Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
1 INTRODUCTION

1.1 DEFINITION OF CLOUD COMPUTING

Although the term “cloud computing” has already been used elsewhere in this publication, for ease of understanding, in this chapter I follow the model used by Quick et al. in their 2014 book, *Cloud Storage Forensics*. Basically, cloud computing comprises three models:

*Cloud IaaS*: This provides clients with access to storage space, bandwidth, and other fundamental computing services. It effectively expands the computing capability of the customer, allowing them to run their own software and applications using the cloud infrastructure;

*Cloud PaaS*: This allows the customer to gain access to the computer platform or operating systems of the cloud instances (e.g. Windows and Linux) and an underlying database so that they can create or acquire applications;

*Cloud SaaS*: This allows clients of the CSP to utilize software and applications running on the cloud infrastructure. The applications are accessed via remote computers and mobile devices using the appropriate cloud interface software. The consumer’s device acts like a portal to the software and data stored in the cloud.

However, describing cloud computing crime in simple terms has been a challenge ever since the early days of the Internetwork revolution. A variety of terms are used when explaining the criminality associated with the popularity and commercialization of information communication technology (ICT), including “new technology crime,” “online crime,” “cybercrime,” and “Internet crime.” These terms tend to be used interchangeably, which makes it difficult to provide universal definitions. ICT is constantly evolving along with the associated criminality, including cloud computing crime. In addition, certain types of online activities considered to be...
“Internet” or “cloud computing” crime in some countries are not considered as such in others. For example, in most Western common law countries, if a female posts topless beach holiday “selfies” on Facebook via a smart mobile phone to share among friends, the act would be considered a harmless private activity. In many Muslim countries, and certainly those in the Middle East, however, the act would be considered a criminal offense; the woman would be subject to criminal prosecution in court and the act would be punishable by public lashing. Both polity and invested interests are at play, and the novelty of the “risk” or “threat” posed by new forms of technology-associated crimes can be used to support a larger share of government funding.

Cloud computing crime has become a broad term that embraces all forms of digital crime such as television and film piracy and location-based smart mobile phone crime. The growth and development of cloud computing crime has largely been a consequence of the expansion of cloud computing environments capable of facilitating criminality. Thus, for the purposes of this chapter, “cloud computing crime” is any criminality committed with the aid of recognized cloud computing models, including the smart mobile phone operation system model.

1.2 GROWTH IN CLOUD COMPUTING: HONG KONG AND SINGAPORE

In recent years, places such as Hong Kong, Singapore, and other parts of Asia have witnessed noticeable growth in cloud computing. The popularity of smaller mobile computing devices such as smart phones, which have resulted from advancements in Internet technologies, has been combined with the nature of cloud computing, which provides faster, easier access to files in remote locations, to allow users to access and update files on the move. Although cloud computing technologies offer efficiency in terms of users’ hardware requirements and access barriers, they also create challenges for both law enforcement authorities and individuals alike. One such issue is the policing of computer-related crime, which involves gathering evidence from, storing data in, the cloud, and then prosecuting the perpetrator. Scholars have drawn attention to some of these issues, but the socio-legal perspective treated here has not received much attention in the literature to date. Policing priority is typically set by country or place individually according to their needs. Factors affecting policing include the economy, legal traditions, police structure and organization, cultural factors, and political structure. The protection of these factors and their perceived importance is different in each jurisdiction and under each government in power, and thus policing varies accordingly.

This phenomenon is also true for policing the Internetwork, as the development and level of Information Technology (IT) access and infrastructures differ in different parts of the world. For instance, in accordance with the United Nation International Telecommunication Union (UNITU) report on the digital divide in 2012,¹ IT

¹See United Nation Telecommunication Union Report (2012).
disparities in terms of access to information and communication technology are pronounced between the developed Western economies such as those of America, Canada, and Western European countries (this group includes a few advanced economies in Asia such as those of Japan, South Korea, Singapore, and Hong Kong), and the less-developed economies such as those of Northern Africa, Latin America, Pacific Ocean Islands, and some parts of South Eastern Asia. The level of policing for the Internetwork is also different, as each country prompts different government perceptions of its level of technology risk or economic threat. These perceptions are largely dependent on the level of technology each country relies on to generate wealth, and sometimes on how much a given government sees technology as a threat to its political structure and systems. Thus, technology policing is prioritized differently from country to country.

However, the same UNITU 2012 report stressed that the digital divide had closed significantly between developed and developing nations, particularly in South East Asia and numerous African countries due to the increase in portable devices such as smart phones and the decrease in their cost. As International Telecommunication Union (ITU) director Brahima Sanou\textsuperscript{2} said:

\textit{The surge in numbers of mobile-broadband subscriptions in developing countries has brought the Internet to a multitude of new users. Despite the downward trend, prices remain relatively high in many low-income countries. For mobile broadband to replicate the mobile-cellular miracle and bring more people from developing countries online, 3G network coverage has to be extended and prices have to go down even further. \ldots Mobile-cellular subscriptions registered continuous double-digit growth in developing country markets, for a global total of six billion mobile subscriptions by end 2011 \ldots noting that China and India each account for around one billion subscriptions. Mobile broadband continues to be the ICT service displaying the sharpest growth rates. Over the past year, growth in mobile-broadband services continued at 40 per cent globally and 78 per cent in developing countries. There are now twice as many mobile-broadband subscriptions as fixed-broadband subscriptions worldwide.}

The increased ownership of smart phones in these countries has not only narrowed the gap between them and traditional fixed-location devices such as desktop computers, but also shifted the information and communication technology landscape. The technique of virtualization in cloud computing has created an economy of scale, such that services are only provided when there is consumer demand. This allows service providers to reduce their materials and service costs. On one hand, almost all smart phone devices now allow users to constantly connect with the Internetwork on the go; anytime, anywhere. On the other hand, to enhance the user’s smart mobile phone experience, service providers must design their services based on users’ needs. This can result in compromised safe-guards and security, which in turn create opportunities

\textsuperscript{2}United Nation Telecommunication Union Report (2012).
for criminal activity, and authorities have yet to catch up to these technologies, especially when perpetrators can be located overseas or in different police jurisdictions.

The increase in mobile smart phone use has also been rapid and significant in Singapore and Hong Kong. To put it in perspective, according to the Nielsen smart phone report in 2013, both Hong Kong and Singapore were ranked at the top for smart phone penetration rate in the Asia Pacific region, with more than 87% of their populations owning smart mobile phones. As Sagar Phadke, Director of Nielsen’s Telecom and Technology Practice in Southeast Asia, North Asia, and the Pacific said:

The growth in connected device ownership across Asia Pacific has been staggering in recent years. While this growth is expected to begin levelling out, consumers’ use of connected devices will continue to evolve and expand, presenting vast opportunities for organisations to engage with consumers on an almost ubiquitous platform. It is becoming more critical than ever for companies to develop sophisticated mobile strategies designed to leverage changing connected device behaviours and develop ongoing consumer engagement.

There has been an ample and growing opportunity for smart phone commerce in fields such as mobile banking, games and videos, and advertising in the Asia Pacific region, particularly in Hong Kong and Singapore. However, the rapid increase in smart phone use and penetration has greatly increased the potential for corresponding growth in smart mobile phone crime. For example, according to a 2011 KPMG International report on cybercrime, cybercriminals are moving beyond desktop computers to target smart mobile phones and other mobile devices. The report stated that in the previous 2 years, digital crimes specifically targeting mobile devices had risen 46%. Although the actual level of smart mobile phone crime is not known, and what is known is probably just the tip of the iceberg, the potential for problems is sobering. What follows are examples of smart phone crime in Hong Kong and Singapore.

In Hong Kong, a local Chinese newspaper reported that during the 2014 World Cup, the Hong Kong Police noticed that betting on illegal football matches through mobile phone apps increased. Mobile apps have also been used to sell counterfeit goods in Hong Kong. In a joint operation between Customs and Excise and the police in April 2014 in the Tsim Sha Tsui area, 7 people were arrested and 1156 items of suspected counterfeit goods valued at HK$270,000 were seized. In July 2014, a similar operation was mounted by the Hong Kong authorities and 42 people (7 of whom were younger than 22) were arrested and goods valued at about HK $340,000 were seized. According to Hong Kong authorities, in the first 6 months

---

3Cited Media Research Asia (2013).
4Media Research Asia (2013).
5See KPMG International (2011).
6See Sing Tao Daily Newspaper (2014).
7See Press Release (2014a).
8See Press Release (2014b).
of 2014 the number of people arrested who are younger than 22 has risen by 67% compared to the same period in 2013. In these cases, most of the young offenders participated in the sale of suspected counterfeit goods on Internet platforms via mobile phones, through auction sites or social networks, during their leisure time. Other types of crime have been committed using smart mobile phones. In January 2014, according to Paul Gordon, Sai Kung divisional commander, thieves used surveillance cameras to monitor their targets instead of doing their own reconnaissance:

“A device will be fixed outside a house and linked to their [smart]-mobile phones, to monitor when it is left unattended. Then they will take the chance to break in. The device was low-tech and could be bought cheaply in the Sham Shui Po electronics market. But it was the first time police had seen it used in this kind of crime.”

In Singapore, for example, according to a report released by WebSynergies, there have been a million Singaporean cybercrime victims. The report estimated a total of US$1 billion lost through cybercrime over the period of a year. Smart mobile phones have become the tool of choice for cybercriminals in Singapore, as viruses can migrate from Personal Computers (PCs) to mobile devices. The incidence of related petty crimes such as smart phone snatching has also risen. In another example from Singapore, Channel News Asia interviewed an Inspector of the Singapore Police. During the live interview, conducted on April 23, 2014, the Inspector described a smart mobile phone crime case involving a woman in her late 40s who was an accountant by profession. She allegedly befriended a male who claimed to be a pilot for Singapore Airline. They met and chatted on Whatsapp through their smart phones for some time, and ultimately agreed to meet face-to-face in a café near the Singapore International Airport. The supposed pilot told the woman that he had been in a hurry to get out of his flat and had forgotten to bring enough Euros with him. He asked the woman if she would transfer 2000 Singapore dollars to a certain bank account under his name, so that when he landed in Germany the next day he could withdraw the cash from an ATM. He promised to repay her in a week’s time, when he returned. The woman agreed and transferred the money via her smart phone. For some time, she did not hear from the man and could not contact him on Whatsapp. After 4 months she reported him to the police. The man was eventually arrested wearing a pilot’s uniform near the international airport, in a sting operation mounted by the police after a few more women fell victim to his scam and reported him.

---

9See Mok and Lo (2014).
10See WebSynergies.
11The Researcher has watched this program on April 23, 2014, at 10 p.m., live at home and took note for the case.
12WhatsApp is a live chat application use on smart mobile phone, in August 2014, tweeted by WhatsApp CEO Jan Koum, which revealed more than 600 millions of registered active users globally.
We only know about these cloud computing-enabled smart mobile phone crimes because they were in the public domain, but the true level of such crime remains unclear. The lack of reports on cloud computing crime is probably related to the fact that cloud computing is a relatively new concept for law enforcement authorities. The term was only coined in the late 2000s. Victims of cloud computing crime might not even realize their status as such, or they may choose not to report it, as the police are sometimes unable to recognize it as such and instead record it as traditional street crime. Even when the police recognize and record an event as cloud computing crime, they may have difficulty following up, especially if the servers and data involved are located overseas or in multiple jurisdictions. As Quick et al. explain, “the key component of cloud computing is multi-tenancy capability, which is referred to as a shared pool of resources . . . individual files may be distributed across multiple disks and storage systems across multiple jurisdictions.”13 Securing and preserving a chain of evidence for prosecution in court involves significant police resources, and even if the culprit is deported to face justice, the case may not pass the prosecution’s test of public interest and the perpetrator could escape justice.

2 KEY FACTORS SHAPING “RESPONSE”: HONG KONG, SINGAPORE

2.1 HONG KONG

2.1.1 Economy

Hong Kong, founded by the British for trade purposes, was a British colony for over 150 years before it was restored to the People’s Republic of China (PRC) on July 31, 1997. As an entrepot14 and capitalist enclave without natural resources, Hong Kong’s economy has largely been dependent on international and interregional trade. In the intermittent period between the 1950s and the early 1980s, Hong Kong was labeled a sweat-shop for the world’s light manufactured goods, but with the open-door policy introduced by Communist China in 1978, Hong Kong industrialization came to an abrupt end in the early 1980s. Almost all of the manufacturing factories were moved northward across the border to Shenzhen City or beyond in mainland China, due to cheaper wages and land. By this time, Hong Kong was beginning to establish itself as a financial center and professional services hub, largely serving the booming mainland China economy supported by the open-door policy and the growth of the Asian economy. By the beginning of the twenty-first century, Hong Kong had become well established as the fourth largest global financial and banking center in the region. Over 90% of Hong Kong’s Gross Domestic Product (GDP) is generated from nonmanufacturing-related industries, including banking, financial and professional services, and retail.

13See Quick et al. (2014, p. 5).
14Entrepot is a term use to describe a place where merchandise can be imported and exported without paying duties or tax, therefore the profit is being maximize.
Without other industries to generate wealth for Hong Kong, what is left is its status as an international financial center and its professional service-based industry, both of which are highly dependent on modern ICT to operate from, protect, and maintain the integrity of Hong Kong’s ICT infrastructure.

2.1.2 Cultural factors
To its advantage, culturally, Hong Kong has been very receptive to newer technologies. The rapid adoption rate of smart mobile phones is one example. This is partially due to the fact that most new technology is manufactured in Asia, and thus the closest source of production is relatively cheap to purchase. Hong Kong’s per capita income is also relatively high (at US$38,124 in 2013), and that wealth and purchasing power means the general population can afford to buy newly marketed technology rapidly, and as such they have become increasingly technologically savvy. For example, Hong Kong was one of only a few places on the globe to launch Apple’s iPhone 6 in August 2014.

2.1.3 Political structure
Hong Kong’s political structure reflects its legacy as a British colony. Characterized as a semiauthoritarian city state, Hong Kong did not become a democracy after its return to the PRC in 1997. Although there is currently an ongoing debate in Hong Kong over the democratic election (supposedly one man, one vote) of the Chief Executive of the Hong Kong Government Special Administrative Region in 2017, things remain uncertain because Beijing is wary about democracy in Hong Kong out of a fear that it might become a base for subversion to undermine the communist party rule in mainland China.

Hong Kong’s governmental decision making is semiauthoritarian and top-down in nature, and the selection of the Chief Executive (formerly Governor) is tightly controlled from Beijing. Only 1200 members of a select committee are allowed to vote in the Chief Executive election, and a great majority of them are pro-Beijing merchants and professionals. The first Chief Executive was a well-known shipping tycoon, and the man who currently holds the office is also a well-known professional-turned-merchant. The Hong Kong Executive Councilors (the executive branch of government policy decision-making body, who act as a cabinet to the government) are largely appointed from a pool of merchants and professionals. Government policy does not answer to the public, and the general population does not vote the government into power. Policy answers only to Hong Kong’s tycoons the small number of select committee members and the political master in Beijing. Ultimately, government policy’s priority is to protect and reflect the interests of the ruling elite and their supporters, rather than those of the general public, because the latter does not vote.

Since Hong Kong’s reintegration with China in 1997, there have been fears that some of the former’s core values are being threatened, such as the erosion of rule of law due to the ways in which things are done in mainland China (corruption, nepotism, gangsterism, and the use of power and connections to avoid the law). Some events have been cause for concern in Hong Kong. For example, Beijing interpreted
the Basic Law (the mini constitutional law of Hong Kong) in the late 1990s and early
2000s, but the major clash between Beijing and Hong Kong over the rule of law
occurred in 2003, when Beijing instructed Hong Kong’s government to introduce
Article 23 into the Basic Law to regulate subversion. Article 23 is similar to the
national security laws in many Western countries, but the very idea of such a
law was new to postcolonial Hong Kong, and given the Chinese Communist Party
and the Chinese government’s track record, it sent chills down the spines of
many in Hong Kong. The legislative process for Article 23 triggered a mass public
outcry, with over half a million people protesting in the streets against the legisla-
ration. Eventually, Hong Kong’s government put the National Security Bill on hold
indefinitely, temporarily shielding the rule of law in Hong Kong from being
“mainlandized.”

However, the “mainlandization” of Hong Kong has accelerated, especially since
2003, after a series of crises including the Asian financial crisis in 1997 and the
avian flu and severe acute respiratory syndrome outbreaks. These crises prompted
Hong Kong to actively seek help from the mainland and push for greater economic
integration. The Closer Economic Partnership Arrangement between mainland
China and Hong Kong is a case in point. Politically, it is in Beijing’s interest to
help Hong Kong, as it would be seen as a failure for Beijing if Hong Kong failed
only a few years after reintegration. These factors have helped to accelerate the
pace of Hong Kong’s integration with the mainland, both politically and
economically.

2.1.4 Criminal justice and legal systems

Hong Kong’s police force, as an arm of the government established in the early
1840s, is directly funded by the government. The Commissioner of Police is
appointed by and answers directly to the Chief Executive. The police force as a
whole is directly accountable to the government officials at the Security Bureau.
The Commissioner of Police, government officials, and the Chief Executive can
be called before the Legislative Council to explain their decisions on issues relating
to policing, but because Hong Kong is not a democratic society, the priorities for
policing in Hong Kong are not set by election manifesto. Thus, policing priorities
are more likely to reflect the interests of the officials at the highest level of
government than those of the general public.

As a former British colony, Hong Kong is founded on common law. The main
piece of legislation on computer-related crime is the Computer Crimes Ordinance
of 1993. According to a report released by the Hong Kong interdepartment working
group on computer-related crime, the Computer Crimes Ordinance was instituted by
amending existing laws and creating some new offenses to broaden the coverage of
the extant legislation. Hong Kong’s computer-related crime legislation is sufficiently
flexible to cover both the physical and the virtual worlds.15

15See Inter-department Working Group on Computer Related Crime Report (2000, pp. 5–8).
2.2 SINGAPORE

2.2.1 Economy

Like Hong Kong, Singapore was also part of the British Empire. However, unlike Hong Kong, Singapore gained independence from Malaysia in the late 1960s as a fully sovereign nation. Singapore’s economy is also different from that of Hong Kong. It comprises manufacturing (including hi-tech manufacturing and R&D), biotechnology, pharmaceuticals, electronics, technology and telecommunications, import and export, oil refinery, shipping and transport (South East Asian hub), financial and banking services and professional services, and retail. Almost 50% of Singapore’s export trades are interregional: Malaysia (12.2%), Hong Kong (10.9%), mainland China (10.7%), Indonesia (10.5%), and Japan (5.5%). Hence, Singapore economy is diverse.

As an independent nation, Singapore’s clear advantage over Hong Kong is that she does not answer to a political master and is free to decide her own economic policy. One benefit of this is Singapore’s technological policy. From early on in its independence, Singapore’s government has exploited technology as leverage for economic development.\(^\text{16}\) As a result, Singapore’s economy has improved by adopting technology as its bedrock to upgrade industries across the economy.\(^\text{17}\) Meanwhile, Singapore’s government has directly nurtured new technology-based industries, especially in the economy’s indigenous sectors such as IT, biotechnology, microelectronics, robotics and artificial intelligence, lasers/optics, and communications technology. The establishment of Infocomm Development Authority (IDA) of Singapore is a case in point. As Connie Carter put it:

> Few can doubt that Singapore is a successful example of a growth-oriented, interventionist, capitalist state... For four decades the Singapore government resolutely promoted economic development by: providing free market access to certain things; establishing and maintaining efficient infrastructure; orchestrating and investing in key export-led sectors of the economy; disciplining and educating the work force; and creating an ideology and delivering social justice and tangible benefits that secure the acquiescence of the people to the activities of the state and its elite bureaucrats.\(^\text{18}\)

Singapore’s technological economy policy not only directly rewards indigenous sectors for innovation and high-tech adoption, but Singaporean society at large also benefits from this technology-focused economy policy by being receptive to newer technology and becoming early adopters of high-tech products. The high penetration rate of the latest smart mobile phone is such an example.

---

\(^{16}\text{Loh (1998, p. 46).}\)

\(^{17}\text{Ibid., p. 47.}\)

\(^{18}\text{Carter (2002, pp. 1–2).}\)
Unlike Hong Kong, Singapore is not dependent on a single industry to generate wealth. Despite being capitalist and unlike Hong Kong, whose government is not directly involved in the economy, the Singaporean government is deeply involved in the economy.\(^\text{19}\) In Singapore, the domestic economy is largely dominated by two sovereign wealth funds: Temasek Holdings and GIC Private Limited (formerly known as Government of Singapore Investment Corporation, GIC). They are used to manage the country’s reserves. Initially, the state’s role was oriented more toward managing industries for economic development, but in recent decades the objectives of Singapore’s sovereign wealth funds have shifted to a commercial basis. As a result, in recent years, government-linked corporations (GLCs) have played an increasingly substantial role in Singapore’s domestic economy. The top six Singapore-listed GLCs account for about 17\% of total capitalization of the Singapore Exchange. These fully and partially state-owned enterprises operate on a commercial basis and are granted no competitive advantage over privately owned enterprises. State ownership is prominent in strategic sectors of the economy, including telecommunications, media, public transportation, defense, ports, airport operations and banking, shipping, airlines, infrastructure, and real estate.

For example, IDA is the Singaporean government’s invisible hand—a statutory board of the Singapore government under the Ministry of Communications and Information. It was formed in 1999 when the government merged the National Computer Board and Telecommunication Authority of Singapore to facilitate the convergence of IT and telephony. With an annual budget of more than S$34 million, the IDA is responsible for the development and growth of the infocomm sector in Singapore, and it functions as the country’s infocomm industry champion, the national infocomm master planner and developer, and the Government Chief Information Officer. The IDA’s most recent project has been Intelligent Nation 2015, a 10-year master plan. Singapore is aiming to be the first nation in Asia to be considered an IT-related “Smart Nation.” In 2014, Singapore has achieved a number of top benchmarks, including having the most digitized government (with 98\% of government services online and in the cloud and more that 60\% of Singapore’s Information Technology and Communication (ITC) in the cloud) and being the most networked country in the world (with 97\% of the school-age population reporting access to a computer at home and 87\% of households reporting access to broadband).\(^\text{20}\)

### 2.2.2 Cultural factors

Like Hong Kong, Singapore is also very receptive to newer technology, and its population is technologically savvy. The British Broadcasting Corporation (BBC) has profiled Singapore as “...a hi-tech, wealthy city-state in south-east Asia.”\(^\text{21}\) Singapore’s per capita income is also relatively high (at US$55,182 in 2013). With this

---

\(^\text{19}\)Trocki (2006, p. 166).
\(^\text{20}\)See IDA.
\(^\text{21}\)See BBC News.
kind of wealth and purchasing power, the latest technological products are easily afforded by the general population. However, unlike Hong Kong, Singapore is recognized by its government as a multiracial society with different ethnicities (Chinese is the majority at almost 70%, with the rest of the population comprising those of Malay and Indian heritage). Singapore’s government has managed its society carefully, through social engineering of ethnicity and by providing subsidy housing (today over 90% of the population is housed through the government housing scheme) and socially engineering education, particularly that with an English language base. This has transformed Singapore from a society once characterized by sharp contrast between ethnic groups who spoke different dialects and were separated by a large wealth gap into an affluent, English-speaking, middle-class industrialized metropolis. This has made Singapore culturally different from many of its neighbors in South East Asia, with the former being more in tune with technological development around the world because English is the common language used in commerce and in top scientific publications. Thus, Singapore has had an easy time acquiring newer technological knowledge and upgrading their skills.

2.2.3 Political structure

In theory, unlike Hong Kong, Singapore is a democratic nation state with a parliament based on the Westminster model. The government is voted into office via a one man–one vote election process. Every 5 years there are free and fair elections. The majority party or coalition gets to choose the prime minister, who then selects his/her cabinet of ministers. However, in practice, there is a similarity between Hong Kong and Singapore. As Vadaketh explains, “Singapore has been governed as an authoritarian state. One party, the People Action Party (PAP), dominates parliament.”

Democracy in Singapore, however, is “Singapore style” or “Asian democracy” whereby political power is in the hands of few Singaporean elites. This “elite governance” or, more importantly the PAP, has been active since 1955 for almost 60 years. Decision making is largely a top-down process because there is little-to-no opposition in the parliament. As Low said, “the PAP government has viewed the economy and society as machines,” and since PAP came to power, its legitimacy has largely been gained through a strategy of social pacification and the institution of repression and redistribution. However, in recent years the PAP suffered a setback in the popularity vote at the 2011 general election, only receiving 60.1%, which was down 15% from the general election in 2001. PAP is facing the call for legitimacy in the government. Nonetheless, with more than 60% of the popular vote, PAP is still firmly in power.

Policymaking is largely pursuing economic growth, and anything else is a secondary consideration for the PAP government, as they believe that economic growth would benefit most segments of society.

22 Vadaketh (2014, p. 189).
23 Low (2014, p. 174).
24 See Dezalay and Garth (2010, p. 141).
2.2.4 Criminal justice and legal systems

Like Hong Kong, Singapore was a British colony, and thus it has a common law tradition and a court system similar to that of Hong Kong, with a Court of Appeals at the top (equivalent to the Court of Final Appeal in Hong Kong, since July 1, 1997), then the High Court and the subordinate courts such as District, Magistrates’, etc. However, the foundation of Singapore’s penal code is different from that of Hong Kong’s, as the former was taken from India’s penal code in its exact entirety\(^\text{25}\) and gradually developed a local flavor. Another difference is the Syariah Court,\(^\text{26}\) which Hong Kong does not possess. One of the important first local pieces of legislation was the Criminal Procedure Ordinance of 1870, which was subsequently revised in 1900. Over time, various criminal laws were enacted. One of the most relevant to IT was the Computer Misuse Act, amended in 1998. Although Singapore’s Computer Misuse Act followed the English act, one noteworthy difference from the Hong Kong Computer Crime Ordinance is that the offense created by the Singapore Act has extraterritorial effects, as Chan and Phang explain:

*Provided either the accused person was in Singapore at the time or if the computer, program or data was in Singapore at the time. This is in recognition of the widespread reliance on computer technology all over the world and its vulnerability to manipulation either from within our shores or abroad.*\(^\text{27}\)

As a former British colony, Singapore’s criminal justice system is a punitive regime with no jury at court trial and punishment based on hard labor. The prison system is designed to be as degrading as possible, and public caning is not a rare punishment for wrongdoers. Although Singapore’s prison system has been reformed in recent years with the introduction of concepts such as restorative justice, rehabilitation, education and training, the police, courts, and other regulatory agencies still take a hard line on crimes by “nipping them the bud” as a deterrent to others.

3 DISCUSSION

According to the Bitglass\(^\text{28}\) Cloud Adoption Report published in August 2014, over 60% of businesses are still hesitant to transfer their data to the cloud due to security risk concerns that are largely about the cloud core architect of leveraging on virtualization. For example, Dropbox for Android smart phones uses cloud technology, and each time

\(^{25}\)See Chan and Phang (2005, p. 245).

\(^{26}\)The Singapore Syariah Court was established in 1955 by the government as an institution in settling disputes between divorcing Muslim couple and related matters, such as maintenance, mut’ah-consolatory gift payable to the ex-wife upon divorce, custody care control and access to children, and matrimonial property (see Syariah Court Singapore).

\(^{27}\)Chan and Phang (2005, p. 256).

\(^{28}\)See Bitglass, 2014.
data are delivered over the Internetwork through different telecommunication channels, the data are virtualized, leaving the user unaware of which servers are involved or which host is delivering and its location, because the cloud only delivers a minimum volume of data stored for any given client.

Businesses that worry about data integrity and that fear losing their sensitive data have questioned whether their data are protected from outsiders and from other tenants sharing the same cloud data center. Small business is especially vulnerable to this, as Australian Institute of Criminology research\(^{29}\) in 2013 (Hutchings et al., 2013) shows that small business is vulnerable to side channel attack or cross-guest virtual machine breaches, because in cloud, resources are shared with different tenants at the same cloud data center. As a result, tenants might crossing the shared virtual machine segment and accessing the data of other tenants using shared physical resources. More importantly, the same research has identified that small business is more vulnerable because they operate in highly financially constrained environment when compared with larger “global multinational” business, yet they are induced by the promise of cloud computing to save on their ICT overhead. As Hutchings et al. said “However, in adopting cloud computing, it is this distinct operating environment that also renders small businesses vulnerable to criminal and security threats [once attack happened some small businesses might not able to recover from it and the business could possibly come to abruptly end].”\(^{30}\) Nevertheless, nearly 90% of the businesses in Hong Kong and in Singapore are regarded as small businesses employing less than 20 people. Interestingly, users also wonder whether the data are protected from the cloud provider. Cloud computing is largely modeled on the demand for access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services. All such resource sharing is to ensure fast provision and saving on costs. For example, US researchers were able to hack into Gmail accounts with a 92% success rate by exploiting a weakness in smart mobile phone memory. The same research also found that once a smart mobile phone memory has been exploited, there is a great risk of collateral damage to other mobile apps on the same smart phone. As Zhiyun Qian said:

*The assumption has always been that these apps can’t interfere with [each] other easily, but such assumption was wrong, one app can in fact significantly impact another and result in harmful consequences for the user.*\(^{31}\)

Although in theory Hong Kong and Singapore are exposed to similar risks and threats in the cloud, their level of readiness depends on how they perceive risk, as each individual jurisdiction interprets and responds to risk differently according to their unique policing needs. For example, Hong Kong would react strongly if its economy was threatened, particularly banking, financial, and professional services, because

---

\(^{29}\)See Hutchings et al. (2013, p. 4).

\(^{30}\)Hutchings et al. (2013, p. 7).

\(^{31}\)See BBC News (2014).
they represent the only industries by which wealth is generated. Hong Kong’s reputation as an international financial center is dependent on the integrity of its ICT. Thus, the Hong Kong police keep a watchful eye on the IT infrastructure to maintain foreign investor confident in Hong Kong, which creates employment and facilitates the payment of government taxes. Furthermore, as a part of China since 1997, Hong Kong must consider internal national politics, such as the growing threat of the separatist terrorism group from the Xinjiang region.

In June 2014, Hong Kong’s government proposed to upgrade its Technology Crime Division (TCD) to the Cyber Security and Technology Crime Bureau. They tabled a proposal to the Legislative Council and explained the rationale behind the upgrade:

*With increasing reliance on information and communication technology infrastructures and rising popularity of the Internet, local reports of technology crime have increased sharply by 18 times since 2002, i.e. from 272 cases in 2002 to 5,133 in 2013. The respective financial loss has also increased by almost 20 times from $45 million to $917 million over the past five years from 2009 to 2013. To enhance the Police’s capability in combating technology crime, the establishment of TCD has increased from 26 posts in 2002 to the current establishment with 98 posts. Nevertheless, the current setup of TCD, with limited manpower and as a division within the CCB, is not able to meet the challenges of the increasingly sophisticated technology crimes and cyber security threats, not to mention the constant support provided by TCD to other formations of the Police in various cases, such as death inquest and locating missing persons. Today, Hong Kong has one of the highest concentrations of Wi-Fi hotspots in the world, and 97% of households are able to access to broadband services. With a high mobile phone penetration rate of 237% which is expected to grow further, individuals, corporates, and critical infrastructure are prone to technology crimes and cyber security threats.*

Subsequently, a more dedicated police formation “organization and structure” is needed to tackle the fast growing technology crime trend, including smart mobile phone crime:

*... to tackle the fast growing technology crime trend have become one of the operational priorities of the HKPF. Given the rapid advancement in information technology and the transnational nature of technology crime, there is a pressing need to strengthen the overall capability of the HKPF in combating technology crime and cyber security incidents.*

Hong Kong’s police have carefully explained their strategies to the Legislative Councilors, to take effect once the new technology crime bureau is established in early 2015:

---

32 See LC Paper No. CB(2)1621/13-14(05) (2014, p. 1).
33 Ibid., p. 1.
Dedicated attention and strategic planning to tackle the fast growing technology crime trend have become one of the operational priorities of the HKPF. Given the rapid advancement in information technology and the transnational nature of technology crime, there is a pressing need to strengthen the overall capability of the HKPF in combating technology crime and cyber security incidents. With the establishment of a new bureau dedicated to the prevention and detection of technology crime and protection of cyber security, the HKPF’s capability in combating technology crime and handling cyber security incidents will be greatly enhanced through the formulation of long-term objectives and strategies and expanded and dedicated efforts in the following areas—

i) detecting syndicated and highly sophisticated technology crimes and conducting proactive intelligence-led investigation; providing assistance to critical infrastructure in conducting timely cyber threat audits and analysis in preventing and detecting cyber attacks against them;

ii) enhancing incident response capability to major cyber security incidents or massive cyber attacks;

iii) strengthening thematic researches on cyber crime trend and mode of operation, vulnerabilities of computer systems and development of malware;

iv) strengthening partnership with local stakeholders and overseas law enforcement agencies in information exchange and sharing of best practices to counter prevalent technology crime and cyber threats; and

v) developing new training programmes on cyber security and technology crimes.34

Hong Kong’s government recognizes the need to upgrade the police and equip them to face the ever-evolving technological landscape, with its ubiquitous mobile electronic devices such as smart mobile phones and tablets. Furthermore, after being reintegrated with China for more than 14 years, Hong Kong is far closer to China than ever before, economically and politically. The threat of terrorism from inside mainland China and especially from the Xinjiang region has increased, and this terrorist group is known to be quite IT savvy, often using social media to disseminate information and communicate with like-minded group members around the globe. They were said to have downloaded a video clip onto their smart mobile phones via the cloud and then watched it before carrying out their bombing attack inside mainland China. Therefore, the Hong Kong government must consider this type of threat. The increase in Muslim militant extremists represents an interregional, if not a global threat, and such militants are also known to use the electronic highway and smart mobile phones to carry out attacks and spreading ideological campaign material among themselves and other affiliated groups in Asia.

Like Hong Kong, Singapore is an important international financial center, yet its economy is more diverse, with a mixture of industries such as manufacturing,
oil refinery, shipping, and biotechnology. Singapore is a democratic and a sovereign state with self-determination, even though its democratic process is regarded as a “controlled” democracy because the PAP has been in power since the first day of independence from Malaysia more than 50 years ago, with little or no opposition in parliament. On August 18, 2014, in a Singapore National Day speech broadcast live on Channel News Asia, Prime Minister Lee Hsien Leong said, “Keep Singapore special in Asia” by transforming it into “a smart nation.” He introduced the Singapore Smart Nation Plan and provided detailed examples of a brand new housing community to be built in Jurong Lake District. The community will feature sensor boxes connected to fiber-optic lines deployed across the community and, eventually the entire country, at street lights, or bus stops. The sensor boxes can be designed to detect air pollutants, heavy rainfall, or traffic jams, or to report how full rubbish bins are, paired with cameras that can detect litter and remind litterbugs to pick up their trash. Singapore has already laid the groundwork for the Smart Nation plan. For example, fiber Internet is available to most households in the country, with super-fast 1 Gbps service costing as little as US$50 per month.

One of the key features of the proposed smart cities is the use of sensor boxes to set up wireless hotspots for a heterogeneous network, allowing smart phones and mobile devices to switch seamlessly between mobile data and Wi-Fi. Singapore has also set aside spectrum to create new super Wi-Fi networks with greater range and coverage but a lower power requirement compared to standard Wi-Fi. The network will also be used to transmit Smart Nation data via the cloud.

Singapore is controlled from the top-down; it is an authoritarian society. The government is trying to harness the power of technology to increase the economy’s productivity and efficiency. Therefore, if the PAP responds and wants to increase the resources provided to the Singapore police to further increase their ability to fight the growing threat of technology-related crime, doing so will be relatively easier than it would be in many other democratic societies in Western developed economies. Singaporean voters may not necessarily agree with the PAP’s decisions regarding finite public resources being transferred from other more pressing social needs, as when they voted to form the government. However, the PAP’s manifesto may not mention anything about resources being earmarked for fighting technology-related crime, rather they may prefer to say that they will tackle traditional street crime and other forms of crime important to Singaporean voters.

Even if both Hong Kong and Singapore have the resources to respond to the potential risk of surging smart mobile phone crime, cloud computing-related crime is relatively new, and what worked in the past for less mobile devices such as personal computers may not work for the constant connectivity inherent in mobile devices. In the cloud, the configuration is usually a many-to-many network. To maximize the computing efficiency, virtualization is adopted, and thus data storage is located in host machine severs located in a many different places or countries. As Gray explains:
Cloud technology offers wonderful potential for users in terms of convenience, ease of obtaining updates etc. However, it presents significant legal challenges. Our laws, largely based on notions of territoriality, struggle to respond to technology in which lines on maps are largely irrelevant.\(^{35}\)

Therefore, providing the financial resources is an important first step for law enforcement agencies to build up their policing capabilities in the cloud. Other important elements are also required, such as knowledge of the cloud and the skills to find and collect electronic evidence in a live flow of data on a distribution network in the cloud, especially in a virtual machine. For example, in cloud data environments, it is often not possible to access the physical media that stores a customer’s data, because cloud data are likely to be stored overseas and outside the investigating officer’s jurisdiction. As Hooper et al. noted:

*Even if the data is stored within jurisdiction, data distribution technologies [in cloud] may split a user’s data across a number (potentially thousands) of storage devices within the cloud computing environment. LEAs would need to rely upon the cloud technology and the cloud service provider to gain access to the data that is stored by a customer and this can introduce issues with chain-of-custody best practices.*\(^{36}\)

Another problem facing the investigating officer is the preservation of the cloud data evidence. The integrity of the data is important, so potential data evidence cannot be modified. However, when exporting cloud data evidence for examination by the investigating officer, there is a high chance of modification, as Hooper et al. explain:

*Preserved (to ensure that the potential evidence is not modified) function which many cloud computing environments do not currently support. Consequently, this could result in accidental modification of data as it is exported from the cloud computing environment for LEA [Law Enforcement Agency] use or intentional destruction of data by the suspect. Once the LEA has secured access to the cloud computing data, the format of the data is still not guaranteed and most of the prevalent digital forensic analysis tools have not yet been updated to decode the major cloud computing data export formats. While many IaaS data exports will likely mimic the data format that is currently supported as virtual machines, SaaS instances are more likely to use proprietary data formats and as such are unlikely to be supported by current tools.*\(^{37}\)

Finally, even if the police in Singapore and Hong Kong do increase their policing capabilities in smart mobile phone and cloud-related crime, the legal limitations

\(^{35}\)Gray (2013, p. 1).

\(^{36}\)See Hooper et al. (2013, p. 156).

\(^{37}\)Ibid.
remain a key factor in whether the perpetrator faces justice for the crime they have committed. Even though Singapore has enacted an extraterritorial law, because each country has enacted their own law according to their own socio-politic, socio-economic, cultural and legal traditions, and regulatory regimes, policing priorities differ by jurisdiction. There has been good progress on harmonizing the laws in recent years (INTERPOL 24/7 mutual legal assistant, Council of Europe Convention on Cybercrime, etc.), but the task remains problematic due to jurisdictional issues. Both Hong Kong and Singapore will have trouble bringing an overseas perpetrator from their country of domicile to face justice for committing a cloud computing crime in Hong Kong or Singapore.

In short, it is clear from this chapter that lots of catching up need to be done for Hong Kong and Singapore in order to beef-up their policing capability on cloud. At the domestic level, both governments in Hong Kong and in Singapore must provide sufficient financial support to the policing agencies to enable them to fight the emerging crime such as cloud and smart mobile phone crimes. Fighting technology-related crimes is an “arms race” which needs both money and human resources. More importantly, the government must provide training opportunities and education (including general public education to increase public awareness on emerging technologies crimes like cloud and smart mobile phone crimes and learning to cooperate with the private sector or businesses to reduce crime) for the law enforcement officers to upgrade their skills and knowledge on cloud which eventually help increase the success rate in bringing the perpetrator to face justice and punish them in court—as a deterrent to others not to commit the same offense. However, at the international level, it seems there is little that Hong Kong and Singapore can do to alter the current situation, except to participate actively within the international bodies and convention on technology-related crime, and to learn from other jurisdictions around the world on what they are doing and, at the same time, tap into latest information on cloud computing crime to get a head start in fighting the emerging technology-related crime for themselves in the region.

REFERENCES
BBC News. Gmail smartphone app hacked by researchers, August 22, 2014.
BBC News. Available: http://www.bbc.com/news/world-asia-15961759 (accessed September 13, 2014).
Bitglass. Available: http://www.bitglass.com/ (accessed August 27, 2014.).
Carter, C., 2002. Eyes on the Prize: Law and Economic Development in Singapore. Kluwer Law International, The Hague.
Chan, W.C., Phang, A.B.L., 2005. The development of criminal law and criminal justice. In: Tan, K.Y.L., (Ed.), Essays in Singapore Legal History. Marshall Cavendish, Singapore.
Dezalay, Y., Garth, G.B., 2010. Asian Legal Revivals. The University of Chicago Press, Chicago.
Gray, A., 2013. Conflict of laws and the cloud. Comput. Law Security Rev. 29, 58–65.
Hooper, C., Martini, B., Choo, R.K.K., 2013. Cloud computing and its implications for cybercrime investigations in Australia. Comput. Law Security Rev. 29, 152–163.
Hutchings, A., Smith, R.G., James, L., 2013. Cloud computing for small business: criminal and security threats and prevention measures. In: Trends and Issues in Crime and Criminal Justice, vol. 456. Australian Institute of Criminology, Canberra, Australia. May.

IDA. Available: http://www.ida.gov.sg/~media/Files/About%20Us/Corporate%20Publications/Corporate%20Brochures/Smart%20Nation%20Infographic.pdf (accessed September 6, 2014).

Inter-department Working Group on Computer Related Crime Report, 2000. Hong Kong Government, Hong Kong, September.

KPMG International, 2011. Cyber Crime—A Growing Challenge for Governments. Available: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf, accessed July 15, 2014.

LC Paper No. CB(2)1621/13-14(05), 2014. Legislative Council Panel on Security Creation of a permanent Chief Superintendent of Police post of the Cyber Security and Technology Crime Bureau. Hong Kong Police Force, Hong Kong, June 3.

Loh, L., 1998. Technological policy and national competitiveness. In: Mun Heng, T., Kong Yam, T. (Eds.), Competitiveness of the Singapore Economy. Singapore University Press, Singapore.

Low, D., 2014. What went wrong for the PAP in 2011. In: Low, D., Vadaketh, S.T. (Eds.), Hard Choices: Challenging the Singapore Consensus. NUS Press, Singapore.

Media Research Asia, 2013. Available: http://www.mediaresearchasia.com/view.php?type¼press&id¼3184 (accessed July 9, 2014).

Mok, D., Lo, C., 2014. Lockup or lose it, residents warned. South China Morning Post Newspaper, January 30.

Press Release, United Nation International Telecommunication Union Report, 2012. Available: http://www.un.org/apps/news/story.asp?NewsID¼43265&Cr¼digital+divide&Cr1#U7tFmf2KCM9.

Press Release, 2014a. Information Service Department, Hong Kong SAR Government, April 2.

Press Release, 2014b. Information Service Department, Hong Kong SAR Government, July 3.

Quick, D., Martini, B., Choo, K.K.R. (Eds.), 2014. Cloud Storage Forensics. Syngress, Waltham.

Sing Tao Daily Newspaper, 2014. Midnight World Cup Favours Illegal Bookmakers Drawing New Blood, June 10.

Syariah Court Lengkok Bahru, Singapore. Available: http://app.syariahcourt.gov.sg/syariah/front-end/SYCHome_E.aspx.

Trocki, C.A., 2006. Singapore: Wealth, Power and the Culture of Control. Routledge, London.

Vadaketh, S.T., 2014. The future of democracy in Singapore. In: Low, D., Vadaketh, S.T. (Eds.), Hard Choices: Challenging the Singapore Consensus. NUS Press, Singapore.

WebSynergies. Available: http://blog.websynergies.biz/?p=996 (accessed 27.07.14.).