norms, the market, and architecture" (p. 123). The law stipulates which behaviors can be carried out to avoid legal punishment. Societal norms "constrain through the stigma that community imposes" (Lessig, 2006, p. 124). Typically, a high financial cost would constrain users' behavior; these costs are termed market forces. The affordability of technology, termed as the architecture, also limits users' actions in cyberspace. This is also sometimes referred to as the design of technology or the infrastructure. "Each constraint imposes a different kind of cost on the [user] for engaging in [a] behavior" (Lessig, 2006, p. 123). The constraints are interdependent, supporting or opposing one another, yet they are distinct. Arguably, these constraints can be perceived as tools that the government uses in order to manipulate cyberspace behaviors. However, each constraint has its own challenges. The following section discusses the challenges associated with each of the constraints and comments on Singapore's regulatory approaches to Internet behaviors using this framework. It will examine the measures implemented to protect its citizens from being victimized, as well as prevent them from being perpetrators.

a. The Law

Globally, the law faces huge challenges in regulating the Internet. Firstly, only 10% of cyber crimes are reported, and less than 2% of reported cases resulted in successful prosecution (Jewkes, 2003; Symantec Corporation, 2011). Secondly, due to the difficulties of cross-border enforcement, it is easy for perpetrators to find shelter outside the reach of national or international Internet laws. This is further complicated by different moral values and laws, and varied enforcement responses in different countries (Broadhurst & Chang, 2012). It is crucial that enforcement responses are timely as the evidence of cyber crime, which is essential for successful prosecution, is volatile in nature (Phair, 2007). As such, the law is limited in its effectiveness, and at times seen as the worst constraint (Grabosky et al., 2001).

Yet Singapore actively supports global efforts in eradicating cyber crime by participating in schemes, such as the Wassenaar Arrangement that promotes the fight against terrorism (Singapore Customs, n.d.), and being a member of organizations such as the World Intellectual Property Organization (WIPO, n.d.) that promotes intellectual property rights. Singapore has also favorably aligned itself to the legal requirements of the Budapest Convention, though not a signatory (Broadhurst & Chang, 2012). Notably, Singapore has passed legislation to give wide-reaching territorial jurisdiction – it is moot whether the offence occurs in Singapore, the perpetrator resides in Singapore when the offence is committed, or facilitation of the offence is done by a computer in Singapore (Brenner & Koops, 2004). Meant as a deterrent, it seeks to prevent global perpetration of cyber crimes from Singapore, though it has rarely been invoked (Leong & Wai, 2005; Urbas, 2008). Being the gateway between the eastern and western Internet cultures, and an economic hub for the Asia-Pacific region, it also signals to the global community, the Singapore's resolve in combating cyber crime. This gesture may encourage other nations, especially the developing ones, to align with international legal and enforcement efforts. Thus, it potentially extends the reach of international Internet laws, and helps to prevent victimization of Internet users locally and globally.

Furthermore, in its efforts to minimize local perpetration of cyber crimes, Singapore has been enacting and amending several laws to keep pace with changing times (Urbas, 2008). The Electronic Transactions Act (ETA) serves to provide the "legal environment" (Leong & Wai, 2005, p. 128) necessary for commercial transactions and e-government services. The ETA also limits the liability of network service providers for accessed content. The ETA 2010 (Electronic Transactions Act, 2010) was revised to be more consistent with the United Nations Convention's interest in promoting better security in online transactions. The Evidence Act legitimizes electronic records as evidence to be used in courts. It also provides for the use of Internet systems, such as tele-conferencing, during court hearings (Leong & Wai, 2005). The Spam Control Act was enacted in 2007 to require marketers to differentiate an advertisement from other messages, making it easier for receivers of these messages to manage them (IDA, 2007). The Computer Misuse Act (CMA), enacted in 1993, serves to protect computers, information and computer programs from "unauthorized access, modification, use or interception" (Leong & Wai, 2005, p. 129). Its jurisdiction extends beyond Singapore, and it classifies preparatory actions as an offence (Urbas, 2008). The CMA was kept up to date with revisions to accommodate for newer forms of cyber crime, such as password trafficking and threats to national security (Leong & Wai, 2005; Urbas, 2008).

Though CMA is broad enough to cover old crimes such as fraud, IP infringements and harassment, which use the computer as a conduit, Singapore has been known to use other legislations for prosecution (Leong & Wai, 2005; Urbas, 2008). The CMA and Penal Code have been used to deal with fraud cases (Urbas, 2008). Harassment, as in the form of cyber stalking or cyber bullying, rarely resulted in prosecution, but when it did, it is normally dealt with under CMA and other physical acts. The Copyright Act and Trade Marks Act are used together with CMA to deal with IP infringements. Treating the Internet as a broadcast media tool, Singapore uses statutes such as the Undesirable Publications Act to deal with the dissemination or storage of content such as child pornography or racial vilification (Ang & Nadarajan, 1996; Urbas, 2008). In addition, the Penal Code was amended to accommodate the use of computers in the commission of crimes, such as sexual grooming (Urbas, 2008). It was also used to handle libel and defamation suits (Putnam & Elliott, 2001).

Singapore has been consistently updating its laws in response to the cyber crimes experienced and perpetrated locally. It has been aligning its laws with the global community, and also extending its territorial jurisdiction to help tackle cyber crimes both locally and globally. It has been touted as one of the countries with the "toughest and most detailed cyber crime laws" (Putnam & Elliott, 2001, p. 51). Local perpetrators have been punished "appropriately" (Urbas, 2008, p. 21). Given the limitations of jurisdiction and enforcement of the law, Singapore has postured the law well as a tool in the regulation of Internet behaviors.

b. The Architecture

The architecture of cyber space, though affording a technical solution to the prevention, monitoring and enforcement of cyber crime, is frequently circumvented. System-based methods for payment of creative materials, which was intended as the solution to piracy, were quickly circumvented by the emergence of peer-to-peer file sharing services (Jewkes, 2003). With "the scope and pervasiveness of digital technologies [opening] up new areas of social vulnerability" (Jewkes, 2003, p. 24), architecture affords easier invasion of privacy. Another example is spam mail, typically considered to be a form of harassment, and an increasingly burden for the Internet Service Providers (ISPs). Though there are surveillance and enforcement procedures for ISPs to adhere to, the majority do not have that capability (Phair, 2007). The affordability of and access to technology have also been harshly criticized for fueling the boom of the child pornography industry, by providing anonymity and allowing "for the size of collections to grow [creating] a constant demand for new and novel materials" (Taylor & Quayle, 2003, p. 7). Malware "has [also] evolved to adapt to countermeasures such as software programs designed to prevent and detect intrusions" (Broadhurst & Chang, 2012, p. 6). While Lessig claims that technology is the "predominant regulatory institution for cyber space" (Grabosky et al., 2001, p. 7), some have argued, that the cyberspace's architecture created the potential for more criminal activities to take place, by affording anonymity to the perpetrator and by the reach and impact of such activities (Jewkes, 2003). The prevalence of hacking and virus attacks globally highlights this inherent neutrality afforded by the design of technology.

The IDA is the governmental organization responsible for Singapore's infocomm development and security. To this end, IDA actively consults and collaborates with the private and public sector, and has invested more than S$70 million in the Infocomm Security Masterplan (MP2) (IDA, 2008). The MP2 seeks to improve technologies in its fight against cyber threats. The Singapore Computer Emergency Response Team (SingCERT) continually delivers patches to update computer systems with the latest security features or plug technological loopholes (IDA, n.d.-b). Investigative technologies are housed in SingCERT and the Technology Crime Division of Criminal Investigation Department, which arguably sends the message that cyber crimes will not go unnoticed (IDA, n.d.-b; Leong & Wai, 2005). In its efforts to enhance security for individual consumers, IDA has mandated a 2-Factor-Authentication process for banking transactions (IDA, n.d.-b; Leong & Wai, 2005).

These technological advancements are meant only to deter computer-attacking behaviors such as malware, viruses and hacking, and does little to minimize social engineering based or harassment-type behaviors, such as scams and cyber bullying (IDA, 2010). But the low incidence of pure cracking activities (not through obtaining of personal information, such as passwords, by trickery) in Singapore, arguably suggests that the nation's preventive measures are bearing fruit. Additionally, acknowledging the limitations of architecture's influence on cyberspace behaviors, the Singapore government has adopted a pragmatic approach. Symbolically blocking one hundred pornographic or offensive websites (Ang, 2007), signifying its cultural and legal stand against possession of such material, is a demonstration of such pragmatism (Ang & Nadarajan, 1996).

c. The Markets

With almost everything practically free in cyberspace, the impact of market forces is arguably limited. This is particularly evident in the IP sphere. Online copies of movies and music are significantly lower in cost compared to their physical counterparts, and as compared to prices in the past (Kirwan & Power, 2012). Yet statistics show that close to one billion people commit piracy every year, with the creative industry (which produces music, movies and software) losing billions of dollars as a result (Symantec Corporation, 2011; Yar, 2006). These perpetrators do not want things cheap; they want it free, and they can get it in cyberspace (Goh, 2012; Hou, 2010a; Kirwan & Power, 2012). Though there were attempts to enable users to download popular songs for free, the adoption rate was dismal as the songs were only allowed to be streamed to a computer with Microsoft software (Hou, 2010b). Transfers to portable music devices were prohibited. Efforts have been made by the IP industry to stem the tide of online piracy by introducing Digital Rights Management (DRM). DRM allows users to download purchased songs or videos into many devices, in effect lowering the cost of the purchased item. Of course, this compromise was also made available by technology. However, this advantage does little to stop cyberspace users from infringing copyright laws.

Therefore, financial barriers or incentives, if any, do not serve well as a constraint in minimizing deviant behaviors in cyberspace. Yet Singapore has seen some success. The Business Software Alliance in Singapore incentivizes whistle blowers with a reward of S$20,000 to expose piracy activities, which has resulted in falling software piracy rates over the years (Tham, 2012).

d. Social Norms

A social norm "governs socially salient behavior, deviation from which makes [one] socially abnormal" (Lessig, 2006, p. 340). The 'freedom of speech' philosophy in cyberspace has resulted in a rampant, callous attitude in handling content. IP infringements and harassment-type behaviors are clear examples of creative content and personal particulars, respectively, being abused as a result of this social norm. Social norms in cyberspace have recently surfaced as a very powerful force in regulating behaviors. The recent Stop Online Piracy Act episode where online activists and other influential parties, such as Google and Wikipedia, successfully rallied against the passing of a stringent anti-piracy law arguably demonstrates the power of social norms over the law (Fight for the Future, n.d.).

In Singapore, cases of online shaming have been shown to effectively modify the behavior of Internet users. This indicates the power of social norms as a mode of constraint (Hou, 2010c; Jin-Cheon et al., 2009; Wong, 2012). But some have taken it too far, prompting the government to develop an online code of conduct (Chew, 2012). Aside from being a powerful constraint, global and local trends in cyber crime suggest that it is the most relevant mode of regulating cyberspace behavior. Firstly, with high involvement rate of youths in cyber crime perpetration (Kirwan & Power, 2012; Yar, 2006), the effects of the architecture, when applied to technologically cognizant youths, are limited. In addition, most youths lack the financial means to mount a legal defense or pay fines, making it impractical to prosecute them (Phair, 2007). Even enforcement agencies acknowledge that "the community of so-called 'Netizens' – must bear the primary responsibility for cleaning up cyberspace" (Jewkes, 2003, p. 19).

Secondly, exhibiting Differential Association Syndrome (Parker, 1998; Power, 2000), perpetrators align the rationale for their actions with other social behaviors. As "education is, in part at least, a process through which we indoctrinate [users] into certain norms of behavior" (Lessig, 2006, p. 129), emphasis on building in youths a sense of what is right and wrong – values education – may eventually lead to less harmful behavior on their part. Education would help align perpetrators' misguided rationalizations. Thirdly, many victims fall prey to social engineering techniques used by perpetrators, especially in frauds and scams. This observation acknowledges the adequacy of the design of technology to prevent online theft, and also highlights the need to educate potential victims and raise awareness of the persuasive techniques adopted by scammers. Notwithstanding the positive effects of the law, architecture and market forces on regulating harmful behaviors in cyberspace, educating users, especially youths, is the most appropriate strategy.

There have been extensive and ongoing efforts in educating youths on the dangers of cyber space and avoiding victimization (Livingstone & Haddon, 2009; Media Development Authority [MDA], 2007, 2010; Microsoft, 2012; National Crime Prevention Council, 2012; Symantec Corporation, 2009). Yet nearly half of young people feel that they are not getting enough education on Internet safety (Symantec Corporation, 2011). However, efforts in preventing the perpetration of cyber crime through education are lacking.

In this regard, Singapore has done well, with the introduction of cyberwellness education. As loosely defined, 'cyberwellness' refers to a state of being healthy in cyberspace and being free from harm, whether as a victim or as a perpetrator. As such, cyberwellness education would holistically include awareness and values education for cyberspace life.

The MDA of Singapore, Singapore's Internet regulatory body, lists four core values necessary for cyberwellness – "Balanced Lifestyle, Embracing the Net and Inspiring Others, Astuteness, Respect & Responsibility" (MDA, 2007, p. 1). These values are part of the nation's educational curriculum. A balanced lifestyle between the real and cyber worlds is encouraged to prevent behaviors such being addicted to video gaming. Users are also cautioned on the harms found in cyber space, and taught to be astute and savvy to such threats. These values also promote respect for others and to use the power of the Internet responsibly and also to identify and deal with the possible harmful intentions of other users. This would be an appropriate message for perpetrators of harmful online behavior. Beyond that, it encourages the active use of the Internet to benefit and inspire others. So it can be seen that Singapore has ventured beyond Internet safety education into cyberwellness education. The focus now is not just on protection from cyberspace harms, but also on encouraging the positive, respectful and responsible use of the Internet.

Conclusion

In conclusion, limited attempts have been made to review Singapore's regulation of Internet behaviors using the four modalities of constraint. Without actual (versus reported) data on the cyber crime prevalence rate, which is challenging to come by (Jewkes, 2003; Symantec Corporation, 2011), the effectiveness of each constraint is hard to assess well. Future studies would do well with such data available. Despite this, this paper has attempted to present just such an assessment.

Surveying the prevalence and characteristics of cyber crime, both globally and locally, this paper has observed an increase in youths as perpetrators, and the need for holistic education as a primary means to regulate their Internet behavior, contrary to Lessig's claim that the architecture is the predominant regulator. Singapore, as befitting its status as a metropolitan city, has to adopt a glocalized approach in regulating its people's behavior in and usage of cyber space. To this end, Singapore has adopted a 'light touch' philosophy towards cyber space, by placing an emphasis on education. But it takes a tougher stance on the financial integrity of cyber space through its laws and technological infrastructure. Indeed, it has a well-balanced approach in its use of the law, the design of technology, market forces and education in regulating cyber crimes.

While Singapore develops a code of conduct for social media use (Chew, 2012; Lim, 2012; Wong, 2012), it has to consider the challenges that each modality presents. This exercise should be pursued holistically, with education as its primary means of regulating social media behaviors.

References

Ang, P. H. (2007). Framework for Regulating the Internet. In I. Banerjee (Ed.), *The Internet and Governance in Asia: A Critical Reader* (pp. 327-339). Singapore: Asian Media Information and Communication Centre (AMIC).

Ang, P. H., & Nadarajan, B. (1996). Censorship and the Internet: a Singapore perspective. *Communications of the ACM, 39*(6), 72-78.

Electronic Transactions Act, Singapore Statues Online (2010, 19 May).

Brenner, S. W., & Koops, B. J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Tech Law, 4*(1).

Broadhurst, R., & Chang, Y. C. (2012). Cybercrime in Asia: Trends and Challenges. In J. Liu, B. Hebenton & S. Jou (Eds.), *Handbook of Asian Criminology* (pp. 49-63). Springer.

Chen, T. (2010, 26 Aug). Arrested for 'inciting violence' on Facebook, *The Straits Times*.

Chew, M. (2012, 6 Apr). Rules in real life must apply online: Yaacob, *The Straits Times*.

Fight for the Future. (n.d.). SOPA Timeline. Retrieved 21 May, 2012, from http://sopastrike.com/timeline

Goh, C. (2012, 4 Mar). Keeping Web free at a price, *The Straits Times*.

Grabosky, P., Smith, R. G., & Dempsey, G. (2001). Theft and Cyberspace *Electronic Theft: Unlawful Acquisition in Cyberspace* (pp. 1-14). Cambridge: University Press.

Gwee, S. (2008, 11 Mar). Caught in Web of Menace. *The Straits Times*.

Ho, A. (2012, 8 Mar). Striking right note to curb cyber harassment. *The Straits Times*.

Hou, C. H. (2010a, 28 Sep). Computer left downloading the whole day. *The Straits Times*.

Hou, C. H. (2010b, 2 Jul). Download songs for free - and legally. *The Straits Times*.

Hou, C. H. (2010c, 13 Feb). Racist Facebook postings: Three youths won't be charged, *The Straits Times*.

IDA. (2007). Singapore Law to Control Spam. Retrieved 27 Apr, 2012, from http://www.ida.gov.sg/News and Events/20060919202026.aspx?getPagetype=20

IDA. (2008). New S$70m Masterplan To Boost Singapore's Infocomm Security Competency And Resilience. Retrieved 16 May, 2012, from http://www.ida.gov.sg/News and Events/20080417090044.aspx?getPagetype=20

IDA. (2010). Securing Our Cyberspace, A Shared Responsibility. Retrieved 16 May, 2012, from http://www.ida.gov.sg/News and Events/20060530102030.aspx?getPagetype=21

IDA. (2012). Statistics on Telecom Services for 2012 (Jan - Jun). Retrieved 10 Oct, 2012, from http://www.ida.gov.sg/Publications/20110209152802.aspx

IDA. (n.d.-a). iN2015 Masterplan. Retrieved 23 Apr, 2012, from http://www.ida.gov.sg/About us/20070903145526.aspx

IDA. (n.d.-b). Infocomm Security. Retrieved 16 May, 2012, from http://www.ida.gov.sg/Infrastructure/20060816193152.aspx

Jewkes, Y. (2003). Policing the Net: crime, regulation and surveillance in cyberspace. In Y. Jewkes (Ed.), *Dot.cons: Crime, Deviance and Identity on the Internet* (pp. 15-35). Cullompton: Willan Publishing.

Jin-Cheon, N., Hao, W., Yong, J., Hao, T. M., & Kandan, R. M. (2009). Analysis of Computer Crime in Singapore using Local English Newspapers. *Singapore Journal of Library & Information Management, 38*, 77-102.

Keyser, M. (2003). The Council of Europe Convention on Cybercrime. *Journal of Transnational Law & Policy, 12*, 287-326.

Kirwan, G., & Power, A. (2012). *The Psychology of Cyber Crime: Concepts and Principles*. Hershey, PA: Information Science Reference.

KPMG. (2011). KPMG Singapore Fraud Survey Report 2011. In KPMG (Ed.). Singapore.

Leong, C., & Wai, C. K. (2005). Cyber-Security: Country Report on Singapore, 2003. In R. Broadhurst & P. Grabosky (Eds.), *Cyber-crime: the challenge in Asia* (pp. 125-140). Hong Kong: Hong Kong University Press.

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review, 113*(2), 501-549.

Lessig, L. (2006). *Code 2.0* (2nd ed.). New York: BasicBooks.

Lim, L. (2012, 11 Oct). Amy Cheong 'could face charges' for online rant. *The Straits Times*.

Livingstone, S., & Haddon, L. (2009). EU Kids Online: Final report *LSE, London: EU Kids Online*. (EC Safer Internet Plus Programme Deliverable D6.5).

Luo, S. (2009, 27 Feb). 'Errors' on Facebook a cyber trap. *The Straits Times*.

MDA. (2007). *MDA accepts NIAC's recommendations (Annex A)*. Singapore. Retrieved 21 May, 2012, from http://www.mda.gov.sg/Documents/mobj.1026.annex-a.pdf.

MDA. (2010). Cyber Wellness. Retrieved 4 Oct, 2010, from http://www.mda.gov.sg/Public/Pages/CyberWellness.aspx

Microsoft. (2012). Age-based guidelines for kids' Internet use. Retrieved 19 Apr, 2012, from http://www.microsoft.com/security/family-safety/childsafety-age.aspx

Ministry of Home Affairs. (2010). Singapore to house INTERPOL Global Complex. Retrieved 23 Apr, 2012, from http://www.mha.gov.sg/news_details.aspx?nid=MTg4OA%3D%3D-Hz78RPSPoMo%3D

National Crime Prevention Council. (2012). Internet Safety: Information and resources for staying safe online. Retrieved 19 Apr, 2012, from http://www.ncpc.org/topics/internet-safety

Osada, J. (2011, 31 Jul). More security is great. *The Straits Times*.

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley & Sons.

Phair, N. (2007). *Cybercrime: The reality of the threat*. Canberra, Australia: E-Security.

Power, R. (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*. Indianapolis: Que Corporation.

Putnam, T., & Elliott, D. (2001). International Responses to Cyber Crime. In A. Sofaer & S. Goodman (Eds.), *Transnational Dimension of Cyber Crime and Terrorism* (pp. 35-66). Stanford, California: Hoover Institution Press.

Singapore Customs. (n.d.). Partnership in global security. *inSync - a Singapore Customs e-newsletter.* Retrieved 29 May, 2012, from http://www.customs.gov.sg/insync/issue03/updates/security.html

Symantec Corporation. (2009). Life and Love Online – A New Report. Retrieved 19 Apr, 2012, from http://us.norton.com/familyresources/resources.jsp?title=ar_life_and_love_online_a_new_report

Symantec Corporation. (2011). Norton Cybercrime Report 2011. Retrieved 18 Apr, 2012, from http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport

Taylor, M., & Quayle, E. (2003). *Child Pornography: An Internet Crime*. New York: Brunner-Routledge.

Tham, I. (2012, 16 May). One in two uses pirated software here: Survey. *The Straits Times*.

Urbas, G. (2008). An Overview of Cybercrime Legislation and Cases in Singapore (Vol. Working Paper Series No. 001): Asian Law Institute (ALSI).

Weizhen, T. (2009, 3 Jun). Trojans target local online banking. *The Straits Times*.

WIPO. (n.d.). The World Intellectual Property Organization. Retrieved 4 May, 2012, from http://www.wipo.int/portal/index.html.en

Wong, T. (2012, 21 Apr). NET VIGILANTES: Are they going too far with online witch-hunts?, *The Straits Times*.

Yar, M. (2006). *Cybercrime And Society*. London: Sage.