AGC SINGAPORE | ATTORNEY-GENERAL'S CHAMBERS

CRIMINAL LAW CONFERENCE 2014

KEYNOTE ADDRESS BY THE HONOURABLE ATTORNEY-GENERAL STEVEN CHONG SC

17 JANUARY 2014

I. WELCOME AND INTRODUCTION

1 A very good morning to all of you. It gives me great pleasure this morning to welcome all of you to the second day of the Criminal Law Conference 2014. As the conference title "The evolving face of criminal justice – Developments and Challenges" suggests, the landscape of the criminal justice system is rapidly changing. In Day One of this Conference, we discussed how improvements in science and technology have had an impact on the criminal justice system.

2 While we enjoy the benefits of technological advances, there is a darker side to technology. With globalisation and the proliferation of information technology and social media, criminals have changed their *modus operandi* and are utilizing new technologies to commit new classes of crimes and expand the reach of their criminal activities. As criminals operate beyond traditional conceptions of national borders and sovereignty, it has become increasingly difficult to trace and stop their nefarious activities. In the face of this new challenge, we simply cannot afford to sit still. What we can and must do to stem the tide of these new vistas of criminal behaviour that rapidly crosses borders is the focus of today's discussion.

3 As crime goes global, international co-operation between law enforcement agencies becomes critical. No country, including Singapore, can realistically operate in a silo, disconnected from the world around us. It is imperative that we adapt accordingly and evolve with the times. Existing laws may have to be revised. New laws may have to be enacted to keep pace with these developments. Lawyers must recognise that the practice of criminal law is becoming increasingly complex and multi-disciplinary in nature and should therefore equip themselves with the appropriate skills to cope with these new trends.

4 The topics to be covered in today's session focus on criminal activities that are cross-border in nature. In the first session, we will consider money-laundering and the international efforts to combat it. Mr Rick McDonell, Executive Secretary of the Financial Action Task Force or FATF, will provide us with an overview of FATF and outline the international Anti-Money laundering and Counter Terrorist Financing standards, with a focus on how they apply to lawyers. Notably, the issue of a lawyer's duty to report suspicious transactions while maintaining obligations in relation to legal professional privilege will be discussed.

5 Next, we will face head on the issues thrown up by the interconnectedness brought about by technology, in the session on Internet Crime. Mr Keith Yeung, Director of Public Prosecutions in Hong Kong, will highlight the challenges of dealing with internet crime. In particular, the issue of extraterritoriality and the difficulties in the obtaining of intelligence and evidence overseas will be examined.

6 Finally, we will look at where the Criminal Bar stands, in this increasingly globalised world.

II. FINANCIAL ACTION TASK FORCE

7 The internationalisation of crime is evident from today's first topic.

A. BRIEF INTRODUCTION TO MONEY LAUNDERING

8. Money laundering is an extremely insidious criminal activity. There is increasing recognition that money laundering has been affecting the global economy. The numbers are staggering. In 2011, the United Nations Office on Drugs and Crime ("UNODC") estimated that global criminal syndicates, especially those involved in drug trafficking, could have laundered some 2.7% of global GDP or approximately US$1.6 trillion in 2009.[1]

9. Financial institutions such as banks and capital market firms are favoured channels through which illicit money is laundered across the world. If left unchecked, there is no doubt that money laundering will pose a grave threat to the integrity of the world's biggest financial institutions. In the well known HSBC money laundering scandal,[2] it was discovered that between 2006 to 2010, the Sinaloa cartel in Mexico and the Norte del Valle cartel in Colombia moved more than $881 million in drug

[1] http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf at pg 7
[2] http://www.bloomberg.com/news/2012-12-12/hsbc-mexican-branches-said-to-be-traffickers-favorites.html

proceeds through HSBC's US and Mexican branches.

10. Obviously, money laundering and other pernicious forms of criminal activity can only be reined in if we have an effective regulatory and law enforcement regime to counter them. This should be one of our main priorities today.

B. OVERVIEW OF FATF AND THE FATF RECOMMENDATIONS

11. The FATF, which was formed in 1989, is an inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and more recently, terrorist financing as well.[3] Comprising 34 member jurisdictions and 2 regional organisations, its core work is the promotion of its recommendations, to combat money laundering and terrorist financing.[4] These include recommendations requiring states to criminalise money laundering, to enact laws that allow authorities to confiscate the proceeds of money laundering and to apply preventive measures for the financial and other designated sectors. Although FATF recommendations are not legally binding upon the member countries, FATF generates political will within the member states to comply with its recommendations. Member states undergo periodic "Mutual Evaluations" to examine the extent of implementation and effectiveness of their anti-money laundering and counter terrorist financing regimes.

[3] http://www.fatf-gafi.org/pages/aboutus/historyofthefatf/
[4] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf

C. SINGAPORE AND FATF

12. Like any other global financial centre, Singapore's highly internationalised economy and well-connected business, financial and transportation hubs expose it to regional and international money laundering and terrorist financing risks. Singapore, which has been a member of FATF since 1991, is committed to the fight against global money laundering and terrorist financing. Our regulatory framework underwent its last mutual evaluation in 2008. We did credibly well and as a whole, we were assessed to be compliant, largely compliant or partially compliant for most of the 40 recommendations and 9 special recommendations. For those FATF recommendations that we were, in 2008, assessed to be 'not compliant' with, much effort has been undertaken to remedy the situation. For example, we did not, in 2008, have a mechanism for lawyers to comprehensively deal with money laundering risks identified in the course of their dealings with their clients. The Law Society has since issued a Practice Direction requiring lawyers to institute client due diligence measures, and to report suspicious transactions.

13. In preparation for the next mutual assessment in 2015, Singapore recently conducted a National Risk Assessment, which was a comprehensive government-wide exercise involving various ministries and government agencies including the Attorney-General's Chambers ("AGC"). The aim was to identify money laundering and terrorist financing risks peculiar to our economic, geographical and regulatory environment and to develop effective counter-measures. I recommend all lawyers, especially those who advise on financial transactions, to read the report.

D. AGC'S ROLE IN SINGAPORE'S FIGHT AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

14. As a key stakeholder in our justice system, my Chambers has a major role to play in Singapore's fight against money laundering and terrorist financing.

15. Given the transnational nature of such criminal activities, and the fact that evidence and money is often located overseas and may be moved instantaneously, it is imperative that investigations are conducted in a timely and coordinated manner. To this end, it is crucial that legal guidance and advice is readily available to investigators at the early stages of investigations.

16. Recently, my Chambers launched an initiative to embed Deputy Public Prosecutors ("DPPs") at several law enforcement agencies across Singapore. These DPPs provide immediate guidance to investigating officers and improve the quality of investigations.

17. AGC also has a satellite office at the Commercial Affairs Department ("CAD") where several experienced DPPs provide timely legal advice to CAD on *inter alia,* money laundering or terrorist financing offences. In addition, AGC set up the Economic Crimes and Governance Division ("EGD") which focuses on complex offences relating to the financial industry, corruption and other commercial offences.

18. In addition to cultivating a pool of local specialist knowledge within AGC, my prosecutors have received exposure to overseas training. Given the international nature of crime, it is crucial for us not only to understand how our counterparts in other jurisdictions operate but to nurture links with them as well. To this end, we have sent many prosecutors for overseas training and attachment stints. These include the Shanghai People's Procuratorate, the Serious Fraud Office in the United Kingdom and the Department of Justice in the United States and Hong Kong.

19. Lastly, the Mutual Assistance in Criminal Matters Act ("MACMA") permits the provision of a wide range of legal assistance to overseas law enforcement agencies even without a mutual legal assistance treaty.

20. All in all, there is a clear recognition within AGC of the need to be adequately prepared to counter the threat of money laundering and terrorist financing in Singapore and I am pleased with the work done thus far to achieve that end.

E. CHALLENGES AHEAD

21. Despite what we have achieved, we simply cannot afford to rest on our laurels. There is no room for complacency because with the emergence of the new frontier of global e-commerce, new opportunities will arise for avaricious money launderers. Not only does the Internet allow vast sums of money to be moved across jurisdictions instantaneously, it also allows transactions to operate with a hitherto unprecedented level of anonymity.

22. The recent Liberty Reserve case in the United States, which is believed to be the largest online money laundering case in history ought to be mentioned. Liberty Reserve was an online centralised digital currency service, which allowed users to transfer money to other users with only a name, an email address and a date of birth. Deposits could be made anonymously through third-parties using a credit card or bank transfers. Richard Weber, head of the Internal Revenue Service's criminal investigation rightly quipped that if Al Capone was alive today, this is how he would be hiding his money. More than US$6 billion was laundered through Liberty Reserve on behalf of drug dealers, child pornographers, identity thieves and other criminals around the globe.[5]

23. I believe Liberty Reserve is only the tip of the iceberg. The proliferation of digital currencies such as Bitcoin, allows criminals to work in a completely unregulated financial environment under the cloak of anonymity. Bitcoins are used for various purposes including the purchase of goods and services online. However, what is more worrying is that Bitcoin has increasingly been used for or associated with criminal activities. In October last year, it was reported that the Federal Bureau of Investigation in the United States seized over US$20 million worth of Bitcoin from the Silk Road – an online black market for illicit narcotics.[6]

24. In view of Bitcoin's links with fraud and money laundering, a number of

[5] http://news.yahoo.com/7-charged-6b-online-money-laundering-case-223715413.html
[6] http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/

countries have taken action to guard against the risks posed by the usage of Bitcoin. The Chinese central government banned financial institutions from handling Bitcoin transactions in December last year.[7] Analysts postulate that this and other measures could cripple Bitcoin trading in China.[8] Here in Singapore, Bitcoins are not legal tender.

25. Evidently, technological developments give rise to new avenues and techniques for criminals to operate and pose difficult challenges for law enforcement agencies. These challenges are multifarious. There may not be existing laws to regulate and punish online behaviour despite its devastating impact on society. Furthermore, even where there are laws to deal with such behaviour, authorities may not have the necessary powers to access evidence and to prosecute individuals. These challenges will be the subject of discussion of the second topic of today's conference.

III. INTERNET CRIME

26. The challenges posed by Internet Crime are manifold, but a significant one is the difficulty in marshalling evidence of crimes. As these activities occur across borders, the necessary evidence is often located in more than one jurisdiction. We must find the way forward to ensure that enforcement and prosecution is not stymied by national borders that are ignored or exploited by criminals.

[7] http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html

[8] http://www.channelnewsasia.com/news/business/bitcoin-crashes-after/926928.html

A. EXTRATERRITORIAL ISSUES OF OBTAINING EVIDENCE

27. Any discussion of the way forward in combating new forms of criminal activity must include a consideration of issues of extraterritoriality in the context of obtaining evidence to identify and prosecute criminals for their crimes. It has often been observed that criminal activities are undergoing a revolution in that network computers permit crimes to be committed remotely and a criminal no longer needs to be at the actual scene of the crime to prey on his victim. This makes it difficult to pinpoint the place where crimes are committed and investigate offences that occur across borders.

28. All these have serious implications on obtaining evidence. Large amounts of data are no longer stored on local computer hard disks, but in the "cloud". As a result of this phenomenon of "cloud computing", traditional search and seizure processes to obtain evidence are rendered largely irrelevant. Searching a suspect's physical computer may not produce any evidence of cybercrime. Instead, we may have to obtain evidence from the "clouds" or servers, which are often located overseas.

29. Consequently, issues of jurisdiction invariably arise. The territorial limitations of conventional investigative powers do not allow for the searching of remote servers located in other jurisdictions. It then becomes necessary to seek the assistance of foreign law enforcement counterparts to obtain "cloud" evidence located overseas.

30. This difficulty is compounded by the limitations in the contractual terms of service of the service provider with their users, or other legal impediments such as privacy and data protection laws, which may also differ greatly across jurisdictions.

B. POSSIBLE SOLUTIONS

31. A number of solutions have been proposed. To begin with, countries could enact domestic legislation with extraterritorial reach that seeks to empower domestic law enforcement to exercise their investigative powers to remotely access data stored overseas. For example, New Zealand has enacted the Search and Surveillance Act 2012, which unilaterally permits transborder access to data on systems or services used by suspects under investigation, such as Gmail accounts.[9] However, this may raise issues of interference with the sovereignty of another nation and may have limited value in terms of enforcement.

32. Alternatively, mutual legal assistance channels can also be utilised. However, this route which requires input from various agencies and hence time-consuming is not entirely satisfactory as cloud data can, by its very nature, be moved very quickly from one state to another.

33. Developing an international framework is, by far, the most viable option. Cloud computing and cybercrime, are both inherently "borderless" in the sense that the data we require as evidence is not geographically isolated or limited. In order to

[9] See s 103(4)(k) of the New Zealand Search and Surveillance Act 2012 http://www.legislation.govt.nz/act/public/2012/0024/latest/DLM2136795.html

effectively combat cybercrime, we must move away from the traditional notions of individuality of each nation and conventional conceptions of territorial sovereignty and jurisdiction to a mindset of cooperation between nations.

C. THE BUDAPEST CONVENTION

34. I will now touch on the Budapest Convention on Cybercrime ("the Convention"). This Convention is the first international treaty on cybercrime, which deals particularly with violations of computer and network security, copyright infringement, computer-related fraud, and child pornography. It provides for powers and procedures concerning the search of computer networks and lawful interception of data. Its main objective is to pursue a harmonized approach to protect society from cybercrime by adopting appropriate legislation and fostering international co-operation.[10]

35. Article 32(b) of the Convention is relevant as it permits transborder access to data without mutual assistance requests where there is consent by the "person who has the lawful authority to disclose the data". Arguably, Article 32(b) is limited in its efficacy as it relies on consent, and may not be a completely adequate solution to obtaining evidence stored in a cloud. This is primarily because consent may not be forthcoming from the user, the service provider or indeed the accused himself, in some cases and the definition of a "person with lawful authority to disclose the data" is also not without controversy.

[10] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

36. In this regard, various countries have developed innovative, and perhaps controversial, laws in relation to transborder access to data. The Portuguese Law on Cybercrime (Law No 109/2009) allows a judge to authorise a search of a computer system if the evidence sought "is necessary to uncover the truth". Under Article 15.5, Portuguese law enforcement officers may access data physically stored in a remote system in a foreign state, if a proper order (normally from the prosecutor but in certain cases from the judge) was duly obtained.[11]

37. In Belgium, Article 88ter of the Belgian Criminal Code of Procedure, which was a response to Article 32 of the Budapest convention, allows an investigating judge who is ordering a search of a computer system to extend the search to *another* computer system or to a part of another computer system located elsewhere in the world provided certain conditions are met.[12] It is noteworthy that Article 88ter also provides that when it appears that the data discovered is not stored on Belgian territory, the data is to be *copied* only, as opposed to transferred. This saves much time in the investigation process especially since the copied data is as valuable as evidence before the court as the original data.[13]

38. The Council of Europe has also recognised the limitations of the consent requirement in Article 32(b). In this regard, the Cybercrime Convention Committee established an ad-hoc sub-group on jurisdiction and trans-border access to data and

[11] Discussion paper – Transborder access and jurisdiction: What are the options? Strasbourg 6 December 2012, at para 199-202 http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf
[12] *Ibid* at para 163 and 164
[13] *Ibid* at paras 167-169

data flows ("the transborder group") in November 2011. This group has made preliminary recommendations that an additional protocol be negotiated which would permit transborder access without consent in limited situations, such as in good faith situations, where a searching party may not know for certain that the system searched is located in a foreign territory. The final recommendations of the trans-border group are scheduled to be released in late 2014, but there is no consensus, as yet, amongst the Parties to the Convention on whether the powers of transborder search should be expanded by way of an additional protocol to the Convention.

39. While wider powers of transborder search, without consent, would involve further derogation of the principle of sovereignty, as between parties to the Convention, there are a number of safeguards to assuage some States' concerns about any expansion of Art 32(b). My Chambers has raised some suggestions with a view to promote an international consensus. First, there should be a requirement to inform the other State of the access within a reasonable time. Secondly, there must be some accountability to the other State for the seized data. For instance, like in the case of Belgium, the data should be copied and not removed and should not be used for any collateral purpose. Finally, there must be exceptions which deny access to sensitive systems, such as data of the government, financial institutions and critical infrastructure.

40. In discussing this issue, it is vital to note that the interested parties involved are not only states, but also the companies that provide cloud services. This is especially true when dealing with huge companies with global reach, such as

Facebook and Google. They have far-reaching influence by virtue of the popularity of the services they offer, and have shown to be willing to do what it takes to stamp out criminal activity. For instance Google has recently announced measures to block child pornography from appearing in searches, to show their commitment to prevent child abuse.[14] Facebook has also banned decapitation videos so as not to irresponsibly glorify violence.[15] Their cooperation is pivotal. As such, their concerns must be recognised and addressed. For instance, it may well be that they should be provided with some form of statutory immunity when they cooperate in this fight against crime.

41. As the Council of Europe has emphasised, "Cybercrime is international crime which implies the need for efficient and immediate international co-operation to preserve volatile evidence across borders."[16] In the face of the new borderless and transnational nature of crime, we must embrace this new reality of cybercrime and understand that we need the cooperation of other nations to tackle it comprehensively. Ultimately, there must be an international consensus with an expansive reach.

IV. FUTURE OF THE CRIMINAL BAR

42. I now turn to consider the final topic of today's conference - the future of the

[14] http://www.telegraph.co.uk/technology/google/10456445/Google-vows-to-block-child-pornography.html
[15] http://gizmodo.com/facebook-changes-its-mind-again-its-now-re-banning-de-1450384342
[16] June 2007 Octopus Conference Interface Summary: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface2007/567%20IF%202007-d-sumconclusions1g%20Provisional.pdf

criminal bar. With new technologies and new breeds of criminal activities, the future looks bright and exciting for criminal lawyers. Another development which will make the future even more promising is the recent decision of the government to expand criminal legal aid by providing direct state funding for the Criminal Legal Aid Scheme. This is expected to benefit an estimated 6,000 accused persons a year. Furthermore, the Law Society will be considering the extension of legal aid to more types of offences. These changes will undoubtedly facilitate access to justice for those charged with criminal offences.

43. While funding for legal aid for accused persons is important, it is imperative that they should be well represented so that their rights are properly safeguarded. I have previously stated that there is a significant difference between legal representation on the one hand and competent and adequate legal representation on the other.[17] When I was on the Bench, I observed that a good number of lawyers practising criminal law are advocates of outstanding calibre and exemplify the best traditions of the Bar. There have, however also been instances in recent years where the Courts have made clear their disquiet about the adequacy or competence of the legal representation in criminal cases before them. I should make it clear that those cases are exceedingly rare but given the weighty issues of life and liberty that are invariably involved in such cases, it may be fair to say that one such instance of inadequate legal representation is perhaps already one too many.

[17] Keynote address by the Attorney-General at the Criminal Justice Conference 2013 (17 May 2013)

44. For us to have a first-rate Criminal Bar, we must attract capable advocates. Today, criminal practice is often seen as less lucrative and perhaps less glamorous than commercial law practice. We must take steps to change this existing mindset. Watershed changes have taken place to level the perceived disparities in the playing field between the prosecution and the defence. The criminal case disclosure regime introduced by way of changes to the Criminal Procedure Code in 2010 imposes *quid pro quo* obligations on both the Prosecution and Defence to disclose key aspects of their respective cases in order to achieve greater transparency.

45. There has also been discernible shift in judicial attitudes towards the practice of criminal law and the courts have taken a robust stand to level the procedural playing field. In *Muhammad bin Kadar & Anor v Public Prosecutor,*[18] the Court of Appeal grafted onto the legislative framework a common law requirement of disclosure by the Prosecution in certain circumstances. This was in stark contrast to earlier cases which suggested that there was no such duty on the part of the Prosecution. The robust stance of the Courts is also evident in the recent case of *Public Prosecutor v Goldring Timothy Nicholas & ors,*[19] where the Court of Appeal held that accused persons have an independent right of access to documents under their ownership, legal custody or control prior to police seizure.

46. To improve the Criminal Bar, we cannot overlook law students, some of whom will eventually join their ranks. Anecdotally many law students enter law school with

[18] [2011] SGCA 32
[19] [2013] SGCA 59

idealistic aspirations to practice criminal law but eventually pursue careers in other areas of the law. Steps must be taken to stem this tide. My Chambers has commenced several initiatives to assist in the training of the next generation of criminal lawyers. The Advanced Criminal Legal Process course provides law students with a first-hand sense of the intricacies and rigours of criminal legal practice. The AG's Cup, which is a heavily contested moot open to all law students, also generates considerable interest among law students in criminal law.

47. I believe that the opening of a third law school, which will focus on community law, will increase the number of criminal law practitioners. It is hoped that this together with other initiatives will bring about a sea-change in the perception of criminal law practice and will in turn attract more capable lawyers to the Criminal Bar.

48. As part of our efforts in increasing interest in criminal law, we have also reached out to schools in the hope of attracting prospective law students to a career at the Criminal Bar. We recently conducted our inaugural Public Prosecution Outreach Programme in November last year. Over two weeks, my prosecutors and staff visited 28 schools to deliver presentations on the role of the Public Prosecutor and the administration of criminal justice to more than 7,000 students. We received very encouraging feedback from the participants. I hope this enthusiasm will eventually translate into the growth and development of the practice of criminal law in Singapore.

V. CONCLUSION

49. As the practice of criminal law becomes more transnational and borderless, traditional notions of jurisdiction and sovereignty will become increasingly anachronistic. The criminal lawyers of the future will have to accept that mastery of local laws and procedures is no longer sufficient. Practitioners have to familiarize themselves with at least basic principles of international law and build up the necessary skills to be able to swiftly attain a working knowledge the relevant laws of various jurisdictions that may be involved in a complex case.

50. These are challenging but exciting times for the criminal justice system in Singapore. In the light of improvements in scientific and information technology coupled with the global nature of new variants of criminal activities, we must redouble our efforts to adapt to the changes and leverage on them in order to stay ahead and not allow criminals to get the better of us.

51. On that note, I wish all of you a productive second day at this conference. Thank you.