Hee Jhee JIOW
Australian Endeavour Award Visiting Fellow

Singapore’s Cybercrime Regulation based on Lessig’s
Modalities of Constraint

Working paper No. 179
March 2015

The views presented in this paper are those of the author(s) and do not necessarily reflect those of the Asia Research Centre or Murdoch University. Working papers are considered draft publications for critical comments by colleagues and will generally be expected to be published elsewhere in a more polished form after a period of critical engagement and revision. Comments on this paper should be directed to the author at jhee@jiowheejhee.com

Copyright is held by the author(s) of each working paper: No part of this publication may be republished, reprinted or reproduced in any form without the permission of the paper’s author(s).
Singapore’s Cybercrime Regulation based on
Lessig’s Modalities of Constraint

Hee Jhee JIOW
jhee@jiowheejhee.com
Australian Endeavour Award Visiting Fellow

This paper is a revised and updated version of the publication in the International Journal of Cyber Criminology. I acknowledge the support of the Endeavour Scholarships and Fellowships Programme. The Endeavour Scholarships and Fellowships Programme maintain the position that the views in this paper are always specific to the author.

Abstract

Singapore is ranked as one of the most wired and cyber-ready nations in the world; it is internationally ranked the highest in terms of average per capita loss per victim of cybercrime. 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. To this end, this paper will begin with a survey of the global and local cybercrime scene, highlighting several pertinent characteristics of both victims and perpetrators. Adopting Lessig’s four modalities of constraint, this paper will examine Singapore’s approaches and efforts in its regulation of cybercrime, and will conclude by discussing Singapore’s challenges in regulating users’ behaviors in cyberspace.
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 87% of its population having broadband access (Infocomm Development Authority of Singapore, 2013a). With a mobile penetration rate of 156% (Infocomm Development Authority of Singapore, 2013b), and ready 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, 2013b). As such, the Internet has evolved into a space – usually termed ‘cyberspace’ – that Singaporeans ‘live’ in (Lessig, 2006). Moreover, the government has recently been actively promoting the usage of the Internet via The National Cyber Security Masterplan 2018 (NCSM2018) (Infocomm Development Authority of Singapore, 2015).

However, with increased Internet usage and penetration, a corresponding increase in the incidence of cybercrimes has frequently been observed (Broadhurst & Chang, 2012; Marsh, 2014). The Internet is increasingly becoming the domain and conduit of harmful activities and 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 cybercrime rates in the world, which is expected to increase significantly (Ministry of Home Affairs, 2010). Latest figures show that 61% of Internet users in Singapore have experienced cybercrime, and the average cost per capita due to cybercrime, which is more than four times higher than the global average, is the highest in the world (Marsh, 2014; Symantec Corporation, 2013a, 2013b). 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. With a glocalized perspective, it will begin by exploring common cybercrimes and harms, both global and local, and highlight certain trends and characteristics relevant to the
regulation of the Internet. It will then conclude by discussing Singapore’s Internet regulatory approaches, in terms of preventing its citizens from being either victims or perpetrators of cybercrimes. It will also consider future challenges.

Cybercrimes and Harms

Cybercrime is defined as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution” (Keyser, 2003, p. 290). The computer is central to the definition of cybercrime. It can be the object (target of the crime) or subject (site at which the crime took place) of the crime. These crimes are heuristically classified as "new crimes using new tools" (Jewkes, 2003). The computer is also the instrument or tool used to perpetuate a crime, and these acts are classified as "old crimes using new tools".

However, due to the “undeveloped international body of law” (Keyser, 2003, p. 294), certain social harms have not been deemed cybercrimes in some jurisdictions, and the perpetrators are prosecuted under existing criminal laws. An example is cyberbullying, which is prosecuted under existing stalking or harassment laws in some countries (Marsh, 2014). Therefore, the list, though not exhaustive, of cybercrimes and harms is as follows: hacking, identity theft, credit card fraud, email bombings, fraudulent schemes, phishing, password sniffers, spoofing, malicious codes (viruses, worms, Trojan horses, etc.), denial of service attacks, cyberterrorism, online hate postings, pornography, child pornography, cyberstalking, cyberbullying, cyberbaiting and software piracy (Jewkes, 2003; Keyser, 2003; Lessig, 2006).

According to the Norton Cybercrime Report 2011 (Symantec Corporation, 2011a), virus/malware attacks, phishing and online scams are the three most common cybercrimes globally. A study showed that hacking, fraud, intellectual property (IP) theft, spamming, identity theft and harassment are common cybercrimes in Singapore (APCERT, 2010; Jin-Cheon, Hao, Yong, Hao, & Kandan, 2009). As such, this study will explore the characteristics of victims and perpetrators of these common cybercrimes and harms. Though there are many ways to classify cybercrimes (Jewkes, 2003; Keyser, 2003), this paper groups them into new crimes using new tools and old crimes using new tools. While it may be worth considering crimes such as cyber-terrorist attacks on national infrastructure, this paper will limit its scope to crimes that affect individual users, as opposed to crimes on a larger, nationwide scale, such as cyber-terrorist attacks on national infrastructure or organized hacking attacks. To this end, the following section surveys the common global and local cybercrimes.
New Crimes Using New Tools

Viruses and malware are malicious computer software programs that cause damage or disruptions to other computer programs, steal information from the computer, or control the computer without permission (Kirwan & Power, 2012). These programs infect computer systems and networks, and are spread through sharing of contaminated computer files, especially through music and video files. Youths are especially susceptible, as they share and consume music and video content frequently, usually through peer-to-peer networks (Yar, 2006). Creation and spread of viruses, worms and Trojan horses are frequently committed by young people (Power, 2000; Verton, 2002). These creators are primarily motivated by the intellectual challenges associated with it, though there are some with financial or ideological motives.

These activities do not require a high skill level or technological knowledge of computer systems, compared to hacking. But not all hacking activities are considered criminal in nature. As such, ‘cracking’ is a term used to distinguish between legal hacking and the illegal type, which would lead to criminal prosecution. Cracking is commonly committed by young people, including preteens (Verton, 2002). Again, the motives of both hackers and crackers are quite similar. They typically “share a curiosity about computer systems” (Power, 2000, p. 11). This curiosity typically desensitizes the perpetrators to the moral aspects of their activities, eventually escalating to the commission of a crime. Again, there is a minority who does it for ideological or financial reasons. Power (2000) claims that though a virus writer may understand the capabilities of the coding of the virus, but “to really understand the implications of [the virus’] interaction with this huge monster we call ‘the Net’, no” (p. 13). Once virus writers have an appreciation about the severe consequences of their actions, they normally stop. Also, crackers have no qualms about attacking computer systems because they do not see what they do as an attack on humans, who can respond with an immediate display of pain or suffering (Parker, 1998; Power, 2000).

Some cybercrime perpetrators have been known to exhibit Differential Association Syndrome (DAS), which describes the rationalization that their harmful activity is not much different from what others (their peers or associates) are already engaging in (Parker, 1998; Power, 2000). For example, taking office supplies (such as paper clips and paper) for personal use and using the office computer resources for personal emails are not perceived as crimes, because it is perceived that every employee does it. Looking at a case study, it was this perception that led two programmers to use their company’s computers to run their own side business dealing in music. However, as their business grew, it ended up using 75% of the company’s computer resources (Parker, 1998). They ended up in prison for it.
Perpetrators have also been known to exhibit the Higher Ethic Motive (HEM), which describes them having to choose between two conflicting ethics (Parker, 1998; Power, 2000). For example, an accountant chose to embezzle company funds instead of allowing his mafia-linked bosses to profit from their ill-gotten gains (Parker, 1998). Perpetrators have at times demonstrated the Robin Hood Syndrome (RHS), a subset of HEM – stealing from the rich and giving to the poor (Parker, 1998; Power, 2000). In these cases, they justified their deeds by perceiving their companies as the rich, and themselves or others as the poor.

Another example of criminal rationalization is the case of a cracker who broke into his own bank account to engineer a delay in interest charges for his overdue payments, until he had fully cleared his debt. The rationale adopted was that no money was stolen, and no parties lost anything (Power, 2000). A youth cracker summed up his crime as an “addiction to knowledge, love of technology, and belief in the inherent freedom of information” (Verton, 2002, p. ix). As such, “overall, the cyber-criminal perceives himself as a problem solver rather than as a criminal” (Power, 2000, p. 15).

Besides being common victims of virus attacks, youths are also the largest group of IP violators, engaging in frequent illegal downloading of software, music and video files (Kirwan & Power, 2012; Yar, 2006). These perpetrators typically do it out of greed – wanting it free instead of paying for it – and instant gratification, or being unwilling to wait till the music or video is released on legitimate channels. But some also hold the perception that by copying music, video or software files, one is not denying anybody else of its use, unlike the traditional definitional requirement of physical theft (Kirwan & Power, 2012; Yar, 2006). Victims of these cybercrimes, especially virus attacks or IP infringements, typically do not have adequate technical safeguards installed on their computers or associated with their IP (Symantec Corporation, 2011a).

Old Crimes Using New Tools

Spamming is the sending of unsolicited messages to many recipients, which typically results in irritation to the recipients; in some cases, the recipients had been billed for it (Jin-Cheon et al., 2009). Spamming has also resulted in the slowing down of Internet traffic. Perpetrators of spam are motivated by the relative ease and cost effectiveness of reaching mass audiences with their advertisements, and may not be aware of the impact on the Internet traffic.

Cyberstalking is commonly defined as the online version of physical stalking, where the victim is repeatedly pursued or harassed in cyberspace (Petherick, n.d.). It does not require an intent
for the activity to be considered cyberstalking (Kirwan & Power, 2012). It was also found that most of these activities resulted from failed intimate relationships. Cyberbullying, on the other hand, refers to repeated activities, via cyberspace, intending to harm, harass or intimidate a person or a group of individuals (Kirwan & Power, 2012). More often, there is a power imbalance between the victim and perpetrator. As such, cyberbullying typically applies to situations in which the victims are minors (Ho, 2012). Hatred and a desire for revenge were identified as the key reasons for such perpetrators’ activities. They have been found to be distanced “from the realization of the harm that they have caused due to the lack of tangible feedback” (Kirwan & Power, 2012, p. 160). Anonymity, afforded by the Internet, facilitates this distancing very well. Statistics show that majority of the perpetrators and victims of cyberbullying or cyberstalking are students (Kirwan & Power, 2012). Academics believe that the growing popularity of social networking sites will fuel an increase in the frequency of cyberbullying and cyberstalking incidents, due to the ammunition available for perpetrators in the form of personal particulars being accessible online.

Associated with the intention of harassment are relatively new behaviors called cyberbaiting and sexting. Cyberbaiting is “a growing phenomenon where kids taunt their teachers, then capture the distressed reactions via cell phone videos” (Symantec Corporation, 2011b, p. 1). The footage is then publicized online with the intention to humiliate the teacher and the school. Sexting is commonly conducted by teens (Lenhart, 2009). It involves the online dissemination of naked pictures of a person whom one knows. Typically, this is done out of anger or for revenge due to a failed relationship; it usually leads to psychological trauma for the victim, who may go as far as committing suicide in extreme cases.

Identity theft occurs when one’s identity is stolen and used for unauthorized purposes, such as making payments for online purchases (Kirwan & Power, 2012; Parker, 1998). There are instances where the perpetrator impersonates another person online, but these cases do not normally result in a criminal prosecution. For identity theft to occur, it requires the victim’s personal details, which can often be obtained through searching extensively for information freely available online, keyloggers (often distributed via malware) or other scams such as phishing or pharming (Symantec Corporation, 2015). Online fraud or scam perpetrators typically promise more money for the victim in return for an outlay of a small, initial sum, thereby exploiting victims’ greed. Once these victims part with their ‘investment’, the perpetrators will abscond. Sometimes, the victims are deceived into transferring money to help a friend or loved one supposedly stranded overseas and in need of money for transport expenses or customs clearance back to their home country.

In these ways, perpetrators of these cybercrimes prey on victims’ ignorance and gullibility. Parker (1998) lists the perpetrators’ techniques as follows: baiting, name-dropping, bulletin-board
Reading, reading initial logon screens, mixing fact and fiction, exaggerating and lying, asserting authority, intimidating, threatening, and shocking, scorning, browbeating, belittling, aggravating, and exhausting, praising, sympathizing, flattering, aggrandizing, persistently calling false alarms, engaging in conspiracy, displaying artifacts, enticing and sexually attracting, eliciting loyalty, and intelligence gathering.

**Singapore’s Cybercrime 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). While the most recent high profile incident of hacking (of the Prime Minister’s Office website) was the result of the hacker’s dissatisfaction with the government (Poh, 2014), other recent incidents of hacking, virus or Trojan attacks in Singapore have largely been the products or results of scamming. Viruses and Trojans have been used to deceive victims into revealing personal information to access banking transactions (Tan, 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. 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 (Chua, 2010c). As such, many netizens have taken to shaming as a means to discourage negative or racist comments from flourishing in cyberspace (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 cyberbullying, 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 was second to the United States in the number of cyberbullying cases per capita (Gwee, 2008).

With more than half of all installed computer programs being pirated copies, Singapore’s IP violation 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.

**Trends of Cybercrime and Harms**

This section reviews some of the interesting trends of cybercrime and harms, globally and locally. Firstly, youths are increasingly not just the victims of crimes and harms, but are the perpetrators as well. This trend does not affect just a minority of youths, especially for burgeoning behaviors such as cyberbullying, cyberstalking, cyberbaiting and sexting (Tham & Toh, 2012). Secondly, perpetrators appear to have misguided rationalizations. RHS, HEM and especially DAS explain their rationalization processes, though some are done purely out of greed, that is, for financial gains. For harms such as cyberbullying, there seem to be a lack of appreciation of the magnitude and cost of the consequences of their actions. Some are committed out of mischief (as in cyberbaiting), or out of revenge (as in sexting), but they, too, lack understanding of their actions’ consequences. “As with most types of crimes, there is no single motive” (Kirwan & Power, 2012, p. 79) that accounts for all these behaviors. However, many of these behaviors observed stem from misjudgment of the consequences or inappropriate rationalization, such that perpetrators do not see their behavior as harmful or criminal. Thirdly, victims were not astute enough. This is particularly poignant in crimes that make use of social engineering to succeed (Parker, 1998). This suggests that the victims lacked the acumen and astuteness to realised they had been tricked. The following section of the review considers how these cybercrimes can be regulated.

**Four Modalities of Constraints**
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.

The Law
Globally, the law faces huge challenges in regulating the Internet. Firstly, only 10% of cybercrimes are reported, and less than 2% of reported cases resulted in successful prosecution (Jewkes, 2003; Symantec Corporation, 2011a). 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 cybercrime, 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 cybercrime by participating in schemes, such as the Wassenaar Arrangement that promotes the fight against terrorism (Singapore Customs, 2008), 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; Council of Europe, 2015). 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 cybercrimes 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 Singapore’s resolve in combating cybercrime. 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 cybercrimes, 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 (Attorney-General's Chambers, 2010) was revised to be more consistent with the United Nations Convention’s interest in promoting better security in online transactions. The Evidence Act (EA) 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 (Infocomm Development Authority of Singapore, 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 cybercrime, 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 cyberstalking or cyberbullying, rarely resulted in prosecution, but when it did, it was normally dealt with under CMA and other physical acts. However, the Protection from Harassment Act, which covers cyberbullying, online stalking and sexual harassment, was recently enacted to keep pace with the changing online harassment landscape (“Protection from Harassment Act,” 2014). 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 statues 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). Recently the Personal Data Protection Act was enacted to protect personal data and allows individuals to legally exercise their option to be excluded from marketing messages (Marsh, 2014; Personal Data Protection Commission, 2014).

In summary, Singapore has been consistently updating its laws in response to the cybercrimes experienced and perpetrated locally. It has been aligning its laws with the global community, and also extending its territorial jurisdiction to help tackle cybercrimes both locally and globally. It has been touted as one of the countries with the “toughest and most detailed cybercrime 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.

The Architecture
The architecture of cyberspace, though affording a technical solution to the prevention, monitoring and enforcement of cybercrime, 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), technology 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 cyberspace” (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 Infocomm Development Authority (IDA) is the governmental organization responsible for Singapore’s infocomm development and security. To this end, IDA initiated NCSM2018, which includes the enhancement of Critical Infocomm Infrastructures (CII) (Infocomm Development Authority of Singapore, n.d.-b). The NCSM2018 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 (Infocomm Development Authority of Singapore, n.d.-b). Investigative technologies are housed in SingCERT and the Technology Crime Division of Criminal Investigation Department, which arguably sends the message that cybercrimes will not go unnoticed (Infocomm Development Authority of Singapore, 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 (Infocomm Development Authority of Singapore, n.d.-a; 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 cyberbullying. But the low incidence of pure cracking activities (not by obtaining of personal information such as passwords through 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, signifying its cultural and legal stand against possession of such material, is a demonstration of such pragmatism (Ang & Nadarajan, 1996).

**The Markets**

With most digital content practically free in cyberspace, the impact of market forces are 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, 2011a; Yar, 2006). These perpetrators do not want things cheap; they want it free, and they can get it in cyberspace (Chua, 2010a; Goh, 2012; 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 (Chua, 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).

**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 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 (Chua, 2010c; Jin-Cheon et al., 2009; Wong, 2012).

Aside from being a powerful constraint, global and local trends in cybercrime suggest that it is the most relevant mode of regulating cyberspace behavior. Firstly, with high involvement rate of youths in cybercrime perpetration, 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 DAS, 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, this paper proposes that educating users, especially youths, is the most appropriate strategy.

There have been extensive and ongoing efforts in educating youths on the dangers of cyberspace and avoiding victimization (Livingstone & Haddon, 2009; Media Development Authority of Singapore, 2007, 2010; Microsoft Corporation, 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, 2011a). However, efforts in preventing the perpetration of cybercrime 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 Media Development Authority (MDA) of Singapore lists four core values necessary for cyberwellness – “Balanced Lifestyle, Embracing the Net and Inspiring Others, Astuteness, Respect & Responsibility” (Media Development Authority of Singapore, 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 cyberspace, 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. The Media Literacy Council, which was recently set up, was tasked to enhance the cyberwellness education. While the council articulated the four core cyberwellness values into five characteristics of a “digital and media literate person” (Media Literacy Council, 2013, p. 1), the thrust remains the pretty much the same.

**Conclusion and Future Challenges**

In conclusion, no prior attempt has been made to review Singapore’s regulation of Internet behaviors using the four modalities of constraint. Without actual (versus reported) data on the cybercrime
prevalence rate, which is challenging to come by (Jewkes, 2003; Symantec Corporation, 2011a), the effectiveness of each constraint is hard to assess well. Future studies would do well with such data available. Despite this, this study has attempted to present just such an assessment.

Surveying the prevalence and characteristics of cybercrime, 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 cyberspace. To this end, Singapore has adopted a ‘light touch’ philosophy towards cyberspace, by placing an emphasis on education. But it takes a tougher stance on the financial integrity of cyberspace 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 cybercrimes.

In preparing its citizens to be digitally ready, Singapore has to consider the challenges that each modality presents. This paper recommends that this exercise be pursued holistically, with education as its primary means of regulating online behaviors – especially so in a season where Singapore reported sharp increase in social engineering type of crimes (Singapore Police Force, 2015).
References


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


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


Tham, I., & Toh, K. (2012, March 28). Racist posts: Culprits 'tend to be young', The Straits Times.


