ALLEN & OVERY
PREPARED FOR THE INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN

COALITION OF STAKEHOLDERS AGAINST COMMERCIAL SEXUAL EXPLOITATION OF CHILDREN ON THE INTERNET

LEGAL FRAMEWORK AND OBSTACLES IN THE ASIA-PACIFIC REGION – PHASE I

December 2012
(Section on Hong Kong updated as of July 2015)

ALLEN & OVERY

International Centre
FOR MISSING & EXPLOITED CHILDREN

CONTENTS

Section **Page**

INTRODUCTION

REPORT REGARDING THE LEGAL FRAMEWORK TO BE CONSIDERED BY A COALITION OF STAKEHOLDERS AGAINST COMMERCIAL SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET

PREPARED BY THE A&O GROUP

ADDRESSEE

To: The International Centre for Missing & Exploited Children
1700 Diagonal Road, Suite 625
Alexandria, VA 22314 USA

This report (hereafter referred to as the **Report**) regarding the legal framework to be considered by a coalition of stakeholders against commercial sexual exploitation of children over the Internet in the Asia-Pacific region (hereafter referred to as the **APAC Coalition**) has been prepared by the A&O Group (as defined below) solely for the International Centre for Missing & Exploited Children (hereafter referred to as **ICMEC**) in connection with the proposed establishment of the APAC Coalition.

Allen & Overy LLP (as defined below) and any other member of the A&O Group do not accept any liability to any person in respect of any matter relating to the Report. The Report may not be disclosed in whole or in part to any person or entity other than ICMEC or quoted to any such person or entity in any other context without our prior written consent, it being understood that we consent to its disclosure, strictly on the basis of the terms of our engagement as agreed with ICMEC, to the APAC Coalition Members in connection with this project. There may be inaccuracies or information that has become outdated since this Report was originally written.

This Report is for reference only and does not purport to provide specific legal, financial, or business advice. If you require specific advice or counsel, you should consult with a proper professional. Allen & Overy and any other member of the A&O Group, ICMEC and the APAC Coalition make no warranties, expressed or implied or statutory as to the information in this Report.

The Report is based on the report dated 5 May 2008 addressed to Missing Children Europe and on our understanding of the APAC Coalition and our task as follows:

We understand that the intention of the APAC Coalition is to establish a coalition of parties that are involved in commercial Internet services and payments relating to commercial provision of Internet services (e.g. Internet service providers, credit card companies, banks and other online payment facilitators). The intention of the APAC Coalition is to fight commercial sexual exploitation of children over the Internet in the Asia-Pacific region by, amongst others, following the money flow triggered by the use of such services (i.e. photos, videos) and, eventually, closing down payment accounts used by the people and entities involved as payers (= site users) and as payees (= site providers).

The following example, based on the functioning of a similar coalition in the US, shall serve as the **case study basis** for our examination of legal obstacles of the APAC Coalition in this Report:

> *In a commercial context, a private person, an enterprise or an organisation (hereafter referred to as the **Offender**) produces images (photos and videos) of children aged below eighteen years, visually depicting a child engaged in real or simulated sexually explicit conduct or containing a lascivious*

*exhibition of a child's genitals or pubic area (= definition of "child pornography" in Art. 1 (b) (i) of Council Framework Decision 2004/68/JHA). The Offender then displays such images on a website (whether registered in his name or registered in a third party's name, e.g. file sharing sites, hereafter referred to as the **Offender's Site**) using the services of an Internet Service Provider and offers access to the Offender's Site to others against payment of a certain amount by either credit card, direct wire transfer or through other online payment facilitators such as PayPal.*

A national hotline, receives notice of the Offender's Site through a tip given directly to the hotline or through other channels. The national hotline forwards this information to the national law enforcement agency which then examines the image. The hotline requests that the law enforcement agency initiates a test or an undercover transaction on their behalf by using (1) a credit card, (2) a direct wire transfer or (iii) another online payment facilitator such as PayPal, in each case provided that such credit card company, bank and online payment facilitator is an APAC Coalition Member. The national hotline further informs the relevant APAC Coalition Members of its payment who then monitor on which of their merchants' accounts such payment is credited. Therewith, the APAC Coalition will have identified the merchant bank or other relevant details about the Offender (person or legal entity).

Following such identification, the national hotline shares the information regarding the identity of the Offender:

- *with the law enforcement agency and/or the public prosecutor in its jurisdiction who may subsequently launch an investigation against the Offender with the intention of enforcement of national and international criminal laws against the Offender; or*

- *if such law enforcement agency decides not to take action, with the other APAC Coalition Members requesting that all accounts and services provided by the APAC Coalition Members to the Offender shall be closed down.*

In relation to phase I of this project, based on the above case study, we have examined the following questions (and, in respect of certain jurisdictions, certain additional questions which appeared to be relevant) in relation to the legal framework of Australia, Hong Kong, Indonesia, New Zealand, the Philippines and Thailand:

(a) Are there laws specifically addressing child pornography in each of the aforementioned jurisdictions?

(b) What is the definition of illegal child pornography pursuant to each of the aforementioned jurisdictions?

(c) Are there legal obstacles to realise the APAC Coalition as described in the above case study, only with regard to the following issues:

- *the undertaking of a test or an undercover transaction by a law enforcement agency on behalf of an APAC Coalition Member to the Offender's account;*

- *the undertaking of a test or an undercover transaction by an entity other than a law enforcement agency (for example, a credit card company or an online payments facilitator) on behalf of an APAC Coalition Member to the Offender's account;*

- *the collaboration of APAC Coalition Members in relation to the test or undercover transaction;*

- *the disclosure by the APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC, the other APAC Coalition Members and the public prosecutor; and*

- *the termination by APAC Coalition Members of the provision of services to the Offender*.

In our examination, we have exclusively focused on legal obstacles originating in the following legal areas:

- data protection and privacy rules,
- banking secrecy rules,
- criminal law (except for criminal procedure law), and
- contracts law.

During phase II of this project, which will commence following the completion of phase I, we will examine the following jurisdictions: Cambodia, India, Japan, Malaysia, South Korea and Vietnam.

We have examined the role of ICMEC and the financial institutions in the project, but not the role of any other parties involved, such as e.g. Internet service providers.

We have not examined, for example, the potential legal obstacles arising from the use of the information obtained by the APAC Coalition through a public prosecutor (i.e. legal obstacles of public law enforcement).

The Report is issue-based and sets out the key legal obstacles that we anticipate will be faced by the APAC Coalition in the areas concerned. The high level summaries set out key legal issues to be considered for each jurisdiction. The executive summaries of this Report set out (i) the key legal issues and obstacles from the A&O Group's examination and (ii) a summary of proposed remedy(ies) to overcome such obstacles.

The high level summaries and executive summaries may cross-refer to the full jurisdiction reports contained in this Report. This Report should be read in its entirety and reading the high level summaries and executive summaries only are not a substitute for reading the information in the remainder of the Report.

We hope you find this Report helpful in your consideration of the realisation of the APAC Coalition's proposals.

December 2012

A&O Group

LEGAL COUNSEL

The relevant offices of the A&O Group have advised on matters governed by, and pertaining to, the laws of Thailand and Hong Kong.

The following firms (**Local Counsel**) have advised on matters governed by, and pertaining to, the laws of their respective jurisdictions:

Australia – Mallesons Stephen Jaques

Indonesia – ABNR Law

New Zealand – Simpson Grierson

The Philippines – Romulo Mabanta Buenaventura Sayoc & Delos Angeles

KEY DEFINITIONS

In this Report, in addition to those definitions which apply specifically to the relevant matter or jurisdiction being discussed, the following words and expressions have the meaning as set out hereafter. Please note that certain terms, for example "DPA" for "Data Protection Act", are used with respect to several jurisdictions and relate in each case only to the jurisdiction on which the specific chapter reflects.

Addressee	means The International Centre for Missing and Exploited Children
A&O Group	means Allen & Overy LLP and other partnerships, corporations and undertakings which are authorised to carry the name "Allen & Overy"; "**member of the A&O Group**" will have a corresponding meaning **Allen & Overy LLP** is a limited liability partnership incorporated in England and Wales with registered number OC 306763 and registered office at One Bishops Square, London E1 6AD
Chapter	means a chapter of this Report
APAC Coalition	has the meaning ascribed to it in the Introduction
APAC Coalition Members	means the members of the APAC Coalition, and **APAC Coalition Member** means each of them
ICMEC or **Client**	means the International Centre for Missing and Exploited Children
Offender	has the meaning ascribed to it in the Introduction
Offender Data	means personal data relating to the Offender
Offender's Site	has the meaning ascribed to it in the Introduction
Phase I APAC Jurisdictions	means each of Australia, Hong Kong, Indonesia, New Zealand, the Philippines and Thailand which will be considered during phase I of the APAC Coalition's proposals in connection with this Report
Phase II APAC Jurisdictions	means each of Cambodia, India, Japan, Malaysia, South Korea and Vietnam which will be considered during phase II of the APAC Coalition's proposals in connection with this Report
Report	means this report regarding the legal framework to be considered by a coalition against commercial sexual exploitation of children over the Internet, comprising a high level summary, executive summary and full jurisdiction report in respect of each Phase I APAC Jurisdiction, and subsequently in each Phase II APAC Jurisdiction.

HIGH LEVEL SUMMARIES

You will find below, listed by country, the issues identified by the relevant jurisdiction report which we consider may be of particular interest. These high level summaries do not, however, purport to be exhaustive, and reading these high level summaries should in no way be considered a substitute for reading the jurisdiction reports in their entirety. Where possible, we have given an indication of the risk associated with the relevant legal issue and our recommendation as to how the APAC Coalition could proceed with the issue.

1. AUSTRALIA[1] (to be read in conjunction with the executive summary and full jurisdiction report set out on pages 18 to 30 of this Report)

The Commonwealth of Australia is made up of six states (New South Wales, Queensland, South Australia, Tasmania, Victoria and Western Australia) and two self-governing territories (Australian Capital Territory and the Northern Territory). Most criminal offences are against state laws for acts that take place within the boundaries of the state. Federal laws generally have an international or interstate element or concern special federal issues such as telecommunications or intellectual property. All of Australia's states and territories have enacted offences that criminalise the production, dissemination and mere possession of child pornography and the federal government has enacted provisions in the Criminal Code Act of 1995 and a co-regulatory online censorship regime to regulate computer-facilitated child pornography offences. Child pornography is generally defined as a description or depiction of a child (a person under the age of 16 or 18 depending on the jurisdiction) engaged in sexual activity or in a sexual context. In some jurisdictions, there is the additional test of whether the description or depiction in question is such that a reasonable person would regard it as offensive.

While there is clearly scope for APAC Coalition Members to co-operate with Australian law enforcement agencies in the investigation of the commercial sexual exploitation of children on the Internet, there are several legal obstacles that will constrain the degree of co-operation that is possible. These are:

(a) potential criminal liability of anyone who is not authorised to conduct a controlled operation for any test or undercover purchases. If the person was charged with an offence under New South Wales, Queensland or Commonwealth law, the person may have a defence to a child pornography charge on the basis that the material concerned was used or intended to be used for a public benefit purpose. However, there is no similar defence under the laws of other Australian jurisdictions. From a practical perspective, an investigator cannot know in advance the location of the seller, so it is not possible for a private person undertaking an investigation to have any confidence that a defence would be available to them. Such purchases, therefore, should be made by police and not APAC Coalition Members and, at most, staff of APAC Coalition Members may, from time to time, be authorised to participate in such an operation where it is wholly impracticable for law enforcement agents to perform the relevant conduct;

(b) APAC Coalition Members may be exposed to civil liability under privacy legislation and defamation laws if they shared information with each other and/or ICMEC regarding holders of merchant accounts suspected of receiving funds from the sale of child pornography and/or the identity of any linked offenders - whilst it may be unlikely that a suspect would commence proceedings (and there are clearly arguments that the members could rely on to defend such a claim if it was commenced (for example, attempt to justify communication and receipt of information on the basis that the information enables them to terminate their arrangements

[1] Please note the contents of the High Level Summary, Executive Summary and Full Jurisdiction Report for Australia are based on the law as researched at 28 April 2011 and any updates to the law since have not been reflected.

with persons who are reasonably suspected of contravening the criminal law or attempt to argue they have a duty to the public to disclose the information etc.)), the possibility of civil liability being imposed cannot be discounted; and

(c) law enforcement agents may take the view that they have limited ability to share information with APAC Coalition Members regarding the results of their investigations based on information provided by APAC Coalition Members until that information enters the public domain through the laying of charges or a court hearing.

Whether the provision of services to the Offender can be terminated by the relevant APAC Coalition Member will depend on what is contained in the contract between the parties. If the contract is governed by Australian law and provided that the contract contains an express right to terminate where the service provider has a suspicion that the customer has been engaged in conduct that is or may be unlawful, there should not be any legal obstacles to the termination of the provision of services to the Offender by the relevant APAC Coalition Member. Many consumer contracts contain a right on the part of the supplier to terminate for convenience (or no particular reason). It may be possible to rely upon that right in addition to any express right to terminate where the supplier has reason to believe that the customer has been engaging in unlawful or improper conduct.

2. HONG KONG[2] (to be read in conjunction with the executive summary and full jurisdiction report set out on pages 31 to 49 of this Report)

Hong Kong became the Hong Kong Special Administrative Region of the People's Republic of China on 1 July 1997. Under Hong Kong law, the Prevention of Child Pornography Ordinance (Cap. 579) (**PCPO**), the Crimes Ordinance (Cap. 200) and the Control of Obscene and Indecent Articles Ordinance (Cap. 390) criminalise the production and possession of child pornography and other activities which relate to child pornography. Under the PCPO, "child pornography" is defined as any visual depiction which is a pornographic depiction of a person who is or is depicted as being a child (i.e. a person under the age of 16) and anything which incorporates or contains such depiction (i.e. data stored in a form which is capable of conversion into a visual depiction). "Pornographic depiction" is defined as any visual depiction that depicts a person as being engaged in explicit sexual conduct or (except for depictions for a genuine family purpose) a visual depiction that depicts, in a sexual manner or context, the genitals or anal region of a person or the breast of a female person.

Whilst there is scope for APAC Coalition Members to co-operate in the investigation of the commercial sexual exploitation of children on the Internet, the following legal constraints should be borne in mind:

(a) Undertaking test or undercover transactions

Generally, inciting or soliciting another to commit a crime is indictable at common law, notwithstanding that the incitement or solicitation has no effect. Additionally, where "agent provocateurs" are used to entice another to commit an offence, there is a risk that the "agent provocateurs" themselves will be criminally liable, although there are certain exceptions in relation to the police.

(b) Disclosure of information - duty of confidentiality and data protection

Banks have a general duty of confidentiality at common law in relation to persons with whom they have a "banker-customer" relationship. A breach of the common law duty of confidentiality is subject to civil law sanctions. However, the duty of confidentiality is subject to certain exceptions, including but not limited to: (i) where the bank is compelled to disclose such information by law (this only applies in the case of compulsion under Hong Kong law and not foreign law); (ii) where the bank has a duty to the public to disclose such information; and (iii) where disclosure is made with the customer's consent (express or implied). One particular statutory exemption is contained in the Organized and Serious Crimes Ordinance (Cap. 455) (**OSCO**), which compels a person to disclose information to "authorized officers" where such person knows or suspects that any property (including property passing through a bank account) directly or indirectly represents the proceeds of an indictable offence. An offence under the PCPO could be an indictable offence for these purposes.

Under the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**), personal data must only be used for the purposes for which it is collected, or a directly related purpose. The term "use" includes the disclosure or transfer of personal data. Therefore, personal data may not be transferred unless a data subject has consented to the disclosure or transfer of his/her personal data. However, an exemption arises where (a) the data is used for the purposes of, amongst others, (i) the prevention or detection of crime; or (ii) the apprehension, prosecution or detention of offenders; or (iii) the prevention, preclusion or remedying (including punishment)

[2] Please note the contents of the High Level Summary, Executive Summary and Full Jurisdiction Report for Hong Kong are based on the law as researched as of 14 July 2015 and any updates to the law since have not been reflected.

of unlawful or seriously improper conduct, or dishonesty or malpractice by persons (whether or not the data are held for such purposes); and (b) the general restriction on transfer without consent would likely prejudice such matters. Further, personal data would be exempt from the general data protection principles under the PDPO if use of the data is (a) required or authorised by law or by an order of a court in Hong Kong; (b) required in connection with any legal proceedings in Hong Kong; or (c) required for establishing, exercising or defending legal rights in Hong Kong.

(c) Termination of services to offenders

APAC Coalition Members may be contractually bound to provide services to offenders. However, the general terms and conditions governing the contractual relationship will normally allow APAC Coalition Members to terminate their services should it be used for an illegal purpose.

Where disclosure has been made to an "authorized officer" under OSCO, the APAC Coalition Member must ensure that it does not "tip off" the Offender or otherwise disclose any matter which is likely to prejudice the investigation.

(d) Dealing with property which represent proceeds of an indictable offence

In addition, APAC Coalition Members may be at risk of committing an offence under the OSCO if they knowingly or have reasonable grounds to believe that they are dealing with property which represents the proceeds of an indictable offence. However, it is a defence to prove that the person dealing with such property intended to disclose such matters to an "authorized officer" and there is reasonable excuse for his failure to do so.

3. INDONESIA[3] (to be read in conjunction with the executive summary and full jurisdiction report set out on pages 50 to 64 of this Report)

Law No. 44 of 2008 (the Pornography Law) prohibits the production of child pornography and other illegal acts of pornography. The term "pornography" is defined as drawings, sketches, illustrations, photos, writings, voices, sounds, moving pictures, animation, cartoons, discussions, body language, or any other forms of messages through many forms of media communication and/or public displays, consisting of indecent acts or sexual exploitation that contravenes the norms of decency in society. The term "child pornography" is defined as "all forms of pornography that involves children on or involves adults performing or acting as children". A child generally means an individual that is not over 18 years of age, unless otherwise specified.

Only Indonesian law enforcement authorities who have received prior authorisation from the head of the law enforcement agency (being police, authorised government officials and the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) or Pusat Pelaporan dan Analisis Transaksi Keuangan (Indonesian abbreviation, "PPATK")) are allowed to engage in undercover operations for undercover transactions. In addition, the PPATK is the institution authorised to regulate the anti-money laundering regime and investigate money laundering offences. Operations must be implemented in compliance with prescribed procedural requirements and must be within the scope of the authority, in particular of Law No. 8 of 1981 concerning Criminal Procedure. APAC Coalition Members should work closely together with the above mentioned authorities when conducting undercover transactions.

Indonesia does not have comprehensive legislation governing privacy and data protection, but recognises the right to protection of privacy and freedom and confidentiality in correspondence. Specifically, Law No. 11 of 2008 concerning Electronic Information and Transactions (the Electronic Information and Transaction Law) prohibits a person from distributing, transmitting or providing access to electronic information which contains contents against propriety, such as the sexual exploitation of children. However, the Law poses an obstacle to the disclosure of the identity of the Offender by APAC Coalition Members to ICMEC or other Coalition Members, as it stipulates that the use of any information through electronic media that involves personal data must be made with the consent of the person concerned unless provided by a legal stipulation or grounds for disclosure.

The current banking secrecy legal framework in Indonesia requires banks or their affiliates to maintain the confidentiality of any information relating to its savings/depositor customers. The confidentiality obligation does not apply to other customers of the bank. Exceptions to the confidentiality obligation include disclosures made for tax purposes, debt settlement of Bank receivables transferred to the Receivables Agency and State Auction/Committee for the State Receivables, court proceedings in criminal and civil cases, interbank exchange of information and upon a request that is proven by a written power of attorney from the respective customer including the heirs of the deceased Depositor. However, information disclosure, under some of these exceptions, requires written authorisation or consent from the Central Bank of Indonesia. Therefore, APAC Coalition Members are encouraged to work closely with the Indonesian Central Bank, the Head of the Criminal and Civil Courts and other authorised officials in order to access and disclose information relating to the perpetrators of child pornography.

Under the Indonesian Civil Code, the procedures for contract termination depend upon the terms and conditions agreed to between the contracting parties. The Civil Code provides that the condition of termination is always assumed to apply in mutual contracts, when one of the parties defaults in

[3] Please note the contents of the High Level Summary, Executive Summary and Full Jurisdiction Report for Indonesia are based on the law as researched at 27 November 2011 and any updates to the law since have not been reflected.

performing its contractual obligation. The termination shall not occur automatically but must be done by a judicial decision. In practice, parties may waive the applicability of this provision to their contract. However, any obligations toward a third party that have arisen due to the contract must continue to be fulfilled by the parties of the contract.

4. NEW ZEALAND[4] (to be read in conjunction with the executive summary and full jurisdiction report set out on pages 65 to 110 of this Report)

Dealings in child pornography are regulated by the Films, Videos and Publications Classification Act 1993 (the "Classification Act") in New Zealand. The Classification Act contains a general ban on dealings in objectionable publications and "child pornography" is defined to mean (a) a representation, by any means, of a person who is or appears to be under 18 years of age engaged in real or simulated explicit sexual activities; or (b) a representation of the sexual parts of a person of that kind for primarily sexual purposes. However, the definition of "child pornography" is only relevant to two provisions of the Classification Act that address the extraterritorial application of the Classification Act and extradition arrangements. In order to fall within the scope of the Classification Act's general ban on dealings in objectionable publications, child pornography images or videos must constitute a "publication" that is "objectionable" within the meaning of the Classification Act. Numerous Courts in New Zealand have held that child pornography materials are objectionable publications prohibited by the Classification Act.

Under New Zealand law, there are various legal obstacles to the undertaking of a test or an undercover transaction by a law enforcement agency or an entity other than a law enforcement agency on behalf of the national hotline to the Offender's account and they include the following:

(a) it is likely that whenever a person (including a law enforcement officer) conducts a test or undercover transaction using an alleged offender's site, that person will commit a possession offence under the Classification Act and they may also commit a distribution or copying offence. However, ICMEC or its representatives would be unlikely to face Classification Act liability if the relevant entity could (i) demonstrate that it has been qualified as a person in the service of the Crown; or (ii) defend by claiming that he or she had "lawful authority or excuse" to be in possession of the objectionable publication or by demonstrating that the acts prima facie constituting distribution offences were performed for an approved purpose under the Classification Act, such as for the purpose of, or with the intention of, delivering the objectionable publication into the possession of a person lawfully entitled to have possession of it; and(b) there is a risk that by conducting an undercover transaction on the Offender's site, ICMEC or its representatives might face liability as a secondary party to the Classification Act offences committed by the Offender in supplying or distributing objectionable publications.

Generally, APAC Coalition Members must not disclose personal information, including the identity of an individual (as opposed to a corporate) account holder, financial information, and information about alleged or proven criminal offending, unless the disclosure is one of the purposes for which the information was collected or that the disclosure is permitted on the basis of one of other permitted grounds for disclosure set out in the Privacy Act 1993. It is also important for APAC Coalition Members to ensure that such personal information is accurate, complete, relevant and not misleading or else they would be exposed to defamation and/or malicious falsehood liability in the event that the disclosure or allegation made against an individual account holder is unfounded. In summary, such information privacy principles are not likely to present an insurmountable obstacle to the proposed disclosure of account holder identities, but it will be necessary for APAC Coalition Members to develop a compliance system to ensure adherence to such principles.

Whether the provision of services to the Offender can be terminated by the relevant APAC Coalition Member will depend on what is contained in the contract between the parties and the application of

[4] Please note the contents of the High Level Summary, Executive Summary and Full Jurisdiction Report for New Zealand are based on the law as researched at 7 December 2011 and any updates to the law since have not been reflected.

the Contractual Remedies Act 1979. It is preferable that each APAC Coalition Member includes an express term in its customer contracts empowering the Member to terminate services provided to a customer where the Member forms a suspicion that the customer's account has been used to receive monies for allegedly unlawful activities.

It is recommended by local counsel in New Zealand that ICMEC discusses the proposed operation of the APAC Coalition framework with law enforcement authorities prior to establishing the framework. New Zealand's Policing Act 2008 acknowledges the role of private sector bodies in assisting the Police in the performance of their roles. If ICMEC can reach an understanding with the law enforcement agencies in New Zealand that allows them to assist in the identification of offenders without the threat of direct or secondary liability, risk can be removed. Such an understanding would also remove risk of critical or adverse issues between other enforcement agencies and ICMEC or APAC Coalition Members.

5. THE PHILIPPINES[5] (to be read in conjunction with the executive summary and full jurisdiction report set out on pages 111 to 130 of this Report)

The Philippines recently enacted a comprehensive legislation on child pornography. Republic Act No. 9975 (the "Anti-Child Pornography Act of 2009") states that it is a criminal offence for any person to "(a) hire, employ, use, persuade, induce, or coerce a child to perform in the creation or production of child pornography; (b) produce, direct, manufacture, or create any form of child pornography and child pornography materials; (c) sell, offer, advertise, and promote child pornography and child pornography materials; (d) possess, download, purchase, reproduce, or make available child pornography materials with the intent of selling or distributing them; (e) publish, post, exhibit, disseminate, distribute, transmit, or broadcast child pornography and child pornography materials; (f) knowingly possess, view, download, purchase, or in any way take steps to procure, obtain, or access for personal use child pornography materials; and (g) attempt to commit child pornography by luring or grooming a child." Notably, the scope of the law would allow for individual officers of enterprises engaging in these activities to be prosecuted. In order to target the enterprises themselves, the APAC Coalition would need avenues and tools to enable them to intercept, track, or otherwise identify suspicious transactions on their systems for onward communication and liaison with local law enforcement.

While the Anti-Child Pornography Act of 2009 imposes certain duties on Internet service providers, Internet content hosts, and other merchants and establishments, including credit card companies and banks, with respect to monitoring, reporting on, and preventing access to and transmittal of child pornography or child pornography materials, current Philippine jurisprudence on secrecy of bank deposits and transactions and data protection prescribe confidentiality in all but the most limited circumstances (such exemptions are unlikely to be of use to the APAC Coalition).

The right to privacy is enshrined both in the Philippines' Bill of Rights and in the Civil Code. Further, the Philippines' Electronic Commerce Act states that any person (being an individual or an enterprise) who "obtains access to any electronic key, electronic data message, or electronic documents, book, register, correspondence, information, or other material shall not convey to or share the same with any other person".

Such restrictive laws would amount to legal obstacles for the APAC Coalition and law enforcement in the Philippines, and in particular, would prevent their ability to make undercover or test transactions.

The Philippine government recognises the problem of child abuse and exploitation in the Philippines and has shown support of the endeavours of the APAC Coalition and the NGOs working in this area. The implementing rules and regulations of the Anti-Child Pornography Act of 2009 are yet to be crafted. The challenge for lawmakers and regulators is to reconcile earnest efforts to combat these problems whilst maintaining adequate restrictions against undue intrusion, privacy protections in relation to Internet transactions, and fostering an environment that would encourage development and confidence in the local banking system.

[5] Please note the contents of the High Level Summary, Executive Summary and Full Jurisdiction Report for The Philippines are based on the law as researched at 2 December 2011 and any updates to the law since have not been reflected.

6. THAILAND[6] (to be read in conjunction with the executive summary and full jurisdiction report set out on pages 131 to 147 of this Report)

Prohibitions against the production, distribution and trade in materials of a pornographic or obscene nature are governed by the Child Protection Act, the Criminal Code and the Computer Act in Thailand. There is however no definition of "illegal child pornography" under Thai law and no differentiation between material which is "obscene" and material which is "pornographic".

Thai law does not penalise the simple possession of pornographic items by a person with no intention of engaging in commercial or public distribution or exhibition of such items. In the absence of any unlawful intention on the part of the APAC Coalition Members, and of any case law indicating to the contrary, it is unlikely that the APAC Coalition Members could be prosecuted for taking part or participating in the trade of obscene materials under the Criminal Code or in relation to any cybercriminal offences when carrying out the actions contemplated by the case-study (including assisting in the identification of the website and the purchase of pornographic material).

There is currently no privacy or data protection law in force in Thailand but the relevant authorities are in the process of preparing a Data Protection Bill with the objective of balancing privacy rights with the freedom to exploit information technology, so that the right of privacy regarding personal data is sufficiently protected from unauthorised interference, and the commercial development of information technology as a marketing tool is not unreasonably hindered. We understand the Data Protection Bill is to be included in the legislative programme for 2012, although this is obviously no guarantee that it will in fact be enacted in 2012.

It is important for banks and financial institutions to keep customer (whether individual or corporate customers) data confidential in Thailand unless any disclosure is required by law or for the purpose of a criminal investigation or court hearing or the disclosure is made to a company being in the same financial business sector. It is likely that APAC Coalition Members may rely on such exceptions when passing on customer data to law enforcement agencies or other members of the APAC Coalition that are also financial institutions. However, more stringent rules apply to other parts of the financial industry such as credit card companies and service providers who provide electronic data capture network, credit card network, other type of electronic money. The rules applicable to these businesses do not permit the disclosure of personal data to a company in the same financial business sector, although they do permit disclosure for the purposes of a criminal investigation or court hearing.

Thai law does not provide the grounds for rescission of a contract other than for circumstances where it is impossible or the failure by any party to perform within the time stipulated under the contract. However, section 150 of the Civil and Commercial Code of Thailand provides that a legal transaction having an objective which is prohibited by law or is contrary to public policy or good morals is void. Any transaction between the APAC Coalition Members and any Offender, which is entered into for the purpose of trading in illegal child pornography will therefore become void for illegality only once the APAC Coalition Member has discovered the Offender and the Offender's activities.

[6] Please note the contents of the High Level Summary, Executive Summary and Full Jurisdiction Report for Thailand are based on the law as researched at 11 January 2012 and any updates to the law since have not been reflected.

EXECUTIVE SUMMARIES AND FULL JURISDICTION REPORTS

AUSTRALIA

1. EXECUTIVE SUMMARY

While there is clearly scope for APAC Coalition Members to co-operate with Australian law enforcement agencies in the investigation of the commercial sexual exploitation of children on the Internet, there are several legal obstacles that will constrain the degree of co-operation that is possible. These are:

(a) potential criminal liability of anyone who is not authorised to conduct a controlled operation for any test or undercover purchases - in our view, such purchases should be made by police and not APAC Coalition Members and, at most, staff of APAC Coalition Members may, from time to time, be authorised to participate in such an operation where it is wholly impracticable for law enforcement agents to perform the relevant conduct;

(b) APAC Coalition Members may be exposed to civil liability under privacy legislation and defamation laws if they shared information with each other and/or ICMEC regarding holders of merchant accounts suspected of receiving funds from the sale of child pornography and/or the identity of any linked offenders - whilst it may be unlikely that a suspect would commence proceedings, and there are clearly arguments that the members could rely upon to defend such a claim if it was commenced, we cannot discount the possibility of civil liability being imposed; and

(c) law enforcement agents may take the view that they have limited ability to share information with APAC Coalition Members regarding the results of their investigations based on information provided by APAC Coalition Members until that information enters the public domain through the laying of charges or a court hearing.

2. FULL JURISDICTION REPORT

2.1 International Legal Framework

(a) Relevant international legal acts, international conventions, protocols, recommendations, mutual legal assistance treaties and/or other international law.

(i) Australia is a party to the following relevant international conventions and protocols:

- Convention on the Rights of the Child[7]. Australia signed the Convention on 22 August 1990 and ratified it on 17 December 1990;
- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography[8]. Australia signed the Convention on 18 December 2001 and ratified it on 8 January 2007;
- International Covenant on Economic, Social and Cultural Rights[9]. Australia signed the Covenant on 18 December 1972 and ratified it on 10 December 1975;

7 <http://www2.ohchr.org/english/law/crc.htm>.
8 <http://www2.ohchr.org/english/law/crc-sale.htm>.
9 <http://www2.ohchr.org/english/law/cescr.htm>.

- Convention for the Suppression of the Circulation of, and Traffic in, Obscene Publications and amended by the Protocol signed at Lake Success, New York, on 12 November 1947[10]. Australia signed the Convention on 13 November 1947;

- United Nations Convention against Transnational Organized Crime[11]. Australia signed the Convention on 13 December 2000 and ratified it on 27 May 2004;

- Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime[12]. Australia signed the Protocol on 11 December 2002 and ratified it on 14 September 2005.

(ii) Australia is a party to mutual legal assistance treaties in criminal matters with the following countries:

- the Argentine Republic;
- the Republic of Austria;
- Canada;
- People's Republic of China;
- the Republic of Ecuador;
- Finland;
- French Republic;
- Greece;
- Hong Kong;
- Republic of Hungary;
- Republic of Indonesia;
- Israel;
- Italy;
- Korea;
- Luxembourg;
- Malaysia;
- United Mexican States;
- Monaco;

10 <http://untreaty.un.org/unts/1_60000/2/5/00002248.pdf>.

11 <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TO Cebook-e.pdf>.

12 Refer to footnote 4, page 41.

- The Netherlands;
- the Philippines;
- Portugal;
- Spain;
- Sweden;
- Switzerland;
- United Kingdom; and
- United States of America.

(b) Relevance of the framework.

(i) **International conventions**

For an international convention to which Australia is a party to have any domestic effect, it must have been implemented into Australian law through legislation. If the convention has not been implemented into Australian law, it does not create any individual rights and obligations. However, it may be used as an interpretative tool by judges where there is ambiguity in a statute to resolve the ambiguity (*Minister for Immigration & Ethnic Affairs v Teoh*[13]). To the extent that the international conventions referred to in section 2.1(a)(i) above have been implemented into domestic legislation and such legislation is relevant to the scenario under consideration, this is discussed further in section 2.2 below.

(ii) **Mutual legal assistance treaties**

Mutual legal assistance treaties are not directly relevant to the scenario under consideration. Mutual assistance requests are made by the Australian Government at the request of an Australian law enforcement agency, a court or in some circumstances a defendant in a criminal matter. Members of the Australian public are not able to make a mutual assistance request. Mutual legal assistance treaties may be relevant to the scenario under consideration to the extent that an Offender is investigated in Australia and the Offender's bank account records are sought from financial institutions in a foreign country to assist with the investigation and possible prosecution of the person.

2.2 Questions and Answers relevant to the APAC Coalition

(a) Are there laws specifically addressing child pornography in Australia?

Yes. Australia has both state and federal legislation addressing child pornography. The state and territory legislation deals with general child pornography offences, which would apply to both online and offline offences. The federal legislation deals specifically with the use of the Internet to access, transmit and make available child pornography, as well as the possession or production of such material with intent to place it on the Internet.

[13] (1995) 183 CLR 273.

(i) General child pornography offences

State and territory legislation

All of Australia's states[14] and territories[15] have enacted offences that criminalise the production, dissemination and mere possession of child pornography. Typically, it is also an offence to involve a child or someone who appears to be a child in the production of child pornography[16]. In order for the offences to apply, there must be (either) conduct within the relevant jurisdiction by the accused (or, in case of some jurisdictions, impact on persons (natural or legal) within the jurisdiction). Refer to section 2.2(b) below for the general definition of child pornography in state and territory legislation. Corporate liability for general child pornography offences is specifically addressed in some states and territories, and the associated fines are high, extending up to AUD$1.1 million (approximately USD$845,500); in the Northern Territory, directors and high ranking management staff are liable to be individually prosecuted for child pornography offences that their body corporate is guilty of. Individual offenders can be liable to imprisonment for a term of up to 21 years depending on which jurisdiction's laws apply, although a maximum of 10 years imprisonment for a first offence is the norm.

(ii) Computer-facilitated child pornography offences

Federal legislation

Sections 474.19 and 474.20 of the Criminal Code Act 1995 (Cwlth)[17] make it an offence, punishable by 10 years' imprisonment, to:

- intentionally use a carriage service (i.e. use the Internet or a mobile phone network) to access, transmit, publish, make available or otherwise distribute child pornography material; and

- possess, control, produce, supply or obtain child pornography material with the intent that it be disseminated using a carriage service in contravention of the Criminal Code.

---

14 See: section 91H(2) of the Crimes Act 1900 (NSW) <http://www.legislation.nsw.gov.au/scanview/inforce/s/1/?TITLE=%22Crimes%20Act%201900% 20No%2040%22&nohits=y>, sections 228B, 228C and 228D of the Criminal Code Act 1899 (Qld) <http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf>, sections 63 and 63A of the Criminal Law Consolidation Act 1935 (SA) <http://www.legislation.sa.gov.au/LZ/C/A/CRIMINAL%20LAW%20CONSOLIDATION%20ACT% 201935.aspx>, sections 130A, 130B and 130C of the Criminal Code Act 1924 (TAS) <http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_id=69%2B%2B1924%2BAT%40E N%2B20090703120000;histon=;prompt=;rec=;term=>, sections 68 and 70 of the Crimes Act 1958 (VIC) <http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubLawToday.nsf/95c43dd4eac7 1a68ca256dde00056e7b/c2f388e1ac022b69ca2575a8001829b3!OpenDocument> and section 60 of the Classification (Publications, Films and Computer Games) Enforcement Act 1996 (WA) <http://www.slp.wa.gov.au/legislation/statutes.nsf/main_mrtitle_151_homepage.html>.

15 See: section 65 of the Crimes Act 1900 (ACT) <http://www.legislation.act.gov.au/a/1900- 40/default.asp> and section 125B of the Criminal Code Act 1983 (NT)<http://notes.nt.gov.au/dcm/legislat/legislat.nsf/d989974724db65b1482561cf0017cbd2/584 c84aee71d734a692575e50082aa6d?OpenDocument>

16 See: section 64 of the Crimes Act 1900 (ACT), section 125E of the Criminal Code Act 1983 (NT), sections 91G(1) and 91G(2) of the Crimes Act 1900 (NSW), section 228A of the Criminal Code Act 1899 (Qld), section 63B of the Criminal Law Consolidation Act 1935 (SA), section 130 of the Criminal Code Act 1924 (TAS), section 69 of the Crimes Act 1958 (VIC) and sections 320(6), 321(6) and 322(6) of the Criminal Code Act Compilation Act 1913 (WA).

17 See: <http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/64443320A8302A33CA2 575F50082CEE7?OpenDocument>.

Section 15.1 of the Criminal Code applies to these offences[18], meaning that it is possible for an offence to occur even where the conduct occurs wholly outside of Australia provided that:

(A) a result of the conduct occurs wholly or partly in Australia; or

(B) the accused is an Australian citizen or a body corporate incorporated under the law of an Australia jurisdiction.

To criminalise dealings in child pornography material by Australians living overseas, the *Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010* [19] was passed by Federal Parliament in March 2010 and took effect on 15 April 2010. This legislation inserted new offences into the Criminal Code Act for dealings in child pornography material overseas. Offenders who are found to be possessing, controlling, producing, distributing, or obtaining such material outside Australia will be subject to maximum penalties of 15 years imprisonment.

Refer to section 2.2(b) below for the definition of child pornography in the federal legislation.

The introduction of these computer-facilitated child pornography offences was coupled with the imposition of reporting obligations on Australian Internet service providers (ISPs) and Internet content hosts (ICHs).[20] These entities must report to the Australian Federal Police material that can be accessed via their services, and which they reasonably believe to be child pornography material. The provision does not impose an obligation on ISPs and ICHs to proactively monitor and report offending material. Rather this provision is intended to ensure that where complaints are made to ISPs and ICHs about particular material accessed using their services, and there appears to be some basis for those complaints, that material, or the details of how to access that material, is sent to the Australian Federal Police. Failure to comply with this reporting obligation, within a reasonable time of becoming aware of the offending material's existence, is a criminal offence that can attract of a fine of up to AUD$55,000 (approximately USD$41,400). Since the enactment of this provision in 2005, we are unaware of any ISP or ICH having been fined under this provision.

(iii) **Grooming offences**

Sections 474.26 and 474.27 of the federal Criminal Code Act 1995 criminalise the use of a carriage service (which includes the Internet, instant messaging, mobile phones etc) to procure or "groom" a person under the age of 16 for sexual activity. These offences are punishable by imprisonment for 15 and 12 years respectively.

18 s 475.2 Criminal Code Act.

19 <http://www.comlaw.gov.au/Details/C2010A00042>

20 See section 474.25 of the Criminal Code Act 1995 (Cwlth).

Similar offences have been enacted in the Australian Capital Territory[21], New South Wales[22], Queensland[23], Tasmania[24], South Australia[25] and Western Australia.[26] These offences attract terms of imprisonment of between 5 and 21 years.

(iv) Cooperative statutory classification scheme

In addition to the general and computer-facilitated child pornography offences discussed above, there is a cooperative statutory classification scheme in Australia that prohibits dealing in offensive and objectionable material, including child pornography. This scheme comprises central federal legislation - *the Classification (Publications, Films and Computer Games) Act 1995 (Cwlth)*[27] - which establishes the classification (ratings system) of publications, films and computer games according to legislated standards of public morality, and complementary state and territory legislation which deals with the enforcement of the national classification scheme (Classification Enforcement Acts). The state[28] and territory[29] Classification Enforcement Acts criminalise the sale, publication, display and delivery of publications, films and computer games, including those with child pornography content, with offences punishable by fines or imprisonment. The Victorian, Northern Territory and Western Australian Classification Enforcement Acts also deal expressly with the online distribution of objectionable content.[30]

(v) Online censorship regime

The federal government has developed a co-regulatory online censorship regime that builds upon the classification scheme discussed above. Previously, this online censorship regime only applied to stored Internet content. However, in July 2007, the Australian Parliament enacted substantial amendments to its earlier regime such that it now applies to both stored

---

21 Section 66(1) of the Crimes Act 1900 (ACT).

22 Section 66EB of the Crimes Act 1900 (NSW).

23 Section 218A of the Criminal Code Act 1899 (Qld).

24 Section 125D of the Criminal Code Act 1924 (Tas).

25 Section 63B(3) of the Criminal Law Consolidation Act 1935 (SA).

26 Section 204B of the Criminal Code Act Compilation Act 1913 (WA).

27 http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/2ACCFFCBA1047667CA2575DD000D67C7?OpenDocument

28 See: Classification (Publications, Films and Computer Games) Enforcement Act 1995 (NSW) <http://www.legislation.nsw.gov.au/scanview/inforce/s/1/?TITLE=%22Classification%20(Publications,%20Films%20and%20Computer%20Games)%20Enforcement%20Act%201995%20No%2063%22&nohits=y>, Classification of Computer Games and Images Act 1995 (QLD) <http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/ClassComGamA95.pdf>, Classification of Films Act 1991 (QLD) <http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/ClassFilmsA91.pdf> and Classification of Publications Act 1991 (QLD) <http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/ClassPubA91.pdf>, Classification (Publications, Films and Computer Games) Act 1995 (SA) <http://www.legislation.sa.gov.au/LZ/C/A/CLASSIFICATION%20(PUBLICATIONS%20FILMS%20AND%20COMPUTER%20GAMES)%20ACT%201995.aspx>, Classification (Publications, Films and Computer Games) Enforcement Act 1995 (TAS) <http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_id=105%2B%2B1995%2BAT@EN%2B20090722000000;histon=;prompt=;rec=-1;term=>, Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic) <http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubLawToday.nsf/95c43dd4eac71a68ca256dde00056e7b/5e3fa038ff3835a7ca25701500198f2e!OpenDocument> and Classification (Publications, Films and Computer Games) Enforcement Act 1996 (WA) <http://www.slp.wa.gov.au/legislation/statutes.nsf/main_mrtitle_151_homepage.html>.

29 See: Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (ACT) <http://www.legislation.act.gov.au/a/1995-47/default.asp> and Classification of Publications, Films and Computer Games Act (NT) <http://notes.nt.gov.au/dcm/legislat/legislat.nsf/d989974724db65b1482561cf0017cbd2/b68227540703f142692575e5007ba044?OpenDocument>.

30 See: Part 7 of the Classification of Publications, Films and Computer Games Act (NT), Part 6 of the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic) and Division 6 of the Classification (Publications, Films and Computer Games) Enforcement Act 1996 (WA).

Internet content and ephemeral Internet content, such as live streamed content. The majority of these amendments came into force on 20 January 2008.

The new regime regulates persons offering content services that host stored content, provide links to content, provide live content and provide commercial content services. In all cases, these content services must have an "Australian connection" to fall within the scope of Schedule 7 of the Broadcasting Services Act.[31] A content service will have an "Australian connection" if:

- in the case of a links service or a commercial content service, any of the content provided by the content service is hosted in Australia;
- in the case of a live content service, the live content service is provided from Australia; or
- in the case of a hosting service, the content hosted by the service is hosted in Australia.

The new regime establishes a series of removal notices that may be issued by the Australian Communications and Media Authority (ACMA, the body responsible for the regulation of broadcasting, the Internet, radio-communications and telecommunications in Australia), requiring:

- hosting service providers to take down prohibited (or potentially prohibited) content from hosting services;
- links service providers to remove links to prohibited (or potentially prohibited) content; and
- live content providers to stop providing live content services which provide prohibited (or potentially prohibited) content.

The concepts of prohibited (or potentially prohibited) content are defined by reference to the federal classification legislation.

ACMA may issue removal notices as a result of complaints made by end users or as a result of its own investigations. Removal notices must be complied with as soon as practicable and by no later than 6pm on the next business day. A failure to comply with a removal notice may result in civil or criminal penalties of up to AUD$55,000 (approximately USD$46,000) per offence.

As was previously the case, the new regime is co-regulatory - it contemplates that industry codes will be registered to regulate various parts of the content industry, including commercial content providers.

(vi) Mobile Premium Services Code

The Mobile Premium Services Code[32] was registered by the ACMA under the Telecommunications Act 1997 (Cwlth) on 14 May 2009 and took effect on 1 July 2009. The Code regulates the provision of premium (i.e. paid content) services to mobile phones via SMS, MMS or 'walled garden' mobile portals (referred to in the Code as 'proprietary network

[31] Broadcasting Services Act 1992 (Cwlth), <http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/0F73006E5F4206B5CA2 5755C00137641?OpenDocument>.

[32] http://www.commsalliance.com.au/__data/assets/pdf_file/0011/2054/C637_2009.pdf

services'); the Broadcasting Services Act continues to regulate content obtained by accessing the Internet via mobile phones. The objective of the Code is to establish appropriate community safeguards and customer service requirements for mobile premium services.

The Code sets out detailed rules for mobile premium services relating to:

- advertising a mobile premium service;
- providing information to customers about a mobile premium service;
- supplying a mobile premium service to customers; complaint handling; and
- unsubscribe and opt-out mechanisms for a mobile premium service.

(vii) **IIA Content Code of Practice**

In May 2005, the ACMA registered the IIA Content Code of Practice version 10.4[33] - which guides ISPs, ICHs, mobile carriage service providers and mobile content providers in the fulfilment of their obligations under Schedule 5 of the Broadcasting Services Act and the ACMA's then in force Mobile Premium Services Determination. Although compliance with the IIA Code is voluntary, the ACMA can direct ISPs and ICHs to do so, and compliance with the Code provides automatic compliance with Schedule 5 of the Broadcasting Services Act. In addition to addressing the practicalities of how ICHs and ISPs can comply with the Schedule 5 regime, the Code requires ISPs to (i) take reasonable steps to ensure that Internet access accounts are not provided to minors, (ii) encourage content host subscribers to label content that is inappropriate for children and inform these subscribers that they may not post illegal material on their websites, and (iii) provide information to subscribers about online safety, including information about filtering software and how this can be obtained. The Code's mobile service provisions establish an 'opt-in' regime for adults who seek access to restricted content (material that is classified as MA, MA(15+), MA15+, R or R18 in accordance with the federal classification scheme), and require mobile carriers and content providers to provide end users with information about supervising minors' access to mobile content, among other things.

(b) What is the definition of illegal child pornography pursuant to Australian law (looking at both domestic and international law)?

State and Territory legislation

In all Australian states and territories, child pornography is generally defined as a description or depiction of a child (a person under the age of 16 or 18 depending on the jurisdiction[34]) engaged in sexual activity or in a sexual context.[35] The reference to 'depicts' and 'describes' is intended to cover both visual images and textual content. In some jurisdictions, there is the additional test of whether the description or depiction in question is such that a reasonable person would regard it as offensive.[36]

---

33 http://www.acma.gov.au/webwr/aba/contentreg/codes/Internet/documents/iia_code_2005.pdf

34 'Child' is defined as a person under the age of 16 in New South Wales, South Australia, Queensland and Western Australia and a person under the age of 18 in the Australian Capital Territory, Northern Territory, Tasmania and Victoria.

35 For the specific definition of child pornography in each State and Territory, see: section 64(5) of the Crimes Act 1900 (ACT), section 125A of the Criminal Code Act 1983 (NT) (definition of 'child abuse material'), section 91H(1) of the Crimes Act 1900 (NSW), section 207A of the Criminal Code Act 1899 (Qld) (definition of 'child exploitation material'), section 62 of the Criminal Law Consolidation Act 1935 (SA), section 1A of the Criminal Code Act 1924 (TAS) (definition of 'child exploitation material'), section 67A of the Crimes Act 1958 (VIC) and section 3 of the Classification (Publications, Films and Computer Games) Enforcement Act 1996 (WA).

36 This additional test is present in the Northern Territory, New South Wales, Queensland, Tasmania and Western Australia.

Federal legislation

Section 473.1 of the Criminal Code Act 1995 (Cwlth) defines child pornography material as images that depict or describe a person under the age of 18 engaged in a sexual pose or sexual activity. 'Depictions' are intended to cover all visual images, both still and motion, including representations of children, such as cartoons or animation. 'Descriptions' are intended to cover all word-based material, such as written text, spoken words and songs.[37] Sexually motivated images of sexual organs, the anal region or the breasts of a person under the age of 18 will usually be covered. Importantly, material is only considered child pornography material if it is depicted or described in a way that a reasonable person would regard as offensive.

(c) Are there legal obstacles to the undertaking of a test or an undercover transaction by a law enforcement agency on behalf of the national hotline to the Offender's account?

In summary, the test or undercover transaction may be made, but the disclosure of the results to the national hotline is problematic.

In Australia, law enforcement agencies have the power to conduct controlled operations. Controlled operations refer to operations conducted by law enforcement agencies for the purpose of obtaining evidence of criminal activity. New South Wales, South Australia, the Australian Capital Territory, Victoria, Queensland and the Commonwealth have enacted legislation specifically addressing the authorisation of controlled operations.[38]

However, law enforcement agencies carry out the controlled operations themselves, and not on behalf of any third party. Civilians may, in unusual circumstances, be permitted to participate in a controlled operation. Typically, however, this occurs only where it is impractical for a law enforcement agent to engage in the relevant conduct.[39] For example, a registered informant was a civilian participant purportedly authorised to engage in aspects of a drug purchase in *Dowe v R* [2009] NSWCCA 23.

It would be unusual for the results of a controlled operation to be communicated to a third party such as the national hotline. Indeed, law enforcement agencies could well take the view that they are not at liberty to make such a communication because the statutes that confer power to gather evidence in this fashion impliedly require the evidence only to be used for the purposes of investigating and prosecuting suspected offences, and the disclosure of the information to a person who is not part of

---

37 Explanatory Memorandum, Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No 2) 2004 – <http://www.comlaw.gov.au/comlaw/legislation/bills1.nsf/0/CFD9EAC222182530CA257695007D61E8/$file/04149emNo2.pdf>

38 See section 15J Crimes Act 1914 (Cwlth) <http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/18204B57CF54288FCA2575CB0003AEC1>, section 9 Crimes (Controlled Operations) Act 2008 (ACT) <http://www.legislation.act.gov.au/a/2008-32/current/pdf/2008-32.pdf>, section 5 Law Enforcement (Controlled Operations) Act 1997 (NSW) <http://www.legislation.nsw.gov.au/fullhtml/inforce/act+136+1997+pt.1+0+N?>, section 4 Criminal Investigation (Covert Operations) Act 2009 (SA) <http://www.legislation.sa.gov.au/LZ/C/A/CRIMINAL%20INVESTIGATION%20(COVERT%20OPERATIONS)%20ACT%202009/CURRENT/2009.7.UN.PDF>, and section 10 Crimes (Controlled Operations) Act 2004 (Vic) <http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubStatbook.nsf/f932b66241ecf1b7ca256e92000e23be/B9AE3A04656D687FCA256E98002B8201/$FILE/04-016adoc.doc> and section 239 Police Powers and Responsibilities Act 2000 (Qld).

39 See, for example, s7(3) Law Enforcement (Controlled Operations) Act 1997 (NSW), which provides that a civilian participant "must not be authorised to participate in any aspect of a controlled operation unless the chief executive officer is satisfied that it is wholly impracticable for a law enforcement participant to participate in that aspect of the operation".

the official investigation or prosecution function would be unlawful.[40] This is an area where the national hotline would need to undertake detailed discussions with relevant law enforcement agencies at the commencement of an investigation, to understand the likely attitude of the agency concerned.

(d) Are there legal obstacles to the undertaking of a test or an undercover transaction by an entity other than a law enforcement agency (for example, a credit card company or an online payments facilitator) on behalf of the national hotline to the Offender's account?

Yes. There is a real risk that a private person undertaking a test or undercover transaction of child pornography material would be committing an offence. If the person was charged with an offence under NSW, Queensland or Commonwealth law, the person may have a defence to a child pornography charge on the basis that the material concerned was used or intended to be used for a public benefit purpose. The Queensland legislation offers some guidance as to what is meant by "public benefit". It states that an example of something made for a "public benefit" is a current affairs television program showing children being tortured during a civil war. However, there is no similar defence under the laws of other Australian jurisdictions and we are not aware of this defence having been successfully raised in the Australian courts.

From a practical perspective, an investigator cannot know in advance the location of the seller, so it is not possible for a private person undertaking an investigation to have any confidence that a defence would be available to them.

(e) Are there legal obstacles to the collaboration of APAC Coalition Members in relation to the test or the undercover transaction?

Refer to section 2.2(d) above - Coalition Members may be knowingly concerned or otherwise an accessory to an offence committed by the person who undertakes the purchase.

(f) Are there legal obstacles to the disclosure by the APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC, the other APAC Coalition Members and the public prosecutor?

There are two main legal obstacles to the disclosure by the APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC and the other APAC Coalition Members. These relate to the provisions of Australia's privacy law and defamation law.

We do not consider that there are any legal obstacles to the disclosure by the APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to the public prosecutor or to police.

---

40 See *Donnelly v Amalgamated Television Services Pty Ltd* (Supreme Court of NSW, 5 November 1998) http://www.austlii.edu.au/au/cases/nsw/NSWSC/1998/509.html for an example of this reasoning:

"If police, in exercising powers under a search warrant or of arrest, were to enter into private property and thereby obtain documents containing valuable confidential information, albeit not protected by the law concerning intellectual property, I believe they could in a proper case be restrained, at the suit of the owner of the documents, from later using that information to their own advantage, or to the disadvantage of the owner, or passing the information on to other persons for them to use in that way; and if other persons acquired such information from the police, knowing the circumstances of its acquisition by the police, then I believe those other persons could likewise be restrained. I believe the same applies to material obtained in that way which is gratuitously humiliating rather than confidential, particularly where no basis has been put forward for suggesting that the dissemination of this material is required for the legitimate publicising of the investigation, prosecution, and disposal of the matters to which the plaintiff has pleaded guilty. "

Privacy law

The first legal obstacle to the disclosure by APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC and other APAC Coalition Members are the provisions of National Privacy Principle (NPP) 2.1(f) of the *Privacy Act 1988* (Cwlth) which relate to use and disclosure of personal information by an organisation.

NPP 2.1(f) provides that an organisation must not use or disclose personal information about an individual (natural person) for a purpose other than the primary purpose of collection unless the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

'Relevant persons or authorities' to which an organisation may report unlawful activity include but are not limited to:

- 'enforcement bodies' as defined in section 6(1) of the Privacy Act;
- agencies and regulatory authorities such as Austrac and State and Territory Departments of Fair Trading and Offices of State Revenue; and
- self-regulatory authorities such as the Australian Stock Exchange, the Telecommunications Industry Ombudsman and the Banking Industry Ombudsman.

There is some risk that ICMEC or other APAC Coalition Members would not be considered 'relevant persons or authorities' for the purposes of NPP 2.1(f). However the APAC Coalition Member could disclose the identity of the holder of the merchant's account and/or the Offender to a law enforcement agency, who after investigating the matter may refer the matter to the public prosecutor.

Defamation Law

The second legal obstacle to the disclosure by the APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC and the other APAC Coalition Members is the risk that the APAC Coalition Member may be liable for an action in defamation. If the APAC Coalition Member only has a reasonable suspicion of the identity of the Offender and communicates this information to ICMEC and other APAC Coalition Members, it may be liable for an action in defamation unless it can bring itself within the defence of qualified privilege.

The publication of defamatory matter is actionable by statute in each State and Territory in Australia[41] (the cause of action arises at common law). The tort of defamation consists of three elements:

- publication of a communication to a third person. Publication may be achieved through many means including spoken or written words, gestures, exclamations or laughter, printed or electronic images, publications on the Internet, communications in person or communications by broadcast;
- the communication must identify (or be about) the plaintiff; and

[41] Civil Law (Wrongs) Act 2002 (ACT), Defamation Act 2006 (NT), Defamation Act 2005 (NSW), Defamation Act 2005 (QLD), Defamation Act 2005 (SA), Defamation Act 2005 (TAS), Defamation Act 2005 (Vic) and Defamation Act 2005 (WA).

- the communication must be defamatory. A publication is defamatory of a person if it tends, in the minds of ordinary reasonable people, to injure their reputation either by disparaging them, causing others to shun or avoid them or subjecting them to hatred, ridicule or contempt.

In all States and Territories, corporations cannot sue for defamation.[42] There are specific exceptions however, which allow not-for-profit organisations (other than a local government body or a public authority) and corporations with fewer than 10 employees that are not related to another organisation (and are not a local government body or public authority) to sue for defamation. Accordingly, corporations that carry on small businesses are entitled to sue for defamation (as are individual merchants).

The defence of qualified privilege is available for the publication of defamatory matter to a person (the "recipient") if the defendant proves that:[43]

(i) the recipient has an interest or apparent interest in having information on some subject, and

(ii) the matter is published to the recipient in the course of giving to the recipient information on that subject, and

(iii) the conduct of the defendant in publishing that matter is reasonable in the circumstances.

Whether or not the defence of qualified privilege will apply to a particular factual situation is often difficult to predict. A recent Australian case found that qualified privilege attached to communications between credit providers and a credit reporting bureau.[44] The court tested whether or not the publication was for the common convenience and welfare of society. Here, APAC Coalition Members may be able to justify the communication and receipt of the identity of the holder of the merchant's account and/or the Offender on the basis that the information enables them to terminate their arrangements with persons who are reasonably suspected of contravening the criminal law, but it is by no means certain that all Coalition Members have a sufficient interest in receiving that information to bring the defence of qualified privilege into play. ICMEC's interest in receiving the information appears to us to be less than that of the Coalition Members, as ICMEC has no commercial relationship with the account holder/Offender to terminate.

Banker's duty of secrecy

The duty of confidentiality owed by a bank to its customers (any person (natural or legal) who has an account with a bank is a customer) was recognised in *Tournier v National Provincial and Union Bank of England*.[45] It was held that it is an implied term of the contract between the bank and its customer that the bank will not disclose to third parties any information about the customer learned from the conduct of the customer's account unless:

- the bank is compelled to do so by law;

- the bank has a duty to the public to disclose the information;

---

42 s 121 of the Civil Law (Wrongs) Act 2002 (ACT), s 8 of the Defamation Act 2006 (NT), s 9 of the Defamation Act 2005 (NSW), s 9 of the Defamation Act 2005 (QLD), s 9 of the Defamation Act 2005 (SA), s 9 of the Defamation Act 2005 (TAS), s 9 of the Defamation Act 2005 (Vic) and s 9 Defamation Act 2005 (WA).

43 s 139A of the Civil Law (Wrongs) Act 2002 (ACT), s 27 of the Defamation Act 2006 (NT), s 30 of the Defamation Act 2005 (NSW), s 30 of the Defamation Act 2005 (QLD), s 28 of the Defamation Act 2005 (SA), s 30 of the Defamation Act 2005 (TAS), s 30 of the Defamation Act 2005 (Vic) and s 30 Defamation Act 2005 (WA).

44 *Dale v Veda Advantage Information Services and Solutions Limited* [2009] FCA 305 (Lindgren J)

45 [1924] 1 KB 461.

- the interests of the bank require disclosure; or
- the disclosure is made with the customer's consent (express or implied).

The Australian law on this issue is likely to be consistent with the English common law. We believe it is more likely than not that a bank would be able to rely upon the 'duty to disclose' exception, provided that the person or persons that the bank informs of the suspicion that the customer's account is being used in connection with child pornography offences has a sufficient interest in receiving that information. This raises the same issues as discussed in relation to NPP 2.1(f) above.

(g) Are there legal obstacles to the termination of the provision of services to the Offender by APAC Coalition Members?

Whether the provision of services to the Offender can be terminated by the relevant APAC Coalition Member will depend on what is contained in the contract between the parties. If the contract is governed by Australian law and provided that the contract contains an express right to terminate where the service provider has a suspicion that the customer has been engaged in conduct that is or may be unlawful, we cannot see any legal obstacles to the termination of the provision of services to the Offender by the relevant APAC Coalition Member.[46] Many consumer contracts contain a right on the part of the supplier to terminate for convenience (or no particular reason). It may be possible to rely upon that right in addition to any express right to terminate where the supplier has reason to believe that the customer has been engaging in unlawful or improper conduct.

However, it is appropriate to note that banks and ISPs are both subject to oversight by specialist industry ombudsmen, to whom complaints regarding unjustified termination of contracts may be directed.

[46] Drafting of these clauses varies - some contracts require reasonable suspicion, others give more discretion to the service provider.

HONG KONG

1. EXECUTIVE SUMMARY

No.	Issue	Recommendation
1.	**Data protection** The Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) imposes requirements on data users with respect to the collection, holding or processing of personal data. Under the PDPO, "data user" is defined as "a person, who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data". Under section 2 of the Interpretation and General Clauses Ordinance (Cap. 1), a "person" includes "any public body and any body of persons, corporate or unincorporated". Therefore, any APAC Coalition Members that are data users will be subject to the PDPO. The PDPO provides for circumstances in which it is permissible for the data user to disclose personal data to third parties.	We recommend that the data protection notices of each APAC Coalition Member that is a data user be amended under which all data subjects consent to the transfer and/or disclosure of personal data for the purpose of detecting crime. Where an APAC Coalition Member that is a data user wishes to disclose information relating to an Offender, those members should document the decision-making process and the reasons for the disclosure (including, if applicable, those sections of the PDPO permitting disclosure upon which reliance is based). In the event that the Offender is a natural person, we recommend cooperation with the Office of the Privacy Commissioner for Personal Data prior to the disclosure of personal data.
2.	**Banking secrecy rules** There is a general duty imposed on banks and financial institutions to keep the affairs of their customers confidential.	Banks are permitted to disclose information about the affairs of their customers to third parties in certain circumstances. There are also certain statutory duties obliging banks to disclose certain confidential account information (e.g., a bank is obliged to disclosure certain information to an authorized officer as defined by section 2 of the Organised and Serious Crime Ordinance (OSCO) where it knows or suspects that any property passing through a bank account directly or indirectly represents the proceeds of an indictable offence).

No.	Issue	Recommendation
3.	**Criminal law: child pornography** In certain circumstances, the actions of a Hong Kong APAC Coalition Member may constitute a criminal offence related to child pornography in Hong Kong. For example, the Hong Kong APAC Coalition Member could be charged with an offence under section 3 of the Prevention of Child Pornography Ordinance (Cap. 579) (PCPO) if it deliberately downloads images of child pornography from the Internet, or is found in possession of child pornography.	Before taking any action that may fall within the definition of one of the offences related to child pornography, a Hong Kong APAC Coalition Member should ensure that the action it proposes to take falls within one of the defences to such a crime. It is a defence to a charge under section 3 of the PCPO if the person charged with the offence can prove that the commission of the offence (e.g. downloading images of child pornography from the Internet) was a necessary act for the public good and the public good only.

2. FULL JURISDICTION REPORT

2.1 International Legal Framework

(a) Analysed treaties, conventions and protocols

The following treaties, conventions and protocols have been analysed and/or considered in this part of the report:

- United Nations: Convention on the Rights of the Child[47] (in force in Hong Kong);
- United Nations: Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography[48] (though the People's Republic of China (**PRC**) is a signatory, this is not in force in Hong Kong);
- United Nations Convention against Transnational Organized Crime[49] (in force in Hong Kong);
- Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime[50] (though the PRC is a signatory, this is not in force in Hong Kong);
- International Convention for the Suppression of the Traffic in Women and Children[51] (in force in Hong Kong);

47 United Nations Convention on the Rights of the Child: http://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf

48 Optional Protocol to the UN Convention on the Rights of the Child on the sale of children, child prostitutions and child pornography: http://www.ohchr.org/Documents/ProfessionalInterest/crc-sale.pdf

49 United Nations Convention against Transnational Organized Crime: http://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

50 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime: http://www.osce.org/odihr/19223?download=true

51 International Convention for the Suppression of the Traffic in Women and Children: http://www.austlii.edu.au/au/other/dfat/treaties/1922/10.html

- Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour[52] (in force in Hong Kong);
- International labour conventions (in force in Hong Kong); and
- The 40 Recommendations[53] and 9 Special Recommendations[54] of the Financial Action Task Force (applied in Hong Kong).

(b) **Relevance of the Framework**

The legal system in Hong Kong

Hong Kong became the Hong Kong Special Administrative Region of the People's Republic of China (**PRC**) on 1 July 1997. According to the terms of the Sino-British Joint Declaration, signed between the PRC and the United Kingdom on 19 December 1984 (**Joint Declaration**), the way of life in Hong Kong is to remain unchanged for fifty years after 1 July 1997. Hong Kong will continue to enjoy a high degree of autonomy, except in foreign and defence affairs.

The Joint Declaration provides the constitutional framework for the legal system in Hong Kong. The Basic Law[55] was enacted by the National People's Congress of the PRC under Article 31 of the Chinese Constitution[56]. The Basic Law came into effect on 1 July 1997 and is Hong Kong's first detailed written constitution.

Both the Joint Declaration and the Basic Law guarantee the continuance of the legal system that was in place before China resumed the exercise of sovereignty over Hong Kong on 1 July 1997. Under the "one country, two systems" principle, Hong Kong's legal system remains rooted in common law and differs from that of the PRC.

The human rights framework in Hong Kong

The Joint Declaration provides that the provisions of the International Covenant on Civil and Political Rights (**ICCPR**)[57] and the International Covenant on Economic, Social and Cultural Rights[58] as applied in Hong Kong, shall remain in force. This provision is reflected under Article 39 of the Basic Law. In addition, the Hong Kong Bill of Rights Ordinance (Cap. 383) (**BORO**)[59], was enacted in 1991 to give effect to the provisions of the ICCPR and remains in force. All legislation, whether enacted before or after the BORO, must conform with the provisions of the BORO. With effect from 1 July 2007, the Constitutional and Mainland Affairs Bureau assumed responsibility for matters relating to human rights in Hong Kong.

---

52 Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour: http://www.ilo.org/ilolex/cgi-lex/convde.pl?C182

53 The 40 Recommendations of the Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

54 The 9 Special Recommendations of the Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

55 The Basic Law of the Hong Kong Special Administrative Region of China: http://www.basiclaw.gov.hk/en/basiclawtext/index.html

56 Constitution of the People's Republic of China (adopted on 4 December, 1982): http://english.peopledaily.com.cn/constitution/constitution.html

57 International Covenant on Civil and Political Rights: http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

58 International Covenant on Economic, Social and Cultural Rights: http://www.ohchr.org/Documents/ProfessionalInterest/cescr.pdf

59 Hong Kong Bill of Rights Ordinance (Cap. 383): To access Hong Kong ordinances, visit the Department of Justice, Bilingual Laws Information System online: http://www.legislation.gov.hk/eng/index.htm

International treaties and conventions

The majority of international treaties that Hong Kong has entered into were entered into prior to 1 July 1997 (i.e. before the reunification of Hong Kong to the PRC). These treaties continue to apply from 1 July 1997 onwards.[60]

From 1 July 1997 onwards, under Article 13 of the Basic Law, the Central People's Government of the PRC is responsible for the foreign affairs relating to Hong Kong. Under Article 153 of the Basic Law, the views of the Hong Kong Government have to be sought before international agreements to which the PRC is a party, are extended to Hong Kong.

As a result of the above, some international treaties are applicable to Hong Kong but not the PRC, some international treaties are applicable to the PRC but not Hong Kong, and some treaties are applicable to both the PRC and Hong Kong.

The following treaties, conventions and protocols, which form part of Hong Kong's international legal framework, are most relevant to this Report:

(i) *Prevention of child pornography*

At the international level, the two key legal instruments which relate to the prevention of child pornography are the United Nations Convention on the Rights of the Child of 20 November 1989 (**CRC**) and the United Nations Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography of 25 May 2000 (**UN Optional Protocol to the CRC**).

The CRC was extended to Hong Kong by the United Kingdom in 1994, three years after the United Kingdom became a signatory to the CRC and five years after the PRC became a signatory to the CRC. Article 34 of the CRC provides that state parties undertake to protect the child from all forms of sexual exploitation and abuse. Measures should be taken to prevent the exploitative use of children in pornographic performance and materials. Towards this, Hong Kong passed the Prevention of Child Pornography Ordinance (Cap. 579) (**PCPO**), which came into effect on 19 December 2003. Details of the PCPO are set out below.

As of 14 July 2015, the UN Optional Protocol to the CRC is not in force in Hong Kong. In September 2005, at a hearing of the United Nations Committee on the Rights of the Child, the Hong Kong Government stated that Hong Kong has very strong protection for children. Both the sale of children and child prostitution are illegal in Hong Kong. In addition, the Hong Kong Government stated that Hong Kong has "every intention" to have the UN Optional Protocol to the CRC applied in Hong Kong. However, Hong Kong needs to first bring existing laws in line with the provisions of the UN Optional Protocol to the CRC. The Hong Kong Government stated that it expects to see Hong Kong's adoption of the UN Optional Protocol to the CRC "soon" (though this statement was made in 2005).

(ii) *International labour conventions*

Under Article 39 of the Basic Law, "the provisions of the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and international labour conventions as applied to Hong Kong shall remain in force and shall be implemented through the laws of the Hong Kong Special Administrative Region."

[60] See further the note from the PRC to the United Nations Secretary-General dated 20 June 1997 addressing this issue.

The International Labour Organization (**ILO**), which is a specialized agency of the United Nations, adopted the Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (**Convention Prohibiting Child Labour**) in June 1999. The Convention Prohibiting Child Labour came into force in Hong Kong on 8 August 2003.

The Convention Prohibiting Child Labour calls for, amongst others, immediate and effective measures to eliminate the "worst forms of child labour". Under Article 3 of the Convention Prohibiting Child Labour, the term "worst forms of child labour" includes, amongst others, "all forms of slavery or practices similar to slavery, such as the sale and trafficking of children, debt bondage and serfdom and forced or compulsory labour, including forced or compulsory recruitment of children for use in armed conflict". Also included under the definition of "worst forms of child labour" is "the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances".

(iii) *Child trafficking*

Hong Kong acceded to the International Convention for the Suppression of the Traffic in Women and Children (**Convention Prohibiting Trafficking**) on 18 September 1922, under which parties agree to prosecute persons who are engaged in the traffic of children. The Convention Prohibiting Trafficking remains in force in Hong Kong.

In addition, child trafficking is one of the "worst forms of child labour" and is prohibited under the Convention Prohibiting Child Labour (see (b) above).

(iv) *Money laundering*

The Financial Action Task Force (**FATF**) is an inter-governmental body established in 1989 whose purpose is to develop and promote national and international policies to combat money laundering and terrorist financing. Hong Kong joined the FATF in 1991.

The FATF issued 40 Recommendations and 9 Special Recommendations (the **Recommendations**), which provide counter-measures against money laundering. Though the Recommendations are not a binding international agreement, as a member of the FATF, Hong Kong is obliged to and has largely adopted the Recommendations. The Hong Kong Monetary Authority has issued the Guideline on Prevention of Money Laundering, which has been amended by various related supplements. The amended Guideline on Prevention of Money Laundering largely incorporates the Recommendations and applies to all authorized institutions. Of relevance to child pornography, under the Recommendations, each member should include a range of offences within each of the "designated categories of offences". "Designated categories of offences", includes, amongst others, trafficking in human beings, as well as sexual exploitation, including the sexual exploitation of children.

In addition to the FATF, Hong Kong is also a member of the Asia/Pacific Group on Money Laundering (**APG**). The APG is closely affiliated with the FATF. Members of the APG are committed to implementing the Recommendations.

2.2 Questions and Answers relevant to the APAC Coalition

(a) Are there laws specifically addressing child pornography in Hong Kong?

The Prevention of Child Pornography Ordinance (Cap. 579) (**PCPO**) was enacted in July 2003 in compliance with the CRC and the Convention Prohibiting Child Labour. The PCPO, which came into

operation in December 2003, enabled a wider scope of enforcement against child sex-related activities. The PCPO prohibits, amongst others, the printing, making, production, reproduction, copying, publishing, import, export, possession and advertising of child pornography, as well as the procurement of children for making pornography.

In addition to the PCPO, the Crimes Ordinance (Cap. 200) (**CO**) and the Control of Obscene and Indecent Articles Ordinance (Cap. 390) (**COIAO**) criminalise various activities relating to child pornography.

For details on the criminalisation of child pornography, data protection law, banking secrecy rules, money laundering and general contract law in Hong Kong, please refer to the analysis on domestic law below.

(b) What is the definition of illegal child pornography pursuant to domestic or International law?

Domestic law

Child pornography is defined in the PCPO. Under Section 2 of the PCPO,

“child pornography” means:

(i) a photograph, film, computer-generated image or other visual depiction that is a pornographic depiction of a person who is or is depicted as being a child, whether it is made or generated by electronic or any other means, whether or not it is a depiction of a real person and whether or not it has been modified; or

(ii) anything that incorporates a photograph, film, image or depiction referred to in paragraph (i),

and includes data stored in a form that is capable of conversion into a photograph, film, image or depiction referred to in paragraph (i) and anything containing such data;

"child" means a person under the age of sixteen; and

"pornographic depiction" means:

(i) a visual depiction that depicts a person as being engaged in explicit sexual conduct, whether or not the person is in fact engaged in such conduct; or

(ii) a visual depiction that depicts in a sexual manner or context, the genitals or anal region of a person or the breast of a female person,

but, for the avoidance of doubt, a depiction for a genuine family purpose does not, merely because it depicts any part of the body referred to in paragraph (ii), fall within that paragraph.

International law

The United Nations defines "child" under Article 1 of the CRC as "every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier." According to Article 2(c) of the UN Optional Protocol to the CRC (which is not in force in Hong Kong), child pornography is defined as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes."

(c) Are there legal obstacles to the undertaking of a test or an undercover transaction by a law enforcement agency on behalf of the national hotline to the Offender's account?

Generally, inciting or soliciting another to commit a crime is indictable at common law, notwithstanding that the incitement or solicitation has no effect.[61]

In addition, an "agent provocateur" is defined as a person that entices another to commit an express breach of the law which he would not otherwise have committed and then proceeds or informs against him in respect of such offence.[62] It is not a valid defence to put that the defendant would not have committed the offence if it were not for the agent provocateur.[63] However, in exceptional cases, a court may stay such proceedings.[64] Agent provocateurs may themselves be criminally liable.

It is unlawful for police to incite, counsel or procure the commission of an offence, which would not otherwise take place. However, for the purposes of apprehending offenders, police may take part in, or encourage an offence which is already "laid on". Police must "do no more than might be expected from others in the circumstances".[65]

(d) Are there legal obstacles to the undertaking of a test or an undercover transaction by an entity other than a law enforcement agency on behalf of the national hotline to the Offender's account?

Please see above.

(e) Are there legal obstacles to the collaboration of APAC Coalition Members in relation to the test or the undercover payment?

Please see above.

(f) Are there legal obstacles to the disclosure by APAC Coalition Members of the identity of the merchant's account and/or the Offender to ICMEC, the other APAC Coalition Members and the public prosecutor?

Banks have a general duty of confidentiality at common law in relation to persons with whom they have a "banker-customer" relationship. A breach of the common law duty of confidentiality is subject to civil law sanctions. However, the duty of confidentiality is subject to certain exceptions, including but not limited to: (i) where the bank is compelled to disclose such information by law; (ii) where the bank has a duty to the public to disclose such information; or (iii) where the interests of the bank require such disclosure. One major statutory exemption is contained in the Organized and Serious Crimes Ordinance (Cap. 455) (**OSCO**), which compels a bank or any person to disclose information to "authorized officers" (even if this means disclosing confidential account information) where such bank or person knows or suspects that any property (including property passing through a bank account) directly or indirectly represents the proceeds of an indictable offence. An offence under the PCPO could be an indictable offence for these purposes.

Under data protection principle 3 of the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**), personal data must only be used for the purposes for which it is collected, or a directly related purpose.

---

61 See *DPP v Armstrong (Andrew)* [2000] Crim LR 379, DC.

62 See *R v Sang* [1980] AC 402 and *R v Cheung Chung Ching* (unrep, Cr App 546/1984).

63 *Ibid*.

64 *R v Looseley, Att-Gen's Reference (No 3 of 2000)* [2002] Crim L R 301, HL, *HKSAR v Wong Kwok Hung* [2007] 2 HKLRD 621, CA, and *HKSAR v Fung Hin Wah Edward* [2012] 1 HKLRD 374, CA.

65 See *R v Birtles* 53 Cr App R 469, CA, *R v McCann* 56 Cr App R 359, CA, *R v Clarke (DG)* 80 CR App R 344, CA, and *R v Looseley Att-Gen's Reference (No 3 of 2000)* [2002] Crim L R 301, HL.

The term "use" includes the disclosure or transfer of personal data.[66] Therefore, personal data may not be transferred unless a data subject has consented to the disclosure or transfer of his/her personal data. However, under section 58 of the PDPO, an exemption arises where (a) the data is used for the purposes of, amongst others, (i) the prevention or detection of crime; or (ii) the apprehension, prosecution or detention of offenders; or (iii) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice by persons (whether or not the data are held for such purposes); and (b) the application of data protection principle 3 in relation to such use would likely prejudice such matters. Under the Code of Banking Practice, banks must observe the provisions contained in the PDPO.

(g) Are there legal obstacles to the termination of the provision of services to the Offender by APAC Coalition Members?

While APAC Coalition Members may be contractually bound to provide their services, the general terms and conditions governing the contractual relationship will normally allow APAC Coalition Members to terminate their services should it be used for an illegal purpose. Under Hong Kong law, any agreement to commit a crime or an agreement which is otherwise contrary to public policy will not be enforceable.

In addition, APAC Coalition Members may be at risk of committing an offence under the OSCO if they knowingly deal with property which represents the proceeds of any indictable offence.[67] However, it is a defence to prove that the person dealing with such property intended to disclose such knowledge, suspicion or matter to an "authorized officer", and there is reasonable excuse for his failure to make disclosure.[68]

2.3 Analysis of Relevant International Cases

International cases in relation to child pornography are less relevant in Hong Kong as there is legislation in Hong Kong which criminalises child pornography and various activities relating to child pornography.

2.4 Domestic Legal Framework

(a) Definition of illegal child pornography

Scope of the definition of child pornography

Section 2 of the Prevention of Child Pornography Ordinance (Cap. 579) (the **PCPO**), defines "child pornography" as:

(i) a photograph, film, computer-generated image or other visual depiction that is a pornographic depiction of a person who is or is depicted as being a child, whether it is made or generated by electronic or any other means, whether or not it is a depiction of a real person and whether or not it has been modified; or

(ii) anything that incorporates a photograph, film, image or depiction referred to in paragraph (i),

and includes data stored in a form that is capable of conversion into a photograph, film, image or depiction referred to in paragraph (i) and anything containing such data.

---

66 PDPO, section 2(1) (definition of '*use*').

67 Section 25(1) of OSCO.

68 Section 25(2) of OSCO.

A "child" is defined as any person under the age of 16.

A "pornographic depiction"[69] is defined as:

(i) a visual depiction that depicts a person as being engaged in explicit sexual conduct, whether or not the person is in fact engaged in such conduct; or

(ii) a visual depiction that depicts, in a sexual manner or context, the genitals or anal region of a person or the breast of a female person,

but, for the avoidance of doubt, a depiction for a genuine family purpose does not, merely because it depicts any part of the body referred to in paragraph (ii), fall within that paragraph.

It has been observed by one commentator[70] that the essence of the definition of child pornography as adopted by the PCPO has been influenced by definitions provided by the UN Optional Protocol to the CRC. According to the same commentator, the key word in the various definitions of "child pornography" is the word "sexual". The definition aims to distinguish sexual activities from innocent activities, such as "children being videoed or photographed naked while swimming in a pool."[71] Notably, the PCPO does not consider the "depiction for genuine family purposes" as being within the definition of a "pornographic depiction". The PCPO however, does not provide a definition of "genuine family purpose".

The PCPO definition of child pornography is broad. Notably, it also criminalises the computer-facilitated publication of child pornography by virtue of the definition of child pornography (which includes data stored in a form that is capable of conversion into a visual depiction) and the scope of the definition of publication (which includes making a message or data available by means of an electronic transmission). Computer-facilitated possession of child pornography is also criminalised by the PCPO. Offenders face the same penalties for computer facilitated dealings in child pornography as they do for offline child pornography offences.

Legislation and regulations

There are three ordinances in Hong Kong which criminalise various activities relating to child pornography:

(i) PCPO

The PCPO came into effect on 19 December 2003, and is the main piece of legislation governing child pornography-related offences in Hong Kong. The PCPO implements Article 34 of the CRC which provides that state parties undertake to protect the child from all forms of sexual exploitation and abuse.

(A) Offences under the PCPO

I. Production, distribution, publication and promotion of child pornography

Section 3(1) of the PCPO criminalises the printing, creation, production, reproduction, copying, import and export of all child pornographic materials

---

69 An objective test should be used when considering whether the materials concerned are pornographic depiction: *Secretary for Justice v Easy Finder Ltd* [2008] 4 HKLRD 555.

70 Rebecca Ong, *Child Pornography and the Internet in Hong Kong,* Rutgers Computer & Technology Law Journal, 22 March 2005, p.90.

71 *Ibid*, p.91.

whether created electronically or in its traditional form. This includes the downloading of pornographic images from the Internet. Section 3(2) of the PCPO criminalises the publication of child pornography.[72] Publication of advertisements likely to be understood as advertising child pornography is criminalised in section 3(4) of the PCPO. The maximum liability for these offences on conviction on indictment is a fine of HK$2,000,000 and imprisonment for 8 years.

II. Possession of child pornography

Section 3(3) of the PCPO criminalises the possession of child pornography. The maximum liability on conviction on indictment is a fine of HK$1,000,000 and imprisonment for 5 years.

(B) Defences under the PCPO

Section 4 of the PCPO creates a number of defences to the section 3 offences. They broadly fall into the following categories:

I. artistic merit;[73]

II. genuine educational, scientific or medical purpose;[74]

III. act was for the public good and the public good only;[75]

IV. reasonable belief that person depicted was not a child and was not depicted as a child;[76] and

V. the accused has not seen the child pornography and did not know or suspect it to be child pornography;[77] alternatively the accused did not solicit the child pornography and endeavoured to destroy it within a reasonable time.[78]

Generally, the burden is on the defendant to establish the facts required to make out his defence on the balance of probabilities.[79] However, defendants charged with possession of child pornography under section 3(3) of the PCPO are presumed to have discharged this burden in respect of certain defences as long as "sufficient evidence is adduced to raise an issue with respect to the fact", and the prosecution fails to prove the contrary beyond reasonable doubt.[80]

---

72 "Publishes" is defined broadly under Section 2(2) of the PCPO to include all means of showing child pornography to another person, with or without reward.

73 Section 4(1)(a) PCPO.

74 Section 4(2)(a) and Section 4(3)(a) of PCPO.

75 Section 4(2)(b) and Section 4(3)(b) of PCPO.

76 Section 4(2)(d) of PCPO.

77 Section 4(2)(c) and Section 4(3)(c) of PCPO.

78 Section 4(3)(d) of PCPO.

79 Section 4(4) PCPO.

80 Under section 4(5) of the PCPO, defendants are presumed to have established defences under sections 4(3)(c), 4(3)(d) and 4(3)(e) if there is sufficient evidence to raise an issue, and the prosecution fails to prove the contrary beyond reasonable doubt. The relevant defences are:

Section 4(3)(c): the defendant had not seen the child pornography and did not know nor suspect that it was child pornography;

Section 4(3)(d): the defendant had not asked for any child pornography and endeavoured to destroy it within a reasonable time after obtaining possession of it;

Section 4(3)(e): the defendant believed that the person depicted was not a child at the time of the depiction, and was not depicted as a child.

(C) Prosecutions under the PCPO

There have been a fair number of prosecutions and convictions under the PCPO since it came into effect. In 2007 there were 10 prosecutions including 7 convictions under the PCPO, while in 2008 there were 24 prosecutions resulting in 21 convictions. Almost all reported cases on possession of child pornography involved pornographic material downloaded from the Internet and stored in a digital format.

Earlier convictions for possession of child pornography attracted relatively light sentences consisting mostly of suspended sentences and community service orders, which has attracted some criticism as not being reflective of the seriousness of the offence. However, the Court of Appeal ruled in 2008 that the prevalent sentencing practice is inadequate and that this offence "should generally attract an immediate custodial sentence unless special circumstances exist"[81], and laid down guidelines for sentencing to address the disparity in penalties issued and to ensure sentences reflected the gravity of the offence.[82] Since then there have been higher sentences imposed.[83]

(ii) The Control of Obscene and Indecent Articles Ordinance (Cap. 390) (the **COIAO**)

The COIAO prohibits the publication of obscene material and restricts the availability of indecent material. Section 2 of the COIAO defines obscene material as that which is unsuitable for publication to anyone for reasons including violence, depravity and repulsiveness. Indecent material is defined as that which is unsuitable for publishing to juveniles (persons under the age of 18) for the same reasons. All child pornography is likely to fall into either one or both of the two categories.

The COIAO criminalises the publishing of indecent material to a juvenile, which carries a maximum penalty of HK$800,000 and 1-year imprisonment.[84] Section 21 of the COIAO makes it an offence to publish obscene material or to possess or import obscene material for the purpose of publishing. The maximum penalty is HK$1,000,000 and 3 years imprisonment.

The COIAO regulated the supply and distribution of both adult and child pornographic materials prior to the enactment of the PCPO. However, it is thought the maximum penalties under the COIAO are inadequate in the context of child pornography.

(iii) Crimes Ordinance (Cap. 200) (the **CO**)

(A) Procurement of persons under 18 for pornography

Section 138A of the CO prohibits use, procurement, or offers to persons under the age of 18 for making pornography or live pornographic performances in which the underage person is or is to be “depicted pornographically”.[85] The maximum penalty

---

81 *HKSAR v Man Kwong Choi* [2008] 5 HKLRD 519. The court also identified aggravating factors, for example previous record involving similar offence against children, the age of the children depicted (e.g. whether particularly young children were involved), possession with intention of publishing and the number of images in possession.

82 *Ibid*.

83 See e.g., *HKSAR v Choy Ka Leung* [2013] HKEC 869, *HKSAR v Tsang Cho Kiu* [2014] HKEC 1770, and *HKSAR v Kwok Po Lun* [2015] HKEC 823.

84 Section 22 COIAO.

85 Section 138A(4) CO defines "depicting a person pornographically" as (a) to visually depict a person as being engaged in explicit sexual conduct, whether or not the person is in fact engaged in such conduct; or (b) to visually depict, in a sexual manner or context, the genitals or anal region of a person or, in the case of a female person, her breast, but, for the avoidance

on conviction in relation to persons under the age of 16 is HK$3,000,000 and 10 years imprisonment, and HK$1,000,000 and 5 years for persons aged 16 or above but under 18.

Section 138A(2) and (3) of the CO establish defences in certain cases where there is consent from the person depicted who is aged 16 or above but under 18, and the pornography or live pornographic performance is solely for the personal use of the defendant and the person depicted.

This section, beyond providing a higher maximum penalty than the PCPO, also covers cases where the victim is aged 16 years or above but under 18 years. However, section 138A of the CO only concerns the maker of the pornography or live pornographic performance, and does not extend to the other classes of persons covered under the PCPO, such as distributors and mere possessors.

(B) Indecency with children under 16

Section 146 of the CO criminalises committing acts of gross indecency with children under the age of 16, or inciting the child to commit such an act. The maximum penalty is 10 years' imprisonment. Neither consent, nor subjective belief that the child is over the age of 16, is a defence.[86] However there is a limited defence of marriage or belief on reasonable grounds of marriage.

(C) The Code of Practice for Internet Computer Services Centres Operators

The Code of Practice for Internet Computer Services Centres Operators was released in July 2003 by the Home Affairs Bureau, and updated in April 2009. It obliges those who operate Internet cafes and the like to use up-to-date devices to filter pornographic, violent or gambling content during the facility's business hours. In addition, operators must ensure that customers below the age of 18 are not permitted access to indecent material (as defined in the COIAO). A breach of the Code of Practice for Internet Computer Services Centres Operators is not a criminal offence.

Criticism of the current legal framework

(i) Reporting obligations of Internet service providers (**ISPs**)

Presently there is no statutory instrument in Hong Kong which addresses the issue as to whether ISPs in Hong Kong should share the responsibility of patrolling and policing materials on their servers. Imposing such a requirement on ISPs is seen as desirable because they "hold the key to the front gate" and are "in a better position (in terms of technical infrastructure, skill and capability) to monitor who or rather what goes in and out of the gate as compared to, for example, the police."[87]

---

of doubt, a depiction for a genuine family purpose does not, merely because it depicts any part of the body referred to in paragraph (b), fall within that paragraph.

86 In *R v Savage* [1997] HKLRD 428, the court held that s. 146 CO is a strict liability offence. However, subsequent cases appear to suggest that the offence is one of absolute liability. In *HKSAR v So Wai Lun* [2004] HKCU 1303, (CA), the court considered similar questions to those in *R v Savage*, but in respect of the offences of intercourse with a girl under the age of 13 (s. 123 CO) and intercourse with a girl under the age of 16 (s. 124 CO). The court declined to follow *R v Savage* and held that ss. 123 and 124 CO were offences of absolute, rather than strict, liability. This has not yet been given further judicial consideration in respect of s. 146 CO.

87 *Above*, n70. p. 106.

While no statutory scheme is in place, the Hong Kong Internet Service Providers Association (**HKISPA**), a trade association for Hong Kong internet service providers, has developed a Code of Practice, which includes a Practice Statement on Regulation of Obscene and Indecent Material (the **Practice Statement**), adopted in September 1997.

The Practice Statement requires HKISPA members to monitor their service for obscene material and to take certain specified steps in relation to users of their service who have utilised the service to make obscene material available on the internet, such as warning the user that their actions may breach COIAO, or cancelling the user's access.[88] The Practice Statement also requires HKISPA members to make a report to HKISPA when action is taken in this regard, and to make monthly reports to the Office for Film, Newspaper and Article Administration, a Hong Kong governmental body tasked with regulating obscene and indecent articles published on the internet and in the media, on any action taken to intervene in respect of internet users in relation to obscene or indecent content in accordance with the Practice Statement.[89]

(ii) Inadequate protection for children aged 16 or above but under 18

As already discussed above, the PCPO only extends to victims who are under the age of 16, in contrast to the CRC's definition of "child" which includes all persons under 18. As noted above, section 138A of the CO does criminalise procurement of all people under the age of 18 for the making of pornography or live pornographic performances, however it is only concerned with the procurer, and does not deal with other categories of people involved in the production and distribution of child pornography, such as those who distribute, advertise, or possess such pornography. It is also a defence to the offence under section 138A if the depicted person (i) is between the ages of 16 and 18; (ii) consented to participation in the production of the material; and (iii) the defendant is the sole audience member of the material.[90] It has therefore been said that children aged 16 or above, but under 18 are left with inadequate protection against exploitation.[91]

(b) Data Protection

Overview of the privacy and data protection regime in Hong Kong

Data protection in Hong Kong is primarily governed by the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**).

Under section 2 of the PDPO, "personal data" is defined as "any data relating directly or indirectly to a living individual (the data subject), from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable".

"Data" means any representation of information (including an expression of opinion) in any document, and includes a personal identifier. A "personal identifier" is an identifier which is assigned to an individual by a data user for its operations which uniquely identifies that individual in relation to the data user, but does not include that individual's name.

---

88 See Articles 10(b) and 10(c) of the Practice Statement.

89 See Article 10(d) of the Practice Statement.

90 Sections 138A(2) and 138(3) COIAO.

91 See for example the Hong Kong Committee on Children's Rights' response to the consultation paper on the proposed legislation for the prevention of child pornography in November 2001.

A "data user" is a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data. Under section 2 of the Interpretation and General Clauses Ordinance (Cap. 1), a "person" includes "any public body and any body of persons, corporate or unincorporated".

Data protection principles

Under section 4 of the PDPO, data users must not contravene the six data protection principles unless the act is required or permitted under the PDPO. In summary, the data protection principles are as follows:

(i) Principle 1 – purpose and manner of collection of personal data:

Principle 1 requires the fair and lawful collection of personal data. In particular, personal data shall not be collected unless it is used for a lawful purpose directly related to a function or activity of the data user. The data sought should be necessary for or directly relating to that purpose, and must be adequate but not excessive in relation to that purpose. Personal data may only be collected by means which are lawful and fair in the circumstances of the case.

In addition, Principle 1 also sets out the information that data users must give to a data subject when collecting personal data from that subject. That information includes (i) informing the data subject whether it is obligatory to supply the data and, if so, the consequences of failing to do so; (ii) the proposed use of the data; (iii) the class of persons to whom the data can be passed; and (iv) the data subject's rights to request access to and request the correction of data (including the details of the person to whom a data request should be made).

(ii) Principle 2 – accuracy and duration of retention of personal data:

All practicable steps shall be taken to ensure that personal data are accurate, up to date and kept no longer than necessary.

(iii) Principle 3 – use of personal data:

Unless the data subject gives prescribed consent, personal data must only be used for the purposes for which the data are collected or a directly related purpose. Under section 2 of the PDPO the term "use" includes the disclosure or transfer of personal data.

(iv) Principle 4 – security of personal data:

All practicable steps shall be taken to ensure that appropriate security measures are applied to personal data.

(v) Principle 5 – information to be generally available:

All practicable steps must be taken to ensure that a person can ascertain (i) a data user's policies and practices in relation to personal data; (ii) be informed of the kind of personal data that a data user holds; and (iii) be informed of the main purposes for which personal data are held and used.

(vi) Principle 6 – access to personal data:

Under Principle 6, a data subject is entitled to, amongst others, (i) ascertain whether a data user holds personal data of the data subject; (ii) request access to personal data; and (iii) request the correction of personal data.

Transfer of personal data

(i) General restriction on transfer

As stated above, under personal data protection principle 3, unless the data subject gives prescribed consent, personal data must only be used for the purposes for which is the data are collected or a directly related purpose. "Use" includes the disclosure or transfer of personal data.

As such, if the data subject does not consent to the transfer of personal data or if a data user's data protection notice does not specify that the personal data can be transferred for specified purposes, the data user is restricted from transferring the personal data.

(ii) Exemption relating to crimes

However, under section 58 of the PDPO, personal data would be exempt from the provisions of data protection principle 3 where: (a) the data is used for the purposes of, amongst others, (i) the prevention or detection of crime; or (ii) the apprehension, prosecution or detention of offenders; or (iii) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice by persons (whether or not the data are held for such purposes); and (b) the application of data protection principle 3 in relation to such use would likely prejudice such matters. Irrespective of whether or not there is "likely prejudice", it is a valid defence to show that a person had *reasonable grounds* for believing that failure to use such data would likely prejudice such matters.

The above exemption from data protection principle 3 is therefore invoked by applying a "harm test" (i.e. determining whether the prejudice to the related interests is likely). The position in Hong Kong in relation to the definition of "likely" is unclear. In *Commissioner of Police v Ombudsman*[92], the New Zealand Court of Appeal stated that, in relation to freedom of information legislation, "likely" does not mean "more likely than not", but means, no more than a distinct or significant possibility. If there is a serious, or real, or substantial risk to an interest, the test is satisfied. However, this appears to be a lower threshold compared to the test adopted by the UK Data Protection Registrar, under which there must be a substantial chance rather than a mere risk.[93]

Unlawful or seriously improper conduct includes criminal and civil wrongs.[94] "Seriously improper conduct" is defined under section 2 of the PDPO as conduct whereby a person would cease to be a fit and proper person where such fitness is a requirement of that person's office, profession or occupation, and any conduct by which a person has or could become a suspended disqualified person under the Hong Kong Jockey Club Rules of racing and Instructions by the Stewards. However, according to "Hong Kong Data Privacy Law"[95] it appears that "seriously improper conduct" is not limited to the definition above. "Unlawful and seriously improper conduct" includes enforcement of regulatory codes of conduct, disciplinary proceedings and the regulation of other behaviour that may have escaped from formal inclusion in codes or

92 [1988] 1 NZLR 385

93 "*Hong Kong Data Privacy Law- Second Edition"*, by Berthold and Wacks, Sweet & Maxwell 2003, p.339.

94 *Lily Tse Lai Yin & Others v The Incorporated Owners of Albert House, [1998] HCFI 811.*

95 *Above*, n30, p.348

disciplinary rules, but which are nevertheless not tolerated by the community generally or the professional sector concerned.[96]

Also, under section 60B of the PDPO, personal data would be exempt from the provisions of data protection principle 3 on the transfer of personal data if the use of the data is (a) required or authorised by law or by an order of a court in Hong Kong; (b) required in connection with any legal proceedings in Hong Kong; or (c) required for establishing, exercising or defending legal rights in Hong Kong. The main point to note about the exemptions contained in section 60B is that they are very wide and not limited to a case by case basis. There is no requirement to show prejudice created by the operation of data protection principle 3 before the exemption can be invoked.[97] This statutory provision will usually apply to the voluntary or court-ordered disclosure of statements and documents, which, notwithstanding redactions, contain personal data.

As such, under section 58 of the PDPO, personal data may be transferred, without the prior consent of the data subject, if the transfer is for the purposes of (i) the prevention or detection of crime; or (ii) the apprehension, prosecution or detention of offenders; or (iii) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, and the restriction of such transfer would likely prejudice such matters. Further, according to the PDPO section 60B, personal data may be transferred in the Hong Kong context if it is (i) required by law or by an order of a court; (ii) required in any legal proceedings; or (iii) required for the assertion of legal rights.

In relation to the identity of transferees under section 58 of the PDPO, the Office of the Privacy Commissioner for Personal Data, Hong Kong (**OPCPD**) stated that there are no specific restrictions on the identity of transferees. There is no specified body (for example, the Hong Kong Police) to whom the personal data must be transferred in order for the exemption under section 58 of the PDPO to apply. Though, "prevention", "preclusion" or "remedying" indicates that a transfer must be to a person performing a role relevant to those activities.[98]

In addition to sections 58 and 60B of the PDPO mentioned above, other possible exemptions from the provisions of data protection principle 3 may require a consideration of (i) the data subject's health (PDPO section 59(2)); (ii) care and guardianship of minors (PDPO section 59A); (iii) due diligence exercise for a proposed business transaction (PDPO section 63B); (iv) emergency situations (PDPO section 63C); and (v) transfer of records to Government Records Service (PDPO section 63D).

Yet, notwithstanding the above exemptions and defences, it is recommended that, for better protection, a data user should obtain the prescribed consent of data subjects in relation to the transfer of their personal data for the purposes of detecting and preventing crime or in situations as may be required by law or by an order of a court for legal proceedings in Hong Kong. This can be specified in the data user's data protection notice or a separate consent form, which should be referred to and/or acknowledged by a data subject in the agreement(s) between the data user and the data subject.

Under section 2 of the PDPO, "prescribed consent" means consent that is given voluntarily. However, prescribed consent may be withdrawn by notice in writing served on the person to whom consent has been given. Naturally, in many cases consent would not be available and the relevant exemption would need to be relied upon when data is used or transferred.

---

96 *Ibid,* p.349.

97 *Chan Yim Wah Wallace v New World First Ferry Services Ltd* HCPI820/2013.

98 *Ibid*.

(iii) Transfer of personal data overseas

Under section 33 of the PDPO (which has not yet come into effect), organisations are prevented from transferring personal data outside Hong Kong unless one of the criteria set out below is met:

(A) The belief that substantially similar laws as those in effect in Hong Kong exist with regard to data protection in the place to which the personal data are to be transferred;

(B) The consent of the data subject has been obtained; or

(C) The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not be dealt with in a manner that would constitute a contravention of the PDPO.

Transfer of data outside Hong Kong may include: (i) transfers from Hong Kong to a place outside Hong Kong; or (ii) transfers between two other jurisdictions where the transfer is controlled by a Hong Kong data user.

As mentioned, section 33 of the PDPO has not yet been brought into effect and the OPCPD is unable to give any indication as to when (if ever) it will be brought in. For this reason, an organisation is currently free to transfer personal data outside Hong Kong *provided that it complies with the six data protection principles*. Nevertheless, it would be prudent to accommodate for (and in practice this is the case) section 33 of the PDPO on the assumption that the provision will come into effect in the future.

The most practical way to ensure compliance is to include provisions in the agreement with any overseas entity to which personal data is transferred, under which the overseas entity agrees that it will deal with the relevant personal data in accordance with the PDPO. It would be preferable to also include a warranty from the overseas entity that data protection laws are in place in the overseas entity's jurisdiction which are substantially similar to those in effect in Hong Kong.

(iv) Consequence of non-compliance

A contravention of the PDPO (except for a contravention of the data protection principles) is an offence and that data user is liable to a fine or imprisonment, depending on the nature of the contravention. Any individual who suffers damage as a result of the contravention of the PDPO may also be entitled to compensation. Contravention of a data protection principle is not an offence but individuals who suffer damage may seek compensation from the data user. Contravention may also result in a complaint to and an investigation by the Privacy Commissioner for Personal Data (the **Commissioner**), who oversees adherence to the PDPO and may grant assistance in respect of proceedings.

(v) Complaints as a result of non-compliance

Complaints made to the Commissioner must be made by the data subject or someone on his behalf and must specify the act complained.

Except in suspected serious contraventions of the PDPO, the Commissioner will liaise with the complainant and data user to see if there is a *prima facie* case of contravention of the Ordinance. If a *prima facie* case is established, the Commissioner will generally try to resolve the dispute through mediation.

Where the Commissioner has been unsuccessful in negotiating a settlement through mediation, or where such an approach is inappropriate, the PDPO gives the Commissioner the power to serve an enforcement notice to remedy the contravention within a specified period. Non-compliance with an enforcement notice served by the Commissioner carries a penalty of a fine at Level 5 (currently HK$50,000) and imprisonment for up to two years.

(c) Banking Secrecy Rules and General Contract Law

Overview of Legal and Regulatory Framework

(i) Common Law Duty of Confidentiality

Banks have a general duty of confidentiality at common law in relation to persons with whom they have a "banker-customer" relationship. The general duty of a bank to keep the affairs of its customers confidential was recognised in the leading English case *Tournier v National Provincial and Union Bank of England*,[99] which held that it was an implied term of the contract between a banker and his customer that the bank would not divulge to third parties, without the express or implied consent of the customer, either the state of the customer's account, or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account.

The duty of confidentiality established in *Tournier* is strict and is subject to four exceptions, namely where:

(A) the bank is compelled to disclose such information by law (this exception only applies in the case of compulsion under Hong Kong law and not compulsion under a foreign law (*FDC Co Limited and others v. The Chase Manhattan Bank, N.A.*[100]));

(B) the bank has a duty to the public to disclose such information;

(C) the interests of the bank require such disclosure; and

(D) such disclosure is made with the customer's consent (express or implied).

When a customer is faced with a potential breach of a bank's common law duty of confidentiality, the relief sought will often be in the form of an injunction. The injunction will usually be granted even though no damage is shown (*FDC Co Limited and others v. The Chase Manhattan Bank, N.A.*).[101]

Banks are subject to civil law sanctions for any breach of such duty. The sanctions sought by an aggrieved party following such a breach would, most commonly, be in the nature of damages.

(ii) Code of Banking Practice

In addition to the common law duty of confidentiality, banks in Hong Kong are expected to comply with the Code of Banking Practice (the **Code**), issued jointly by the Hong Kong Association of Banks and the Deposit-taking Companies Association and endorsed by the Hong Kong Monetary Authority (**HKMA** – the banking regulator in Hong Kong). The Code

99 [1924] 1 KB 461.

100 [1990] 1 HKLR 277, at p. 283G.

101 [1990] 1 HKLR 277, at p. 285 D-E.

applies to "authorized institutions", defined under section 2 of the Banking Ordinance (Cap. 155) as:

(A) a company which holds a valid banking license;

(B) a company which holds a valid restricted banking license; and

(C) a company which is registered as a deposit-taking company.

In relation to customer information, the Code states that institutions should:

- treat the banking affairs of their current and former customers as private and confidential;[102] and
- at all times comply with the PDPO,[103]

as well as prescribing certain practical steps for authorised institutions to take in relation to that information.[104] The Code is non-statutory and expressed to be issued on a "voluntary" basis. However, as a matter of practice, it has considerable force from a regulatory viewpoint. In a press release issued following the recent comprehensive review of the Code, the HKMA stated that authorised institutions "*are expected to achieve full compliance with the new provisions as quickly as possible within 6 months of the effective date. Another 6 months is allowed for compliance with those provisions that require system changes. The HKMA will monitor compliance as part of its ongoing supervision of [authorised institutions]*".[105] The consequences of non-compliance with the Code would be essentially regulatory in nature (for example, in extreme cases, an institution's authorisation to carry on banking or deposit-taking business could be revoked or suspended).

(iii) Organized and Serious Crime Ordinance

Having considered the common law duty of confidentiality which banks owe to their customers and the *Tournier* exceptions, it is notable that the Organized and Serious Crime Ordinance (Cap. 455) (the **OSCO**) is one of the major statutory exceptions to the common law duty of confidentiality. An obligation to disclose information under the OSCO could fall under the first limb of the *Tournier* exception, namely compulsion by law to disclose confidential information. Section 25A of the OSCO compels a bank or any person to disclose confidential account information to "authorized officers" where such bank or person knows or suspects that any property (passing through a bank account, or otherwise) directly or indirectly represents the proceeds of an indictable offence (which could be, for instance, an offence under the Prevention of Child Pornography Ordinance (Cap. 579)). Under section 2(1) of the OSCO, "authorized officer" means:

(A) any police officer;

(B) any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); and

(C) any other person authorized in writing by the Secretary for Justice for the purpose of the OSCO.

---

102 See, e.g. section 8.1.

103 See, e.g. section 8.2.

104 See Section 8, Code.

105 HKMA Press Release, dated 6 February 2015, which reflects the provisions of Section 1.5 of the Code.

Furthermore, section 25A of the OSCO makes it an offence for banks to "tip-off" account holders in circumstances where the bank knows or suspects that a disclosure has been made.[106]

General Contract Law

While ISPs, banks and financial institutions who are APAC Coalition Members will be contractually bound to provide their services to the holder of the recipient account and/or the Offender, the general terms and conditions governing the contractual relationship will normally allow ISPs, banks and financial institutions to terminate their services should it be used for an illegal purpose. Under Hong Kong law, an agreement to commit a crime or an agreement which is otherwise contrary to public policy, will not be enforceable by the courts.

Furthermore, ISPs, banks or other financial institutions may be at risk of committing an offence under the OSCO if it knowingly deals with property which represents the proceeds of any indictable offence. Under Section 25(1) of OSCO, it is an offence to, without reasonable excuse, deal with any property if the person knows or has reasonable grounds to believe that the property, in whole or in part, directly or indirectly, represents any person's proceeds of an indictable offence. In addition, as mentioned above, pursuant to section 25A of OSCO, there is also a duty to make a report to an authorized officer of any knowledge or suspicion relating to such property, as soon as it is reasonable for him to disclose such knowledge or suspicion. A person who contravenes Section 25A commits an offence

In *K Ltd v National Westminster Bank plc (1) HM Revenue & Customs and Serious Organised Crime Agency (2)*[107], the Court of Appeal held that where a bank suspects that money in a client account is criminal property and makes the appropriate reports, there is no breach of contract by the bank for refusing to honour its client's instructions (such as transferring money to third parties).

In addition, in *Shah v HSBC Private Bank (UK) Ltd*[108], the Court confirmed that "suspicion" is a subjective matter and that there is no additional requirement that the suspicion be reasonable, provided it was honestly held. However, where a bank fails to take reasonable care in making the requisite disclosures as soon as reasonably practical, it may be in breach of its general duty of care to its customers.

It is likely that the issues determined in these cases are applicable in Hong Kong given that English judgments remain highly persuasive as legal authority in Hong Kong.

The Joint Financial Intelligence Unit encourages institutions and businesses to make reports to it where one or more suspicious activity indicators exist, even though the specific crime connected to the suspicious transaction cannot be immediately determined. Such indicators include evidence of large or frequent cash transactions, "U-turn" transactions where money passes from one person to another and is then returned to the original person, use of shelf or shell companies or companies located in recognised tax havens. In addition to these indicators, suspicion is reinforced if a bank's customer is unable or unwilling to provide a reasonable and/or legitimate explanation of financial activities undertaken. In these circumstances, a bank may need to carry out a thorough investigation and make a decision as to whether a report should be made.

We recommend that all ISPs, banks and financial institutions who are APAC Coalition Members incorporate provisions permitting them to terminate their services to the Offender immediately if the

---

106 See section 25A(5), OSCO.

107 [2006] EWCA Civ 1039

108 [2009] EWHC 79. This decision was later overturned on appeal in *Shah v HSBC Private Bank (UK) Ltd* [2010] EWCA Civ 31, but on a procedural point only. The principle that, where a financial institution holds a suspicion in respect of a transaction, it must make a report, even if the suspicion is not reasonable, was not disturbed on appeal and was re-applied when the matter was re-tried in *Shah v HSBC Private Bank (UK) Ltd* [2012] EWHC 1283 (QB).

member suspects that the Offender is using his or her account for illegal purposes. In addition, it is possible for APAC Coalition Members to include in their general terms and conditions provisions governing circumstances in which they may release customer information to third parties.

Analysis

Where an APAC Coalition Member knows or suspects that any property passing through a bank account represents the proceeds of an indictable offence (such as, for example, an offence under the PCPO), and reports the identity and account information of the Offender to the "authorized officers" pursuant to section 25A of the OSCO, under ordinary circumstances no civil, criminal and/or regulatory liability should arise. In fact, the APAC Coalition Member would be under a *positive legal duty* to make such a report under section 25A of the OSCO.

Where an APAC Coalition Member shares the identity and account information of the Offender with other APAC Coalition Members for the purpose of the prevention of an offence under the PCPO, it seems highly likely that the APAC Coalition Member could rely on the second limb of the *Tournier* exception, namely duty to the public, and the crimes exemption under section 58 of the PDPO, in making such disclosure.

INDONESIA

1. EXECUTIVE SUMMARY

No	Issue	Recommendation
1.	**Data Protection** Article 26 paragraph (1) of Law No. 11 of 2008 concerning Electronic Information and Transactions ("Law No. 11 of 2008") stipulates that the use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned. Such personal data means part of the privacy rights available in Indonesia, which based on the elucidation of Article 26 paragraph (1) of Law No. 11 of 2008 are: a. the right to enjoy personal life and be free from any invasion; b. the right to communicate with other Persons without surveillance; c. the right to inspect access to information about personal life of and data on individuals. If by any means the use of the personal data by a third party without their consent causes loss to the owner of the personal data, such person may lodge a claim for damages incurred under Law No. 11 of 2008. However, Article 27 paragraph (1) of Law No. 11 of 2008 considers that any Person who consciously and without authority distributes and/or transmits and/or provides access to Electronic Information and/or Electronic Records with contents against propriety, will be considered as an unlawful act. Such act will be subject to a maximum prison sentence of 6 (six) years and/or a maximum fine of Rp. 1,000,000,000 (one billion Rupiah), which is equivalent to almost USD$100,000 (one hundred thousand United States Dollars)	Although Law No. 11 of 2008 provides provisional certainty against the act of sexual exploitation of children, investigations by law enforcers against such act shall follow the rules and guidelines stipulated in the Indonesian Criminal Procedural Code and with consideration of the above stated privacy rights available in Indonesia. Any investigative procedures in contradiction to the Indonesian Criminal Procedural Code will give rise to the right of a pre-trial against the investigation and the right of claims for damages incurred under Law No. 11 of 2008 for infringement of privacy rights.

No	Issue	Recommendation
	pursuant to Article 45 paragraph (1) of the same Law. Article 52 aggravates such sentence, specifying that the criminal acts of propriety mentioned in Article 27 paragraph (1) of Law No. 11 of 2008 that involves sexual exploitation of children to be subject to an increase in the sentence by one third of the basic sentence mentioned in Article 45 paragraph (1) above. It is to note that pursuant to Article 1 point 21 of Law No. 11 of 2008 that a "Person" means an individual, whether an Indonesian citizen, foreign citizen, or legal entity. Article 1 point 22 further stipulates that a "Business Entity" means a sole proprietorship or partnership of both legal entity and non-legal entity. Therefore, Law No. 11 of 2008 both applies to Commercial Entities/Enterprises as well as individuals.	
2.	**Criminal Law** There are few provisions prohibiting the act of exploiting children sexually by means of child pornography in the Indonesian Criminal Code. Nevertheless, the following are issues towards such provisions against child pornography: a. The formulation of the available provisions in the Indonesian Criminal Code is not similar with the cause of action from the crime of child pornography. Such formulation may give rise to the possibility of wrongful interpretation in court proceedings of child pornography cases. b. Weak sanctions and fines available in the Indonesian Criminal Code for crimes of child pornography do not support the idea of justice against the persecutor. c. The legal language formulated which provides the basis of the criminal offence of pornography is still unclear and does not provide legal certainty. Although the Criminal Code is weak to support prohibition against Child Pornography and the exploitation of	Although the Criminal Code seems weak to support the prohibition against Child Pornography and the Exploitation of Children, other laws such as Law No. 44 of 2008 concerning Pornography that do state the prohibition of producing child pornography or illegal acts of Pornography is currently always being criticized for its very broad meanings and easily ambiguous interpretation for the general public. With this regard, we recommend to continually use the Criminal Code as a basis for all criminal acts concerning child pornography or illegal acts of pornography.

No	Issue	Recommendation
	Children, other Laws such as Law No. 44 of 2008 concerning Pornography do state the prohibition of producing, child pornography or illegal acts of Pornography. The Indonesian Criminal Code defines a "Person" who has conducted a criminal act within the Indonesian jurisdiction as a natural person who is an Indonesian citizen or a foreign citizen with no differentiation of sex or religion, standing or rank. Therefore, under the Indonesian Criminal Code, a Criminal is only defined as a natural person and not a legal entity (commercial entity/enterprise). However, it is understood in the Indonesian judicial system that a commercial entity/enterprise is under a criminal obligation because it is also considered as a legal subject that can be subject to criminal sanctions. Consequently, a legal entity can be subject to criminal provisions under various specified laws in the Indonesian judicial system (i.e. corporate environmental crimes). Certainly the punishment will differ from a natural person in comparison to a legal entity (such as fines, penalties and revocation of approvals, winding up, etc.).	
3.	**Banking Secrecy Rules** The current Banking Secrecy Regulation requires Banks or its Affiliates to maintain the confidentiality of any information related to their savings/ depositor customers. Banks or its Affiliates do not have any obligations to maintain the confidentiality of any of its other customer's information other than the Depositor Customer's information. However, there are several exceptions to disclose such information (i.e. tax purposes, court proceedings in criminal and civil cases, interbank exchange of information and request that are proven by a written power attorney from the respective customer). However, these exceptions will require a written	Working together closely with the Indonesian Central Bank, the Head of the Criminal and Civil Courts and other authorized officials related to the above exceptions will open up to easier access of information towards the perpetrators of child pornography.

No	Issue	Recommendation
	authorisation or consent from the Head of Bank of Indonesia (Central Bank of Indonesia) to disclose the Confidential Bank Information.	

2. FULL JURISDICTION REPORT

2.1 International Legal Framework

(a) List of the international legal acts/conventions/protocols analysed are as follows:

- United Nations: Convention on the Rights of the Child of 20 November 1989 ("**UN Convention on the Rights of the Child**")[109];
- ILO Convention No. 182 Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labor of 17 June 1999 ("**ILO Convention 182**")[110];
- International Covenant on Civil and Political Rights of 16 December 1966 ("**the ICCPR**")[111];
- Optional Protocols to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography of 25 May 2000 ("**Optional Protocol to the UN Convention on the Rights of the Child**")[112].

(b) The relevance of the international legal framework:

The aforementioned international conventions are the international legislation concerning or related to child protection **which has been signed and/or ratified** by the Republic of Indonesia.

Based on Law No. 24 of 2000 concerning International Treaties, an International Treaty shall bind and be applicable within the jurisdiction of the Republic of Indonesia once it is ratified in a manner required by the said international treaty. Treaties on human rights, including the UN human rights conventions, are ratified by a national Law issued by the House of Representatives.

In certain cases, the Government of the Republic of Indonesia is likely to enact national legislation to further implement the provisions stipulated in the international conventions. This is particularly true if the international legislation merely set forth general obligations of the State Parties and requires them to further implement them in its national legislation.

The ratification and the enactment of national legislation to implement the international conventions can level the applicability of the international legislation within the national jurisdiction of the signatory parties and thus help to increase the cooperation between the parties (including between APAC countries) to achieve the visions and missions under the international law/convention.

109 http://www2.ohchr.org/english/law/crc.htm
110 http://www.ilo.org/public/english/standards/relm/ilc/ilc87/com-chic.htm
111 http://www2.ohchr.org/english/law/cescr.htm
112 http://www2.ohchr.org/english/law/crc-sale.htm

(c) List of general definitions on the international conventions used:

UN Convention on the Rights of the Child

"Child" means every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier.

ILO Convention No. 182

"Child" shall apply to all persons under the age of 18.

"the worst forms of child labor" comprises:

(i) all forms of slavery or practices similar to slavery, such as the sale and trafficking of children, debt bondage and serfdom and forced or compulsory labor, including forced or compulsory recruitment of children for use in armed conflict;

(ii) the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances;

(iii) the use, procuring or offering of a child for illicit activities, in particular for the production and trafficking of drugs as defined in the relevant international treaties;

(iv) work which, by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of children.

UN Protocol of Convention on Transnational Organized Crime

"Trafficking in persons" shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.

"Child" shall mean any person less than eighteen years of age.

Optional Protocol UN Convention on the Rights of the Child

For the purposes of the present Protocol:

(i) Sale of children means any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration;

(ii) Child prostitution means the use of a child in sexual activities for remuneration or any other form of consideration;

(iii) Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

(d) Information in relation to international Legal Instruments for the fight against child pornography:

Criminalisation of child pornography

The gist of the legal framework in the fight against pornography is the criminalization of child pornography. International conventions have mandated such criminalization through the provision in the UN Convention on the Rights of the Child particularly Article 34 which stipulates that State Parties must protect the child from all forms of sexual exploitation and sexual abuse and shall in particular take all appropriate measures to prevent the inducement or coercion of a child to engage in any unlawful sexual activity, the exploitative use of children in prostitution or other unlawful sexual practices and the exploitative use of children in pornographic performance and materials. This provision is further enforced by Article 3 and 4 of the Optional Protocol to the UN Convention on the Rights of the Child where State Parties are obliged to criminalise and establish jurisdiction over certain actions, including activities related to child pornography.

The UN Convention on the Rights of the Child is one of the bases of the **enactment** of Law No. 23 of 2002 concerning Child Protection (the "**Child Protection Law**") which provides protection for a child against sexual violations. Furthermore, Indonesian national regulations such as the Criminal Code, the Pornography Law, the Child Protection Law, and the Electronic Information and Technology Law (as defined as Law No. 11 of 2008) regulate that any harmful act against a child including child pornography is subject to criminal sanction. Although the Child Protection Law does not have specific provisions on child pornography, it criminalises indecent acts of a sexual nature towards children as regulated in Article 81 and 82. Another criminalization is found in Article 27 (1) of the Electronic Information and Technology Law which penalizes distribution or transmission of electronic documents or information containing indecent materials.

2.2 Questions and Answers relevant to the APAC Coalition

(a) Is there laws specifically addressing child pornography in each of the APAC Jurisdictions?

The elucidation of Article 4 letter f. of Law No. 44 of 2008 concerning Pornography ("**Pornography Law**") defines child pornography as… *"any form of pornography that involves children or involves adults performing or acting as children."*

Furthermore, Article 1 paragraph 1 of the Pornography Law defines "pornography" as drawings, sketches, illustrations, photos, writings, voices, sounds, moving pictures, animation, cartoons, discussions, body language, or any other forms of messages through many forms of media communication and/or public displays, consisting of indecent acts or sexual exploitation that prohibits the societal norms of decency. A legal subject under the Pornography Law is defined under Article 1 point 3, which defines every "Person" as a natural person or corporation established as a legal entity (corporate) or a non-legal entity (unincorporated).

Early 2010, the Constitutional Court of the Republic of Indonesia (the "Constitutional **Court**") conducted a judicial review on this law, particularly regarding Article 1 on the definition of pornography, and Article 4 regarding the production and distribution of pornographic materials. The arguments of the applicant concern the possibility of arts and cultural activities to be deemed as pornographic by this law. The Constitutional Court rejected the argument by saying that the Pornography Law already excludes matters on arts and culture as they will be governed by another law. The Constitutional Court then declared these provisions to be in line with the Constitution, and

thus remain enforceable as law.[113] Currently, there is an application to conduct another judicial review on this law, regarding Article 4 on the production and distribution of pornographic materials and Article 6 on exposing materials referred to in Article 4.

Indonesian Courts have issued decisions based on the Pornographic Law, particularly in criminal cases regarding the production and distribution of pornographic materials governed in Article 4 of this law, for example the 2009 decision of District Court of Karanganyar regarding the production of a pornographic video of a couple. In its decision, the District Court also relied on Article 282 of the Criminal Code on the distribution of pornographic materials. The tendency is that the Court will not only base its decision on the Pornography Law on cases involving pornography, but will also rely on the Criminal Code.

Children based on relevant regulations are as follows:

(i) Article 1 paragraph 4 of the Pornography Law

"Children are individuals that are not 18 (eighteen) years old"

(ii) Law No. 39 of 1999 concerning Human Rights

"Children mean all unmarried persons under the age of 18, including, should this be in their interest, all unborn children."

(iii) Law No. 23 of 2002 concerning Child Protection

"Children are individuals that are not 18 (eighteen) years old, including an unborn child."

The elements of this 'child pornography' are penalized under various legislations such as the:

(i) Article 282 criminalises those who disseminate information containing indecent matters.

Articles 295 – 297 jobs. Articles 300 and 301 of the Criminal Code.

Article 295 of the Criminal Code states… *"Any person shall be punished:*

1st, by a maximum imprisonment of five years, if he with deliberate intent causes or facilitates the commission of any obscene act by his under age child, step-child or foster-child, his pupil, a minor entrusted to his care, education or vigilance or his underage servant or subordinate, with a third party;

2nd, by a maximum imprisonment of four years, if he accepts the cases enumerated under 1st, with deliberate intent causes or facilitates the commission of any obscene act by a minor, whose minority he knows or must reasonably suspect, with a third party."

Article 296 of the Criminal Code stating… *"Any person who makes an occupation or a habit of intentionally causing or facilitating any obscene act by others with third parties, shall be punished by a maximum imprisonment of one year and four months or a maximum fine of one thousand rupiahs."*

[113] The Constitutional Court Decision No. 10-17-23/PUU-VII/2009, dated 25 March 2010. There is a dissenting opinion on this decision which takes the view that since there is no other law on arts and culture, thus the Pornographic Law theoretically can still govern on arts and culture.

Article 297 of the Criminal Code stating… *"Trade in women and minors of the male sex shall be punished by a maximum imprisonment of six years."*

Article 300 of the Criminal Code stating…

(A) *By a maximum imprisonment of one year or a maximum fine of three hundred rupiahs shall be punished:*

1st, any person who with deliberate intent sells or administers intoxicating drinks to a person who is in an obvious state of drunkenness;

2nd, any person who with deliberate intent makes drunk a child under the age of sixteen years;

3rd, any person who by force or threat thereof with deliberate intent forces someone to use intoxicating drinks.

(B) *If the fact results in a grievous bodily harm, the offender shall be punished by a maximum imprisonment of seven years.*

(C) *If the fact results in death, he shall be punished by a maximum imprisonment of nine years.*

(D) *If the offender commits the crime in his profession, he may be deprived of the exercise of said profession.*

Article 301 of the Criminal Code stating…

"The person who surrenders or leaves a child under the age of twelve years who is under his legal authority to another person, knowing that it will be used for begging or carrying out begging, for performing dangerous feats or dangerous labour or labour detrimental to the health, shall be punished by a maximum imprisonment of four years."

(b) What is the definition of illegal child pornography pursuant to each of the APAC Jurisdictions (looking at both domestic and international law)?

(Please refer to the definitions of Child Pornography in letter (a) above…)

(c) Are there legal obstacles to the undertaking of a test or an undercover transaction by a law enforcement agency on behalf of the national hotline to the Offender's account?

Under the Indonesian legal framework, only the competent law enforcement authorities are allowed to engage in undercover operations that will always require prior authorisation of the head of the law enforcement agency subject to their authority in the Indonesian Jurisdiction.

There have been several cases where law enforcement agencies have performed undercover operations to trace Offenders. However, these operations must be implemented subject to complying with prescribed procedural requirements and must be within the scope of their authority, in particular of Law No. 8 of 1981 concerning Criminal Procedure.

(d) Are there legal obstacles to the undertaking of a test or an undercover transaction by an entity other than a law enforcement agency (for example, a credit card company or an online payments facilitator) on behalf of the national hotline to the Offender's account?

As far as legislation speaks, entities that are authorized to conduct such an undertaking are the Indonesian Police and/or Authorized Governmental Officials that are given special authority to investigate under relevant laws and regulations to conduct an investigation ("**Investigators**") and the Officials from the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)) or *Pusat Pelaporan dan Analisis Transaksi Keuangan* (Indonesian abbreviation, "**PPATK**"). With this regard, the Criminal Procedural Law provides that in the event that there is reason to believe that a criminal act is and/or has taken place; an Investigator is obligated to promptly take the necessary actions to investigate. Furthermore, an investigator who knows, receives a report or a complaint about the occurrence of an event which may reasonably be presumed to be a criminal act, shall be obligated to promptly take the necessary investigation.

The PPATK on the other hand was established to deter and abate the criminal offense of money laundering. PPATK is an institution with the mission of preventing and eradicating money laundering in Indonesia. The Money Laundering Laws positioned PPATK as the focal point in the anti-money laundering regime in Indonesia.

Based on the above, it is unlikely that an entity other than those considered as Investigators and the PPATK will be allowed to perform such investigations on behalf of the national hotline to the Offender's account. We suggest working closely together with the Indonesian National Police or Authorized Governmental Officials and the PPATK in each Governmental Agencies and Departments to have direct access with the above mentioned Investigators.

(e) Are there legal obstacles to the collaboration of APAC Coalition Members in relation to the test or the undercover transaction?

(Please refer to the response on letter (d) above…)

(f) Are there legal obstacles to the disclosure by the APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC, the other APAC Coalition Members and the public prosecutor?

One of the principles pursuant to Law No. 4 of 2004 concerning Judicial Power is the principle of disclosure. The mentioned law states that… "*every examination hearing are open to public, unless the laws provide otherwise*." With respect to such stipulation, the disclosure of the identity of the holder of the merchant's account and/or the Offender to ICMEC are mandatory. Furthermore, the Pornography Law provides the procedural guidelines to an examination of a trial relating to pornography. Such guidelines mention the procedure to disclose the identity of the perpetrators. Nevertheless, the pornographic materials contained as evidence must be kept secret and confidential by the public prosecutors and officials of the respective trial at all times.

However, considering that the victims of these exploitation and pornographic cases are the children themselves, it should be considered by the supervising Judge to apply the non-disclosure principle to the victims in question in a court proceeding to protect the child's future credentials.

(g) Are there legal obstacles to the termination of the provision of services to the Offender by APAC Coalition Members?

Pursuant to Article 41 of the Pornography Law, other than the penal sanctions such as imprisonment and large amount of fines, the services of the Offender shall be subject to:

(i) the freezing of its business permit;

(ii) the revocation of its business permit;

(iii) the confiscation of all income related to the services of the Offender; and

(iv) the revocation of the status of the legal entity.

With respect to the enactment of the above law, the stipulation of Article 41 of the Pornography Law shall apply against the services of the Offenders in question.

2.3 Analysis of domestic and international statutory law

(a) Key Problems

Some of the international conventions on child protection, and in particular child pornography, such as the Optional Protocol of the UN Convention on the Rights of the Child are not yet ratified by the Republic of Indonesia and thus the applicability in the national jurisdiction is not binding.

The other problem is that the definition of a child in various national laws is different particularly regarding the maximum age at which a person can be categorized as a child. This can become an obstacle to determine whether the case can be categorized as a child pornography case.

2.4 Subjects of direct relevance

UN Convention on the Rights of the Child

After the ratification of the UN Convention on the Rights of the Child by virtue of national legislation (i.e. Presidential Decree No. 36 of 1990), the Republic of Indonesia is bound by the provisions of the said convention.

The UN Convention on the Rights of the Child provides obligation for the State Parties to protect the rights of the child. With regard to child pornography, one of the provisions in the UN Convention which relates to this matter is Article 34, as follows:

"State Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, State Parties shall in particular take all appropriate national, bilateral, and multilateral measures to prevent:

(i) inducement or coercion of a child to engage in any unlawful sexual activity;

(ii) the exploitative use of children in prostitution or other unlawful sexual practices;

(iii) the exploitative use of children in pornographic performances and materials."

Article 34 requires state parties to enact national legislation that will make sure the implementation of the above obligations. It also encourages the State Parties to cooperate in preventing the exploitation of children in pornographic activities.

In order to implement the obligations set forth in the UN Convention on Rights of the Child, the Republic of Indonesia has enacted Law No. 23 of 2002 concerning Child Protection to protect all the rights of children within the Indonesian jurisdiction.

ILO Convention No. 182

ILO Convention No. 182 was ratified by the Republic of Indonesia by virtue of Law No. 1 of 2000 and thus the provisions of ILO Convention No. 182 are binding and applicable within the national jurisdiction of the Republic of Indonesia.

Article 6 of The ILO Convention 182 stipulates that Each Member shall design and implement programmes of action to eliminate as a priority the worst forms of child labour. Article 3 of the ILO Convention 182 provides that worst forms of child labour are as follows:

(i) all forms of slavery or practices similar to slavery, such as the sale and trafficking of children, debt bondage and serfdom and forced or compulsory labour, including forced or compulsory recruitment of children for use in armed conflict;

(ii) the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances;

(iii) the use, procuring or offering of a child for illicit activities, in particular for the production and trafficking of drugs as defined in the relevant international treaties;

(iv) work, which by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of children.

As mentioned above, child pornography is one of the forms of child labour that must be prioritized to be eliminated. Indonesian national legislation prohibits such type of works for children and violation of the said provisions is subject to criminal sanction. The Government also established an independent commission i.e. Commission of Child Protection of Indonesia (*Komisi Perlindungan Anak Indonesia* or "**KPAI**") to help, to monitor and ensure the implementation of all regulations related to child protection, as well as provide assistance to a child and its family which are victims of any kind of abuse including sexual abuse.

Optional Protocol UN Convention on the Rights of the Child

Indonesia signed the Optional Protocol of the UN Convention on the Rights of the Child on 24 September 2001, but has not yet ratified it. Therefore, the provisions set forth in said Optional Protocol are not binding to the Republic of Indonesia. However, as a signatory country, Indonesia is bound by Article 18 of the Vienna Convention on the Law of Treaties to refrain from taking any action that would defeat the object and purpose of such Protocol.

The government has shown political will and commitment to ratify this Protocol and adhere to the provisions therein. This commitment is shown through the enactment of the Presidential Decree No. 40/2004 on the Indonesian Human Rights Action Plan (*Rencana Aksi Nasional Hak Asasi Manuisa* or abbreviated *RAN HAM Indonesia*) 2004-2009, which was further amended and updated by Presidential Decree No. 23/2011 on the Indonesian Human Rights Action Plan (*RAN HAM Indonesia)* 2011-2014 in which one point of the action plan is to prepare the ratification of the Optional Protocol of the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. Such ratification plan has been endorsed by various fractions of political parties in the House of Representatives.[114]

Article 1 of the Optional Protocol stipulates that State Parties shall prohibit the sale of children, child prostitution and child pornography as provided for by the present Protocol.

Furthermore, Article 3 paragraph (1) states that each State Party shall ensure that, at a minimum, the following acts and activities are fully covered under its criminal or penal law, whether such offences are committed domestically or trans-nationally or on an individual or organized basis particularly in the context of the sale of children for the purpose of sexual exploitation, offering, obtaining, procuring

[114] Indonesia Against Child Trafficking, http://groups.yahoo.com/group/ASAFI/message/153., accessed per 3 August 2010.

or providing a child for child prostitution, producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes of child pornography.

The aforementioned prohibitions are also regulated under Indonesian national law.

Privacy and Data Protection Rules

Advances in sophisticated technology with the capacity to collect, analyse and distribute information from individuals have brought about a need for legal protection. Furthermore, new developments in medical research, health care, and telecommunications, and more advanced systems of transportation and financial transactions have dramatically increased the flow of personal information. Computers integrated into high-speed networks with more advanced processing systems allow for the creation of comprehensive dossiers of personal data without the need for a central computer.

Surveys suggest that current concerns regarding invasion of privacy will become even more apparent in the future. This almost universal fear of invasion of privacy has prompted several countries to introduce special laws to protect the privacy of their citizens. Human rights groups are concerned that too much of this technology has been exported to developing countries that, unlike advanced countries, lack the capacity to or are unconcerned about protection of privacy. Evidently this impedes trade in technology.

The power, capacity and speed of information technology is increasing rapidly, thus presenting greater opportunities for the invasion of privacy.

Comprehensively, Indonesia does not have specific regulations which collectively govern privacy and data protection. However, with regards to the subject at hand, the following are provisions from relevant regulations governing privacy and data protection.

Under Indonesian law, Article 14 of Law No. 39 of 1999 concerning Human Rights ("**Law No. 39/1999**") states that:

(i) *Everyone has the right to communicate and obtain the information they need to develop themselves as individuals and to develop their social environment.*

(ii) Everyone has the right to seek, obtain, own, store, process, and impart information using all available facilities.

Furthermore, Article 21 of Law No. 39/1999 states that:

Everyone has the right to integrity of the individual, both spiritual and physical, and as such shall not be made the object of any research.

The provisions of Law No. 39/1999 do not explicitly define whether subjects under the said law are also applicable to commercial entities/enterprises since the main objective of the said law is to protect the principle rights of a natural person (human) and not a legal entity.

For political interests, the Indonesian Police Service maintains extensive files on citizens who have not been accused or suspected of committing a crime. Anyone who requests the services of the police must be asked for his or her biographical information. However, Act No. 8 of 1981 prohibits publication of the content of investigation reports.

Under Indonesian law, Article 29 point (1) of Law No. 39 /1999 states that:

Everyone has the right to protection of his privacy, family, honor, dignity and rights of ownership.

Furthermore, Article 32 of Law No. 39 of 1999 states that:

Freedom and confidentiality in correspondence, including communication through electronic telecommunications means may not be interfered, except upon the order of a court or other legitimate authority according to the prevailing laws and regulations.

Broader issues also appear in the private sphere in which electronic transactions for trade via electronic systems (electronic commerce) have become a part of national and international trade. This fact shows that the convergence in the field of information technology, media, and informatics (telematics), inevitably, continues to develop in line with society's intention to further advance the fields of information technology, media, and communications.

The globalization of information has placed Indonesia as part of the world's information community; therefore the creation of regulations concerning the organization of Electronic Information and Transactions at the national level is required in order to develop Information Technology that can be carried out in an optimal, distributive, and widespread manner throughout all levels of society. In connection therewith, the Government of Indonesia enacted Law Number 11 of 2008 concerning Electronic Information and Transactions ("**Law No. 11/2008**").

This Law shall apply to any Person who commits legal acts as governed by this Law, both within the jurisdiction of Indonesia and outside the jurisdiction of Indonesia, having legal effect within the jurisdiction of Indonesia and/or outside jurisdiction of Indonesia and detrimental to the interest of Indonesia. "Detrimental to the interest of Indonesia" shall include but is not limited to the detriment of the interests of national economy, strategic data protection, nation's dignity and degree, state defence and security, sovereignty, citizens, as well as Indonesian legal entities.

Pursuant to Article 1 point 21 of Law No. 11 of 2008, a "Person" means an individual, whether an Indonesian citizen, foreign citizen, or legal entity. Article 1 point 22 further stipulates that a "Business Entity" means a sole proprietorship or partnership of both legal entity and non-legal entity. Therefore, Law No. 11 of 2008 both applies to Commercial Entities/Enterprises as well as individuals.

In respect to Article 26 of Law No. 11/2008 provides that:

"Unless provided otherwise by Laws and Regulations, use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned."

In the usage of Information Technology, personal data shall be a part of the privacy rights to be protected. Privacy rights shall contain the following meaning:

(i) A privacy right shall be the right to enjoy personal life and be free from any invasion.

(ii) A privacy right shall be the right to communicate with other Persons without surveillance.

(iii) A privacy right shall be the right to inspect access to information about the personal life of and data on individuals.

On this basis, no personal or transactional data may be disclosed to a third party without the consent of the concerned individual without a legal stipulation or ground.

Activities via electronic media systems also called cyber (cyberspace), despite being virtual, can be categorized as actual legal acts and actions. Speaking judicially, activities in cyberspace cannot be approached by parameters and qualifications of conventional law only, and if such conventional methods are adopted, it is too complicated and many would evade the law. Activities in cyberspace are virtual activities that have actual impacts even if the means of proof is electronic in nature. Therefore, the subject actor must be qualified as a Person who has committed an actual legal act. In e-commerce activities, there are such things known as, inter alia, electronic records, and the position of which is held equivalent to documents made on paper.

The Constitutional Court has conducted a judicial review on parts of this law: in particular to Article 27 paragraph (3) regarding the dissemination of electronic information containing insult or defamation. The arguments supporting this application is freedom of speech granted to individuals. However, the Constitutional Court has declared this Article to be in line with the constitution, and thus remains enforceable as law.[115]

The Indonesian Courts have yet to decide a case based on this law, including on the provisions related to pornography. This is because this law has only come into force just recently in April 21, 2010. However, the trend to utilize this law to eradicate the dissemination of pornographic images, videos, and films has been apparent during the recent ongoing investigation process of a celebrity sex scandal video in Indonesia.

2.5 Subjects of indirect relevance

International Covenant on Civil and Political Rights (1966)

The Republic of Indonesia ratified the International Covenant on Civil and Political Rights on 23 February 2006 by virtue of Law No. 12 of 2005. The International Covenant on Civil and Political Rights set forth general rights of a child as regulated in Article 24 paragraph (1) which stipulates: Every child shall have, without any discrimination as to race, colour, sex, language, religion, national or social origin, property or birth, the right to such measures of protection as are required by his status as a minor, on the part of his family, society and the State.

Money Laundering

The Republic of Indonesia has enacted Law No. 15 of 2002, as recently amended by Law No. 8 of 2010 concerning the Prevention and Eradication of the Criminal Act of Money Laundering ("**Money Laundering Laws**").

Various crimes that are either committed by **individuals or corporations** (in this regard is also applicable to commercial entities/enterprises) within the territory of a state or committed crossing the boundaries of the territory of other states, have been increasing. These crimes include, inter alia: corruption, bribery, goods smuggling, worker smuggling, immigrant smuggling, banking, illicit traffic in narcotic drugs and psychotropic substances, trafficking in slaves, women, and children, illicit trafficking in firearms, kidnapping, terrorism, theft, embezzlement, fraud, and various other white-collar crimes. Such crimes have involved or produced a large amount of Property.

Property derived from these crimes or criminal offenses is not generally directly spent or used by perpetrators, because if directly used, the origin of the Property will be vulnerable to be traced by law enforcement officers. Usually, the perpetrators first attempt to introduce the Property that is realized from a crime into the financial system, particularly the banking system. In this manner, the perpetrators expect that the origin of the Property is not traceable by law enforcement officers. Attempts to conceal

115 The Constitutional Court Decision No.50/puu-VI/2008 jo Putusan MK No.2/PUU-VII/2009.

or disguise the origin of the Property realized from a criminal offense is known as money laundering as outlined by the Money Laundering Laws. Acts of money laundering, besides being significantly detrimental to the public, also harm the state, as they may affect or destroy national economic stability or state finance through the increase of various crimes.

In addition, for effective court proceedings against a criminal offense of money laundering, this Law regulates the powers of investigators, public prosecutors, or judges in accordance with the levels of case administration to order a Financial Service Provider to freeze Property. The Money Laundering Laws also regulate the powers of investigators, public prosecutors, or judges to propound questions to Financial Service Providers on Property of every person who has been reported by the INTRAC/PPATK, suspect, or defendant. The functions and authorities of INTRAC are further stipulated in article 40 and 41 of the Money Laundering Laws.

NEW ZEALAND

1. EXECUTIVE SUMMARY

No.	Issue	Recommendation
	Data Protection New Zealand's Privacy Act 1993 (Privacy Act) only regulates dealings with "personal information", which is defined to mean information about an identifiable individual. Information about non-natural persons, such as corporations, is not regulated by the Privacy Act. There are no separate data privacy rules that apply to information about corporate legal persons. The information privacy principles in New Zealand's Privacy Act will regulate each collection, use and disclosure of personal information that occurs as part of the proposed operation of the APAC Coalition. This advice only considers the particular question of whether there are any legal obstacles to the disclosure by APAC Coalition Members of the identity of natural persons who are account holders to fellow Coalition Members, the public prosecutor and/or investigating authorities. Where an APAC Coalition Member regulated by the Privacy Act discloses the identity of a natural person to any other person (whether a fellow Coalition Member or the public prosecutor or investigating authorities), the disclosing Coalition Member must be satisfied that there is no contravention of the non-disclosure rule in Principle 11 of the Privacy Act. The Member will therefore need to demonstrate that the disclosure falls within one of the permitted grounds of disclosure under Principle 11. These grounds are discussed further in section 3.2.2 of the main report. In addition, Coalition Members must comply with Principle 8, which provides that regulated agencies shall not use personal information without taking	Neither Principle 11 (disclosure) nor Principle 8 (data quality) is likely to present an insurmountable obstacle to the proposed disclosure of account holder identities, but it will be necessary for APAC Coalition Members to develop compliance systems to ensure adherence to those principles. From a compliance point of view, the authorisation exception to the non-disclosure rule in Principle 11 is probably the most robust exception that APAC Coalition Members could seek to rely on in disclosing the identity of individual account holders. We therefore recommend that APAC Coalition Members obtain the informed, express authorisation of their customers to disclose account holder information as contemplated by the APAC Coalition framework. In practical terms, this might involve APAC Coalition Members updating their privacy policies and obtaining their account holders' informed, express authorisation to the same. To comply with Principle 8 (data quality), APAC Coalition Members will need to develop appropriate procedures to ensure that the personal information that they disclose to fellow Coalition Members, ICMEC and/or law enforcement agencies is not inaccurate, incomplete, irrelevant or misleading. These procedures will need to address situations such as where the account into which a payment for child pornography has been received is a joint account.

No.	Issue	Recommendation
	reasonable steps to ensure that the information is accurate, complete, relevant and not misleading, having regard to the purpose for which it is proposed to be used. The present case requires a relatively high standard of data quality since account holders who are natural persons may suffer a significant degree of harm in the event that they are mistakenly identified as persons involved in the receipt of payments for online child pornography.	
1.	**Criminal Law** There is no rule of law in New Zealand requiring investigations underlying criminal proceedings to be undertaken by law enforcement. Criminal cases have been successfully prosecuted in circumstances where undercover private investigators have gathered the relevant evidence. **Classification Act offences** It is likely that whenever a person (including a law enforcement officer) conducts a test or undercover transaction using an alleged Offender's Site, that person will commit a possession offence under the Films, Videos, and Publications Classification Act 1993 (Classification Act). They may also commit one or more distribution or copying offences. There are several defences to liability in the Classification Act. Some of these defences can be relied upon only by named law enforcement officers (such as members of the Police and persons in the service of the Crown). Others, such as the 'approved purpose' and 'lawful authority or excuse' defences, are not limited to a defined class of persons. The possible application of these defences is discussed in section 3.1.2 of the main report.	**Classification Act offences** Law enforcement officers named in the Classification Act enjoy broader defences than civilian testers and so will usually be better placed than ICMEC or APAC Coalition Members to undertake tests or undercover transactions (at least from a liability point of view). It might be worthwhile exploring whether ICMEC or its representatives can qualify as a person in the service of the Crown. This will permit ICMEC or its representatives to rely on the Classification Act defences that are specific to named officials. Where ICMEC or APAC Coalition Members determine to undertake undercover tests themselves, it would be prudent for them to develop compliance systems to help demonstrate how they fall within the bounds of the Classification Act defences they intend to rely on.

No.	Issue	Recommendation
	Secondary liability There is a risk that by conducting an undercover transaction on the Offender's Site, a tester might face liability as a secondary party to the Classification Act offences committed by the Offender in supplying or distributing objectionable publications.	**Secondary liability** From a practical perspective, the risk of ICMEC or APAC Coalition Members being prosecuted as secondary participants to Classification Act offences appears to be relatively remote. We anticipate that there will often be difficulties in making out the mens rea (mental element) required to establish secondary liability. Further, the Prosecution Guidelines issued by the Crown Law Office set out a number of factors that appear to militate against any such prosecution. These factors are further discussed in section 3.4.2 of the main report. However, in order to eliminate the risk of secondary liability for ICMEC and APAC Coalition Members altogether, we recommend that undercover transactions only be taken by or with the authorisation of law enforcement officers. We recommend that ICMEC discuss the proposed operation of the APAC Coalition with law enforcement authorities prior to implementing the framework in New Zealand. New Zealand's Policing Act 2008 acknowledges the role of private sector bodies in assisting the Police in the performance of their roles. If ICMEC can reach an understanding with law enforcement authorities in New Zealand that allows ICMEC and the APAC Coalition Members to assist in the identification of alleged Offenders without the threat of direct or secondary liability, risk can be removed.
2.	**Banking Secrecy Rules** New Zealand banks and financial institutions owe a strict duty of confidence to their customers, whether legal or natural persons. The proposed disclosure of account holder identities is likely to constitute a breach of this duty, unless the relevant Coalition	From a compliance point of view, the consent exception to the bankers' duty of confidence is probably the most robust exception that Coalition Members could seek to rely on. We therefore recommend that APAC Coalition Members obtain the informed, express authorisation of their customers to disclose account holder

No.	Issue	Recommendation
	Member can establish that its disclosure falls within one of the well-established exceptions to that duty. These exceptions will be discussed in section 3.5.2 of the main report.	information as contemplated by the APAC Coalition framework. There may also be instances where the proposed disclosure is required by law, such as where the transaction is relevant to the enforcement of the Proceeds of Crime Act 1991 (from 1 December 2009, the Criminal Proceeds (Recovery) Act 2009) and/or under the Financial Transactions Reporting Act 1996. APAC Coalition Members should keep records of when they make disclosures mandated by legislation.

No.	Issue	Recommendation
3.	**Other Legal Obstacles** Termination of customer contracts The question of whether a Coalition Member can terminate a customer contract as contemplated by the APAC Coalition framework will turn on the construction of the relevant contract and the application of New Zealand's Contractual Remedies Act 1979. Each Coalition Member will need to separately assess their position vis-à-vis the particular customer concerned. Defamation/malicious falsehood liability ICMEC and APAC Coalition Members should be aware of the risk of defamation and/or malicious falsehood liability in the event that the allegation made against the account holder is unfounded. Defamation and malicious falsehood actions can be brought by natural and legal persons alike. However, the Defamation Act 1992 provides that proceedings brought by a body corporate will fail unless the body corporate alleges and proves that the publication complained of has caused, or is likely to cause, pecuniary loss to that body corporate. Even where the allegation is well-founded, aggrieved account holders may nonetheless commence defamation and/or malicious falsehood proceedings against ICMEC and APAC Coalition Members. It may be that ICMEC and APAC Coalition Members can rely on the defences of truth and/or qualified privilege in respect of at least some of their publications if limited to enforcement agencies, for example. However, it is fair to say that the outcome of defamation proceedings in New Zealand (as in many other jurisdictions around the world) cannot always be predicted with certainty.	Termination of customer contracts It is preferable that each APAC Coalition Member includes an express term in its customer contracts empowering the Member to terminate services provided to a customer where the Member forms a suspicion that the customer's account has been used to receive monies for allegedly unlawful activities. Care needs to be taken in drafting any such term so that an APAC Coalition Member can safely rely on the term in circumstances where its suspicion may not be reasonably held, and/or the material in question turns out not to be an objectionable publication within the meaning of the Classification Act. Defamation/malicious falsehood liability ICMEC and APAC Coalition Members should develop and implement robust procedures to verify the correctness of any information disclosed as part of the APAC Coalition framework. Crucially, ICMEC and APAC Coalition Members need to be mindful of the fact that the identified account holder may not be the person responsible for the website on which the child pornography material is being sold. Consideration should also be given to the extent to which it is necessary to disclose the identity of an account holder to fellow Coalition Members and ICMEC. From a liability perspective, each further disclosure increases a defendant's exposure in damages.

No.	Issue	Recommendation
4.	**Other Points to Note** Search and Surveillance Bill We have not considered law enforcement search and surveillance powers in this Report. However, we note that a significant piece of legislation reforming New Zealand's laws in this respect – the Search and Surveillance Bill – was reported back from a Select Committee (the Justice and Electoral Committee) of the New Zealand Parliament on 4 November 2010. One of the purposes of the Bill is to provide "appropriate legislative powers to enable law enforcement and regulatory agencies to extract electronic information and use surveillance devices in order to investigate and combat criminal activity." Public debate regarding the operation of the proposed APAC Coalition While not a legal obstacle in itself, we anticipate that civil libertarians will promote debate about the proposed operation of the APAC Coalition. ICMEC and the APAC Coalition Members will need to develop a strategy to address any such debate.	

2. FULL JURISDICTION REPORT

2.1 International Legal Framework

The following international legal instruments are relevant to the issues presented by the case study on which the Report is based.

Sexual exploitation of children

United Nations Convention on the Rights of the Child (20 November 1989)

New Zealand signed the U.N. Convention on the Rights of the Child on 1 October 1990, and ratified it on 6 April 1993. The Convention entered into force on 6 May 1993.

On 16 June 2000, New Zealand acceded to the amendment to Article 43, paragraph 2 of the Convention on the Rights of the Child. The Article 43 amendment increased the number of members required for the Committee on the Rights of the Child. It entered into force on 18 November 2002.

United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (25 May 2000) (Optional Protocol on the Sale of Child Pornography)

New Zealand signed the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography on 7 September 2000.

New Zealand has not yet ratified the Optional Protocol, pending an amendment to the *Adoption Act 1955*.[116] We understand that this amendment involves the addition of a new offence of improperly inducing consent as an intermediary, for the adoption of a child.[117]

116 http://www.legislation.govt.nz/act/public/1955/0093/latest/DLM292661.html?search=ts_act_adoption+act_resel&p=1&sr=1

117 Accessible here.

New Zealand has enacted several pieces of legislation to implement its obligations under the Optional Protocol on the Sale of Child Pornography, including:

- *the Films, Videos and Publications Classification Amendment Act 2005*;[118] and
- *the Crimes Amendment Act 2005*.[119]

Data protection

(i) OECD: Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data (23 September 1980)

New Zealand became a member of the OECD on 29 May 1973, and adopted the OECD Privacy Guidelines on 23 September 1980.

The OECD Privacy Guidelines were a major influence on the drafting of New Zealand's *Privacy Act 1993*,[120] as reflected in the long title of that legislation:

An Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data …

(ii) United Nations: International Covenant of Civil and Political Rights (19 December 1966)

New Zealand ratified the ICCPR on 28 December 1978. The ICCPR entered into force for New Zealand on 28 March 1979.

Article 17 relevantly provides that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to, unlawful attacks on his honour or reputation.

2. Everyone has the right to protection of the law against such interference or attacks.

The long title of the New Zealand Bill of Rights Act 1990 ("**NZBORA**")[121] purports to affirm New Zealand's commitment to the ICCPR, but not all of the rights guaranteed by the ICCPR are secured by the NZBORA. For example, there is no provision in NZBORA that corresponds to Article 17 of the ICCPR. That said, the NZBORA does protect some privacy interests indirectly, including by section 21, which protects the "right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise".

We note that the NZBORA is not superior law like the US Constitution. NZBORA is an ordinary statute of the Parliament of New Zealand. Where possible, the NZBORA requires

---

118 http://www.legislation.govt.nz/act/public/2005/0002/latest/DLM333252.html?search=ts_act_classification_noresel&p=1&sr=1

119 http://www.legislation.govt.nz/act/public/2005/0041/1.0/DLM346155.html?search=ts_act_crimes+amendment_noresel&p=1&sr=1

120 http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html?search=ts_all%40act%40bill%40regulation_privacy+act_resel&p=1&sr=1

121 http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html?search=ts_act_bill+of+rights+act_resel&sr=1

that all enactments be given such meaning as will ensure consistency with its rights and freedoms. If that cannot be achieved, the NZBORA is subordinate to the inconsistent enactment.[122]

(iii) APEC Privacy Framework (29 October 2004)

As an APEC (Asia-Pacific Economic Cooperation) member economy, New Zealand has been involved in the development of the APEC Privacy Framework, which was adopted in Chile in October 2004.

The APEC Privacy Framework[123] contains nine privacy principles, applies to both private and public sector entities, and offers guidance for its domestic and international implementation. The stated objective of the APEC Privacy Framework is to protect privacy, while avoiding the creation of unnecessary barriers to information flows.

(iv) Memorandum of Understanding between the Office of the Australian Privacy Commissioner and the Office of the New Zealand Privacy Commissioner (4 September 2006)

This non-binding memorandum of understanding between the offices of the Australian and New Zealand Privacy Commissioners provides for bilateral meetings, the sharing of information and cross-border cooperation in investigation and enforcement, among other things. The signatories have undertaken to share information about "common issues, important and significant privacy events, emerging and evolving issues, and experience of and approaches to policy, compliance and promotional activities".[124]

The current memorandum was signed in August 2008 and will remain in force for a term of two years.

(v) Asia Pacific Privacy Authorities Forum

As a member of the Asia Pacific Privacy Authorities Forum, the Privacy Commissioner of New Zealand has resolved to adopt the following statements:

- Statement of Objectives[125] (17 November 2005);
- Statement of Common Administrative Practice: case note citation[126] (17 November 2005); and
- Statement of Common Administrative Practice: case note dissemination[127] (9 December 2006).

These statements focus on the role and administration of privacy authorities, rather than the substantive law in the member jurisdictions.

---

122 *New Zealand Bill of Rights Act 1990*, ss 4, 5 and 6.

123 http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

124 See further paragraphs 8.1 to 8.3 of the MOU, which is accessible here.

125 http://www.privacy.gov.au/aboutus/international/appa#st

126 http://www.privacy.gov.au/aboutus/international/appa#com

127 Accessible here.

Fundamental rights

(i) United Nations: International Covenant on Civil and Political Rights (19 December 1966)

(ii) See paragraph (b) in the 'Data protection' section above.

(iii) ILO Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (17 June 1999)

(iv) New Zealand signed the Worst Forms of Child Labour Convention on 19 November 2000, and ratified it on 14 June 2001. It entered into force on 14 June 2001 also.

(v) Hague Convention on Jurisdiction, Applicable Law, Recognition, Enforcement and Co-operation in Respect of Parental Responsibility and Measures for the Protection of Children (19 October 1996) (Child Protection Convention)

The New Zealand Government has agreed that New Zealand accede to this Convention subsequent to the satisfactory completion of the Parliamentary treaty examination process and the passage of legislation to amend various enactments. The New Zealand Ministry of Foreign Affairs and Trade states that *"changes to existing laws for recognition, enforcement and co-operation with respect to overseas court orders and administrative decisions that fall within the scope of the Convention are likely to be required."*[128]

The Parliamentary treaty examination was completed on 29 July 2010 and a bill to enable accession was expected in 2011. At the time of writing (6 December 2011) no bill has been introduced.

(vi) United Nations: Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices Similar to Slavery (7 September 1956).

New Zealand acceded to this Supplementary Convention on 26 April 1962. The Supplementary Convention also entered into force on the same date.

Money laundering

(i) Financial Action Task Force (1989) (FATF)

New Zealand has been an active member of the FAFT since 1991. The FAFT is a strategic inter-governmental body with the broad purpose of developing international standards for anti-money laundering (**AML**) and to counter the financing of terrorism (**CFT**).[129] The FATF Recommendations on AML/CFT have become the international standard for AML/CFT regulation.

New Zealand achieved partial compliance with the FAFT Recommendations by the enactment of the *Financial Transactions Reporting Act 1996.* Among other things, the Financial Transactions Reporting Act obliges financial institutions to verify the identity of their customers and report suspicious transactions to the Commissioner of Police (see further section 3.5.2 below).

---

128 New Zealand Ministry of Foreign Affairs and Trade, *International Treaties List January 2009, A list of treaties New Zealand is currently involved in negotiating, concluding, ratifying or amending,* p49.

129 Ministry of Justice, *Anti-Money Laundering and Countering the Financing of Terrorism, The Financial Action Task Force (FATF),* see http://www.justice.govt.nz/?came_from=http%253A//www.justice.govt.nz/policy-and-consultation/aml-drop/anti-money-laundering-and-countering-the-financing-of-terrorism/.

New Zealand is partially compliant with the FATF's 9 Special Recommendations relating to terrorist financing. Compliance is primarily achieved through the *Terrorism Suppression Act 2002*. [130] This level of compliance was evaluated as of October 2009. It is important to note that New Zealand's AML-CFT Act (see below) entered into force after that assessment. That Act would increase our compliance with the 9 Special Recommendations as the new legislation addresses areas such as suspicious transaction reporting and wire transfer rules, which were identified as lacking by the October evaluation.

The New Zealand Parliament recently enacted the *Anti Money Laundering and Countering Financing of Terrorism Act 2009* (**AML CFT Act**). This Act supplements the existing obligations of financial institutions to carry out AML CFT activity under the Financial Transactions Reporting Act. The New Zealand Ministry of Justice website states that the AML CFT Act "seeks to bring New Zealand into line" with the international standards set out by the FATF recommendations.[131] The FATF's last assessment of New Zealand's compliance with the 40 recommendations showed a number of non-compliant aspects.[132] However, as noted above, this evaluation was carried out in October 2009, prior to the enactment of the AML CFT Act. There has been no further assessment of New Zealand's compliance since then.

The purpose of the AML CFT Act is to engage the assistance of the financial sector, casinos and other designated persons (natural or legal) in detecting and deterring money laundering and terrorism. Specifically, the Act provides for a set of reporting requirements for "reporting entities", and a regime for the supervision, monitoring and enforcement of AML CFT obligations. There are three supervisors of the new regime: the Reserve Bank of New Zealand, the Securities Commission and the Department of Internal Affairs.

The AML CFT Act as it stands provides for a complete AML CFT system. In some respects, the Act has been intentionally cast at a high level, leaving the detail for secondary legislation, which is better placed to respond to the changing risks that New Zealand faces. These secondary legislative instruments are currently under development and will be the subject of public consultation.

At this stage, only financial institutions, certain financial advisors, trust and company service providers and casinos (as defined in section 4 of the AML CFT Act) are regulated by the Act. Lawyers, conveyancers, accountants, real estate agents and government departments have been excluded from coverage by the AMLCFL (Definitions) Regulations 2011.

(ii) Asia/Pacific Group on Money Laundering (1997) (APG)

New Zealand was a founding member of the APG, which was officially established in February 1997 as part of the FATF's global AML/CFT strategy. To improve the AML/CFT process, members of the APG evaluate each other. The APG meets once a year to discuss these evaluations, technical assistance and training issues, as well as the structure and nature of the APG.[133]

---

130 http://www.legislation.govt.nz/act/public/2002/0034/latest/DLM151491.html?search=ts_act_terrorism_resel&p=1&sr=1.

131 http://www.justice.govt.nz/?came_from=http%253A//www.justice.govt.nz/policy/criminal-justice/archive-put-all-outdated-retracted-material-here-do-not-publish/aml-and-cft/aml-cft-act.

132 The full report and executive summary is http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236963_43998044_1_1_1_1,00.html.

133 Ministry of Justice, *Anti-Money Laundering and Countering the Financing of Terrorism, The Asia Pacific Group on Money Laundering (APG)*, see here.

(iii) United Nations Convention Against Transnational Organised Crime (15 November 2000)

New Zealand signed the Convention Against Transnational Organised Crime on 14 December 2000 and ratified it on 19 July 2002. This Convention entered into force on 29 September 2003.

(iv) United Nations Convention Against Corruption (31 October 2003)

New Zealand signed the United Nations Convention Against Corruption in December 2003. New Zealand is presently working toward ratifying this Convention.

Human trafficking

(i) The Hague Convention on Protection of Children and Co-operation in Respect of Intercountry Adoption (29 May 1993)

New Zealand acceded to the Hague Convention on Protection of Children Convention on 18 September 1998. This Convention entered into force on 1 January 1999.

(ii) Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, supplementing the United Nations Convention Against Transnational Organised Crime (15 November 2000)

New Zealand signed this Protocol on 14 December 2000, and ratified it on 19 July 2002. The Protocol entered into force on 25 December 2003.

(iii) Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime (15 November 2000)

New Zealand signed this Protocol on 14 December 2000, and ratified it on 19 July 2002. The Protocol entered into force on 28 January 2004.

(iv) United Nations International Convention for the Suppression of the Traffic in Women and Children (30 September 1921)

New Zealand signed this Convention on 1 October 1921, and it was ratified on behalf of New Zealand on 28 June 1922. The Convention entered into force on 28 June 1922 also.

Evidence

(i) Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (18 March 1970)

It is expected that no further legislation will be needed in order for New Zealand to accede to this Convention; the provisions of the *Evidence Act 2006*[134] are considered sufficient.

E-Commerce

(i) United Nations Convention on the Use of Electronic Communications in International Contracts (23 November 2005)

[134]http://www.legislation.govt.nz/act/public/2006/0069/latest/DLM393463.html?search=ts_act_evidence_resel&p=1&sr=1.

No further information on the likelihood of, or timeline for, signature is publicly available at the time of writing.

It is expected that amendments to the *Electronic Transactions Act 2002*[135] will need to be enacted in order for New Zealand to sign this Convention.

(ii) UNCITRAL Model Law on Electronic Commerce (adopted by the United Nations Commission on International Trade Law on 16 December 1996)

New Zealand is currently considering signing the Convention.[136] This would require amendments to the *Electronic Transactions Act 2002*.

That said, New Zealand's *Electronic Transactions Act* already draws on the UNCITRAL Model Law. The explanatory note to the bill that became the *Electronic Transactions Act 2002* states that the legislation closely follows the Model Law on Electronic Commerce. More specifically, section 6 of the *Electronic Transactions Act 2002* provides that the Model Law and any UNCITRAL document relating to the Model Law may be referred to in interpreting the *Electronic Transactions Act 2002*.

2.2 Relevance of international legal instruments to New Zealand's domestic law

The New Zealand Courts have adopted a dualist approach to the reception of international treaty law: rules contained within a treaty cannot be applied by New Zealand Courts unless they are first incorporated by statute.[137]

However, there is also a presumption of statutory interpretation that domestic legislation should be read in a way that is consistent with New Zealand's international obligations, in so far as the wording of domestic legislation allows.[138] The New Zealand Court of Appeal has gone so far as to say that this presumption of statutory interpretation "may apply whether or not the legislation was enacted with the purpose of implementing the relevant [international] text".[139]

Furthermore, it has been established that unincorporated treaty obligations may, and in some limited circumstances must, be taken into account by persons exercising statutory powers of decision.[140]

The real force of unincorporated international instruments in domestic law is difficult to estimate. This is because such instruments may be accounted for under either the presumption of consistency, in which the courts will presume that Parliament did not intend to legislate contrary to the country's international obligations, or as mandatory considerations, which decision-makers must have regard to.

The former model is outcome focused, requiring the decision-maker to reach a result that is substantively consistent with the relevant international obligation. The latter model, on the other hand, affects only the way in which the decision-making process is carried out. Parliamentary supremacy is

---

135 http://www.legislation.govt.nz/act/public/2002/0035/latest/DLM154185.html?search=ts_act_electronic+transactions_resel&p=1&sr=1.

136 New Zealand Ministry of Foreign Affairs & Trade, *Treaties and International Law – International Treaties List as at January 2009 – 55. UNCITRAL Model Law on Electronic Commerce*.

137 Attorney-General for Canada v Attorney-General for Ontario *[1937] AC 326*, *cited with approval in* New Zealand Air Line Pilots' Association Inc v Attorney-General *[1997] 3 NZLR 269 at 279 (CA).*

138 *Rajan v Minister of Immigration* [1996] 3 NZLR 543 at p 551, cited with approval in New Zealand Air Line Pilots' Association Inc v Attorney-General *[1997] 3 NZLR 269 at 289(CA).*

139 New Zealand Air Line Pilots' Association Inc v Attorney-General *[1997] 3 NZLR 269 at 289 (CA).*

140 Paul Rishworth et al, *The New Zealand Bill of Rights*, p15. For example, Immigration Departmental Guidelines now mandate consideration of international human rights protections when key decisions are being made as to a person's immigration status.

maintained under either option, however, as international obligations will be overridden by clear parliamentary language or an inconsistent statutory scheme.[141]

2.3 Questions and Answers relevant to the APAC Coalition

Please note: The following advice proceeds on the assumption that all of the relevant acts take place in New Zealand and are thereby regulated by New Zealand law. Where some acts take place outside New Zealand, closer consideration will need to be given to whether the relevant conduct is regulated by New Zealand law.

(a) Are there laws specifically addressing child pornography in New Zealand?

New Zealand's *Films, Videos, and Publications Classification Act 1993* (**Classification Act**)[142] regulates dealings in child pornography. The Classification Act contains a general ban on dealings in objectionable publications, as well as extraterritorial and extradition provisions that refer specifically to the defined term 'child pornography'.

(b) What is the definition of illegal child pornography in New Zealand?

'Child pornography' is defined in section 145A of the Classification Act to mean:

(i) *a representation, by any means, of a person who is or appears to be under 18 years of age engaged in real or simulated explicit sexual activities; or*

(ii) *a representation of the sexual parts of a person of that kind for primarily sexual purposes.*

However, this definition of 'child pornography' is only relevant to two provisions of the Classification Act that address the extraterritorial application of the Act and extradition arrangements (sections 145A and 145C). These provisions were specifically enacted to implement New Zealand's obligations under the Optional Protocol on the Sale of Child Pornography.

So, to fall within the scope of the Classification Act's general ban on dealings in objectionable publications, child pornography images or videos must constitute a "publication" that is "objectionable" within the meaning of the Classification Act. Numerous Courts in New Zealand have held that child pornography materials are objectionable publications prohibited by the Classification Act.[143]

(c) Are there legal obstacles to the undertaking of a test or an undercover transaction by a law enforcement agency on behalf of the national hotline to the Offender's account?

While the New Zealand Courts have acknowledged the practice of law enforcement agencies (and for that matter, private individuals) undertaking undercover transactions, we are not aware of any arrangements pursuant to which law enforcement agencies have agreed to conduct undercover transactions *on behalf of* private organisations. Such an arrangement will need to be the subject of discussions with the law enforcement agencies concerned. In these discussions it might assist ICMEC that New Zealand's *Policing Act 2008* acknowledges the role of private sector bodies in assisting the Police in the performance of their roles.[144]

---

141 See Claudia Geiringer "Tavita and all that: Confronting the Confusion Surrounding Unincorporated Treaties and Administrative Law" (2004) 21 NZULR 66.

142 http://www.legislation.govt.nz/act/public/1993/0094/latest/DLM312895.html?search=ts_act_films+videos_resel&p=1&sr=1.

143 See, for example, *Kellet v Police* (2005) 21 CRNZ 743; *Department of Internal Affairs v Young* [2004] DCR 231; *Meyrick v Police* (High Court Hamilton, 31 July 2007, Nicholson J, CRI-2005-419-000058).

144 *Policing Act 2008*, s 10.

From a Classification Act perspective, it is likely that whenever a person (including a law enforcement officer) conducts a test or undercover transaction using an Offender's Site, that person will possess child pornography material – at least on a temporary basis – and will thereby commit a possession offence under the Classification Act. A tester might also commit the offences of distributing an objectionable publication or making a copy of an objectionable publication for distribution to another, depending on what the tester does with the child pornography images or videos.

However, if the person conducting the test or undercover transaction is an official named in section 131(4) of the Classification Act (such as the Chief Censor or a Deputy Censor, a classification officer, any Inspector of Publications, any member of the Police, or a person in the service of the Crown) (each a **named official**),[145] the official will not face Classification Act liability for conducting the test or undercover transaction (provided that the test or undercover transaction is carried out for the purpose of or in connection with that person's official duties). This is because there are exceptions to liability in sections 131 and 124A of the Classification Act that can be relied on by named officials who deal with objectionable publications for the purpose of, and in connection with, their official duties. These exceptions are discussed further in section 3.1.2 of this paper.

The concept of a "person in the service of the Crown" is not defined in primary legislation[146] or case law. However, on a plain and ordinary reading, we expect it would have a broad meaning not affected by the usual employment law distinction between a "contract *of* service" and a "contract *for* services". On this basis, if an understanding is reached between the Coalition and the Crown as to the conduct of the Coalition, it would be worthwhile for a memorandum of understanding or other document recording any such understanding to make it clear that ICMEC and its representatives are to be considered "persons in the service of the Crown" for the purposes of the Classification Act defences.

(d) Are there legal obstacles to the undertaking of a test or an undercover transaction by (for example, a credit card company or an online payments facilitator) on behalf of the national hotline to the Offender's account?

There is no rule of law in New Zealand requiring investigations underlying criminal proceedings to be undertaken by law enforcement.[147] Criminal cases have been successfully prosecuted in circumstances where undercover private investigators have gathered the relevant evidence.[148] That said, the conduct of undercover agents – whether undercover police officers, police informants[149] or private individuals – is subject to scrutiny by the Courts. So, for example, it has been accepted that in some cases the actions of law enforcement agents in generating the offending may be such as to justify the exclusion of any evidence derived from the entrapment. The New Zealand Court of Appeal has confirmed that similar considerations apply to the conduct of private individuals acting as undercover agents:

"[t]he fact that Mr Smith is a private individual and not an agent of the State is not inconsistent with the jurisdiction to exclude his evidence if a prosecution based on that evidence could fairly be described as being an abuse of process or an affront to public conscience."[150]

---

145 For the complete list of named officials, see section 131(4) of the *Films, Videos, and Publications Classification Act 1993*.

146 The only recorded definition of this phrase is in the *Rules Relating to the Acceptance and Wearing of Commonwealth, Foreign and International Honours by New Zealand Citizens*. Under these Rules, "a person in the service of the Crown" includes "persons in the service of the Crown on a temporary, part time or contract basis."

147 *R v Dawson* (2004) 2 NZELR 126 at [17]

148 See for example, *R v Karalus* (2005) 21 CRNZ 718

149 By police informants, we mean those who participate in the offending (or on the edge of the offending) at the instigation and under the supervision of police: see *R v Karalus* (2005) 21 CRNZ at [38]

150 *R v Karalus* (2005) 21 CRNZ 728, at 741.

For the reasons given in section 2.3 above, it is likely that representatives of entities other than law enforcement agencies (**civilian testers**) will commit one or more Classification Act offences when they undertake a test or undercover transaction on the Offender's Site.

Nevertheless, civilian testers might be able to rely on the defences under the Classification Act. In the first instance, civilian testers might be able to demonstrate that they committed the acts *prima facie* constituting distribution offences[151] for an 'approved purpose' under section 131(5) of the Classification Act, such as for the purpose of, or with the intention of, delivering the objectionable publication into the possession of a person lawfully entitled to have possession of it. Civilian testers might also be able to rely on the more general defence to liability under sections 131 and 131A of the Classification Act that he or she had "lawful authority or excuse" to be in possession of the objectionable publication.

From a general criminal law perspective, there is a risk that by conducting an undercover transaction on the Offender's Site, civilian testers might face liability as secondary parties to the Classification Act offences committed by the Offender in supplying or distributing the objectionable publication in question. Although we consider that the practical risk of prosecution in these circumstances is relatively remote, to eliminate the risk of liability for ICMEC and APAC Coalition Members altogether, we recommend that undercover transactions only be undertaken by or with the authorisation of law enforcement officers or by the named officials identified in s131(4) of the Classification Act.

(e) Are there legal obstacles to the collaboration of APAC Coalition Members in relation to the test or the undercover transaction?

The existence of legal obstacles to the collaboration of APAC Coalition Members in performing a test or undercover transaction depends on the nature of that collaboration.

Information sharing among APAC Coalition Members will be restricted by:

(i) the provisions of the Privacy Act (which apply only to information about identifiable individuals, not information about corporate legal persons); and

(ii) the confidentiality obligations that APAC Coalition Members are likely to be bound by.

These restrictions are considered in paragraph 2.6 below insofar as they relate to the disclosure by APAC Coalition Members of the identity of their client to ICMEC, the other APAC Coalition Members and law enforcement agencies. We also discuss in paragraph 3.2.2 below the way in which the Privacy Act regulates the transfer of personal information outside New Zealand.

APAC Coalition Members may also collaborate to fund the activities of the Coalition. It is theoretically possible, though far from certain, that APAC Coalition Members who contribute funds for the purchase of illegal child pornography could face liability as secondary parties to the Classification Act offences committed by the Offender in supplying the illegal material. Whether or not such liability accrues is a highly fact dependent enquiry that cannot be conducted in the abstract. We anticipate that it will often be difficult to establish that the Coalition Member had the requisite mens rea (state of mind) in order to attract secondary liability. The requisite mens rea is generally described as an intention to help or encourage the principal party to do the acts that constitute the offence. To remove any doubt, we recommend that ICMEC discusses the proposed funding

[151] By distribution offences, we mean the offences of (i) distributing a publication; (ii) making a copy of a publication for the purposes of distribution to any other person; and (iii) possessing a publication for the purposes of distribution to any other person.

arrangements for the APAC Coalition with law enforcement authorities prior to implementing the framework in New Zealand.

(f) Are there legal obstacles to the disclosure by the APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC, the other APAC Coalition Members and the public prosecutor?

The duty of confidence that New Zealand banks and financial institutions owe to their customers is likely to pose an obstacle to the proposed disclosure by APAC Coalition Members unless the disclosing APAC Coalition Member obtains its customers' informed, express consent to the same.

There may be instances where the proposed disclosure is required by law, such as where the transaction is relevant to the enforcement of the *Criminal Proceeds (Recovery) Act 2009* [152] or under the *Financial Transactions Reporting Act 1996*. Disclosures that are required by law do not constitute a breach of the duty of confidence bankers owe to their customers. However, statutory obligations to disclose are likely to be of limited assistance in facilitating the disclosures contemplated under the APAC Coalition framework, not least because they do not generally contemplate the broad disclosure to ICMEC and fellow Coalition Members that the APAC Coalition framework contemplates.

The key Privacy Act provisions that APAC Coalition Members will need to be mindful of when disclosing the identity of individual account holders will be Principle 11 (non-disclosure rule) and Principle 8 (accuracy of personal information to be checked before use). Neither of these principles is likely to present an insurmountable obstacle to the proposed disclosure, but it will be necessary for APAC Coalition Members to develop compliance systems to ensure adherence to them. So for example, it is likely that most APAC Coalition Members will need to rely on the 'authorisation' exception to Principle 11 to justify the disclosure of individual account holder identities, and will therefore need to obtain (and maintain) the informed, express authorisation of their customers to the proposed disclosure.

(g) Are there legal obstacles to the termination of the provision of services to the Offender by APAC Coalition Members?

The question of whether a Coalition Member can terminate a customer contract as contemplated by the APAC Coalition framework will turn on the construction of the relevant contract and the application of New Zealand's *Contractual Remedies Act 1979*. Each Coalition Member will need to separately assess their position vis-à-vis the particular customer concerned.

It is preferable that each APAC Coalition Member includes an express term in its customer contracts empowering the Member to terminate services provided to a customer upon the Member holding a suspicion that the customer's account has been used to receive monies for unlawful activities. Care needs to be taken in drafting any such terms so that an APAC Coalition Member can safely rely on the terms in circumstances where its suspicion may not be reasonably held, and/or the child pornography material in question turns out not to be an objectionable publication within the meaning of the Classification Act.

2.4 Domestic Legal Framework

Please note: The following advice proceeds on the assumption that all of the relevant acts take place in New Zealand and are thereby regulated by New Zealand law. Where some acts take place outside

---

152 http://www.legislation.govt.nz/act/public/2009/0008/latest/DLM1451001.html?search=ts_act_criminal+proceeds_resel&p=1&sr=1.

New Zealand, closer consideration will need to be given to whether the relevant conduct is regulated by New Zealand law.

(a) Definition of illegal child pornography

The legal framework

The Classification Act contains a general ban on dealings with objectionable publications, as well as extraterritorial and extradition provisions that refer specifically to the defined term 'child pornography'.

'Child pornography' is defined in section 145A of the Classification Act to mean:

(i) a representation, by any means, of a person who is or appears to be under 18 years of age engaged in real or simulated explicit sexual activities; or

(ii) a representation of the sexual parts of a person of that kind for primarily sexual purposes.

However, this definition of 'child pornography' is only relevant to two provisions of the Classification Act that address the extraterritorial application of the Act and extradition arrangements (sections 145A and 145C). These provisions were specifically enacted to implement New Zealand's obligations under the Optional Protocol on the Sale of Child Pornography.

So, to fall within the scope of the Classification Act's general ban on dealings in objectionable publications, child pornography images or videos must constitute a "publication" that is "objectionable" within the meaning of the Classification Act. The Classification Act deems certain publications to be objectionable, including any publication that promotes or supports, or tends to promote or support, the exploitation of children, or young persons, or both, for sexual purposes. Neither of the terms 'children' or 'young persons' are defined in the Classification Act, but the Court of Appeal considers that this is deliberately so, given the scheme of the Act. Numerous Courts in New Zealand have held that child pornography materials are objectionable publications prohibited by the Classification Act.[153]

The Classification Act's definition of "publication"[154] is broad and encompasses any writing, drawing, photograph, sound recording and film. It specifically includes recorded or stored "things" (including, but not limited to, a disc or an electronic computer file) that are capable of electronic retrieval.

A publication is "objectionable" under the Classification Act if it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good. [155]

The purposive deeming provision in the Classification Act's definition of "objectionable", coupled with the absence of any statutory age restriction, means that New Zealand's Classification Act is likely to cover a broad range of materials depicting the sexual exploitation of children, including works of fiction, cartoons and images depicting sexualised nudity.

It is an offence under the Classification Act to:[156]

---

153 See, for example, *Kellet v Police* (2005) 21 CRNZ 743 in which the objectionable material comprised stories and images depicting children having sexual relations with others and children posing sexually provocatively; *Department of Internal Affairs v Young* [2004] DCR 231; *Meyrick v Police* (High Court Hamilton, 31 July 2007, Nicholson J, CRI-2005-419-000058) in which the objectionable material comprised children depicted in various stages of undress and in sexually provocative poses.

154 *Films, Videos, and Publications Classification Act 1993*, s 2.

155 *Films, Videos, and Publications Classification Act 1993*, s 3(1).

156 *Films, Videos, and Publications Classification Act 1993*, s 123(1).

- make an objectionable publication; [157]

- make a copy of, import into New Zealand or possess an objectionable publication, for the purposes of supply or distribution to any other person;

- supply or distribute an objectionable publication; and

- display or exhibit an objectionable publication to any other person in exchange for payment or other benefit.

Each of these offences is a strict liability offence; it is not a defence that the Offender had no knowledge or reasonable cause to believe that the publication was objectionable.[158] Individual offenders are liable to a fine of up to NZD$10,000; body corporate offenders are liable to a fine of up to NZD$30,000.[159]

The Classification Act also includes more serious knowledge-based offences that involve the acts described in paragraphs (a) to (d) above.[160] These knowledge-based offences attract higher sanctions, including periods of imprisonment (of up to 10 years) in the case of individual offenders.[161]

The Classification Act separately criminalises the mere possession of an objectionable publication without lawful authority or excuse. The strict liability version of this offence[162] is punishable by a fine of up to NZD$2,000 in the case of an individual and NZD$5,000 in the case of a body corporate. The knowledge-based version of this offence[163] attracts higher sanctions, including periods of imprisonment (of up to 5 years) in the case of individual offenders.

When determining the sentence for a person found guilty of one of the Classification Act's knowledge-based offences, the Courts must take into account as an aggravating factor the extent to which the offending publication:[164]

(i) promotes, supports or tends to promote or support the sexual exploitation of children or young persons;

(ii) describes, depicts or otherwise deals with sexual conduct with or by children or young persons; and

(iii) exploits the nudity of children and/or young persons.

Finally, section 138 of the Classification Act regulates the liability of employers and principals for the illegal actions of their employees and agents. Illegal action is defined in section 138(1) to mean the supply, distribution, display, exhibition, advertisement, or making available of an objectionable publication contrary to the provisions of the Classification Act.

---

157 In *Kellet v Police* (2005) 21 CRNZ 743 at 748, it was held that "making an objectionable publication" under s 123(1)(a) requires some element of compilation or creativity beyond simple copying. A change in medium, or the fact that something new is brought into existence, or the fact that the source of the publication is pre-existing, will not necessarily be decisive in every case.

158 *Films, Videos, and Publications Classification Act 1993*, s 123(3).

159 *Films, Videos, and Publications Classification Act 1993*, s 123(2).

160 *Films, Videos, and Publications Classification Act 1993*, s 124(1).

161 *Films, Videos, and Publications Classification Act 1993*, s 124(2).

162 *Films, Videos, and Publications Classification Act 1993*, s 131(1).

163 *Films, Videos, and Publications Classification Act 1993*, s 131A.

164 *Films, Videos, and Publications Classification Act 1993*, s 132A.

In the case of an employee,[165] section 138(2) provides that an employer will be held responsible for the illegal action of an employee where the action is done in his or her capacity as an employee, and whether or not the illegal action was done with the employer's knowledge or approval.

However, it is a defence under section 138(4) of the Classification Act for an employer to prove that he or she took such steps as were reasonably practicable to prevent the employee from doing that illegal action or from doing acts of a class, category, or description that includes illegal actions.[166]

Similarly, directors and managers will sometimes be taken to be guilty of offences for which their bodies corporate have been convicted.[167]

Companies and other corporate entities can face criminal liability for certain offences in New Zealand, including the Classification Act offences discussed above.

Application to the present case

Will the tester commit a Classification Act offence by conducting an undercover transaction using the Offender's Site?

Whenever a person conducts a test or undercover transaction using an Offender's Site, it is likely that that person will possess child pornography material, if only on a temporary basis. This is because, in the usual operation of the Internet, temporary copies of material accessed online are made on a user's computer as part of the download process. The tester may also elect to retain a more permanent copy of the image as part of the evidence gathering process.

Even where no temporary copy of material accessed online is made, the tester may still be in possession of an objectionable publication within the meaning of section 131 of the Classification Act. In *Department of Internal Affairs v Young*,[168] the defendant was held to be in possession of objectionable images as a result of deliberately downloading those images from the Internet in the full knowledge of the nature of the material and to the intent that it may be displayed on the computer screen.[169] It was immaterial in that case that the defendant was not aware that by engaging in the download process that some of the images would be saved to the hard drive.[170]

See further the discussion below for the defences that might be available to testers.

Having regard to the vicarious liability provisions in the Classification Act, it is possible that both the tester and the tester's employer or principal (i.e. ICMEC or an APAC Coalition Member) or their directors or managers will be taken to have committed the illegal acts.

Are there any defences available to a tester who might commit a Classification Act offence in the course of conducting an undercover transaction using the Offender's Site?

The answer to this question depends on the identity of the tester and the purpose for which the tester does the acts that are regulated by the Classification Act.

---

165 We note that s 138 also addresses the liability of principals for the actions of their agents.

166 *Films, Videos, and Publications Classification Act 1993*, s 138(4).

167 *Films, Videos, and Publications Classification Act 1993*, s 139.

168 [2004] DCR 231.

169 *Department of Internal Affairs v Young* [2004] DCR 231.

170 *Department of Internal Affairs v Young* [2004] DCR 231, paragraph [4].

As discussed above, If the person conducting the test or undercover transaction is an official named in section 131(4) of the Classification Act (such as the Chief Censor or a Deputy Censor, a classification officer, any member of the Police, or a person in the service of the Crown) (each a **named official**), the official will not face Classification Act liability for conducting the test or undercover transaction. This is because there are several exceptions to liability in sections 131 and 124A of the Classification Act that can be relied on by named officials who deal with objectionable publications for the purpose of, and in connection with, their official duties.

Specifically, section 131(4) provides that it is not an offence for any of the following named officials to be in possession of an objectionable publication, where such possession is for the purpose of, and in connection with, the person's official duties:

(i) The Chief Censor;

(ii) The Deputy Chief Censor;

(iii) Any classification officer;

(iv) Any person holding office pursuant to clause 2 of Schedule 1 to this Act (being Classification Office staff);

(v) Any member of the Board;

(vi) The labelling body or any person who is carrying out the functions of the labelling body;

(vii) Any Inspector;

(viii) Any member of the Police;

(ix) Any officer of the Customs;

(x) Any Judge of the High Court, or District Court Judge, Coroner, Justice, or Community Magistrate;

(xi) In relation to any publication delivered to the National Librarian pursuant to Part 4 of the National Library of New Zealand (Te Puna Matauranga o Aotearoa) Act 2003, the National Librarian, any other employee of the National Library Department, or any person employed in the Parliamentary Library; and

(xii) Any other person in the service of the Crown.

Section 124A(1) further provides that nothing in section 123 (strict liability offences in relation to objectionable publications) or section 124 (knowledge-based offences in relation to objectionable publications) makes it an offence for a named official to do any or all of the following things for the purpose of, and in connection with, his or her official duties:

(i) import a publication into New Zealand (whether with the involvement of an overseas official or not);

(ii) export a publication from New Zealand to an overseas official;

(iii) distribute a publication to a named official if that person takes possession of the publication for the purpose of, and in connection with, his or her official duties;

(iv) make a copy of a publication for the purposes of distribution of the kind specified in paragraph (iii);

(v) be in possession of a publication for the purposes of distribution of the kind specified in paragraph (iii).

It is important to note, however, that the Classification Act does not excuse named officials from all types of liability under the Classification Act. So, for example, there is no exception to liability for the offences of:

- in expectation of payment or otherwise for gain, or by way of advertisement, displaying or exhibiting an objectionable publication to any other person.

We turn now to consider the situation where the person conducting the test is a representative of ICMEC or an APAC Coalition Member.

Under section 124A of the Classification Act, it is a defence to a charge under section 123 (strict liability offence) or section 124 (knowledge-based offences) that the defendant:

(i) distributed a publication;

(ii) made a copy of a publication for the purposes of distribution to any other person; or

(iii) possessed a publication for the purposes of distribution to any other person,

if the defendant proves that he or she did so, in good faith, for an approved purpose under section 131(5). The approved purposes under section 131(5) are:

(i) For the purpose or with the intention of delivering it into the possession of a person lawfully entitled to have possession of it; or

(ii) For the purposes of any proceedings under this Act or any other enactment in relation to the publication; or

(iii) For the purpose of giving legal advice in relation to the publication; or

(iv) For the purposes of giving legal advice, or making representations, in relation to any proceedings; or

(v) In accordance with, or for the purpose of, complying with any decision or order made in relation to the publication by the Chief Censor, the Classification Office, the Board, or any court, Judge, Justice, or Community Magistrate; or

(vi) In connection with the delivery of the publication to the National Librarian in accordance with Part 4 of the National Library of New Zealand (Te Puna Matauranga o Aotearoa) Act 2003.

The approved purposes in paragraphs (a) and (b) above are most relevant to the present fact scenario.

It is also a defence to the mere possession offences in sections 131 (strict liability offence) and 131A (knowledge-based offence) of the Classification Act for the defendant to prove that they possessed the objectionable publication, in good faith, for an approved purpose under section 131(5) of the Classification Act (as set out above). Alternatively, a tester could seek to rely on the more general defence to liability under sections 131 and 131A of the Classification Act that he or she had to be in possession of the objectionable publication. The concept of "lawful authority or excuse" is not defined

in the Classification Act. However, it is a phrase that appears in a number of sections of New Zealand's Crimes Act 1961. A leading criminal law commentary in New Zealand (Adams on Criminal Law) describes the concept as follows:[171]

The concept of "lawful authority" relates to something where there is some statutory or common law rule entitling a person to have the item in his or her possession; lawful excuse is more likely to apply to cases where the purpose for which the item is possessed is to further some lawful activity or enterprise.

It would be prudent for ICMEC and each APAC Coalition Member that intends to rely on these defences to develop compliance systems to ensure that they are well-placed to successfully demonstrate how they fall within the bounds of these defences.

It might also be worthwhile exploring whether ICMEC or its representatives can qualify as a "person in the service of the Crown". This would permit ICMEC or its representatives to rely on the Classification Act defences that are specific to named officials.

(b) Privacy and data protection rules

The legal framework

(i) Data protection

New Zealand's *Privacy Act 1993*[172] establishes a personal information protection regime that applies broadly to private and public sector organisations. There are no separate data privacy rules that apply to information about corporate legal persons which is a key constraint on the scope of the Privacy Act's application.

The Privacy Act defines "personal information" as "information about any identifiable individual".[173] This definition is cast in broad terms and has been interpreted widely.

An "agency" is "any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector" except for certain excluded persons not relevant to the present case.[174]

The Privacy Act contains 12 information privacy principles,[175] which all agencies must comply with. The principles can be summarised as follows:

Principle 1: Purpose of collection of personal information

Agencies must not collect personal information unless the information is collected for a lawful purpose connected with a function or activity of the agency, and the collection of personal information is necessary for that purpose.

Principle 2: Source of personal information

171 *Adams on Criminal Law*, CA233.01.

172 http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html .

173 *Privacy Act 1993*, s 2(1). The definition of 'personal information' also specifically includes "information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995."

174 *Privacy Act 1993*, s 2(1).

175 *Privacy Act 1993*, s 6.

Agencies must collect personal information directly from the data subject, except in certain cases.

Principle 3: Collection of personal information from subject

When personal information is collected directly from the data subject, agencies must take reasonable steps to ensure that the data subject is aware of certain matters.

Principle 4: Manner of collection of personal information

Agencies must not collect personal information by means that are unlawful, unfair or that intrude to an unreasonable extent on the personal affairs of the individual concerned.

Principle 5: Storage and security of personal information

Agencies must use reasonable security safeguards to protect personal information they hold against loss, unauthorised access, use, modification or disclosure, or other misuse. Where an agency gives personal information to a service provider, the agency must do everything reasonably within its power to prevent the unauthorised use or disclosure of the information.

Principle 6: Access to personal information

Data subjects are entitled to access personal information that is held by an agency unless there is a good reason for refusing access to personal information (see Part IV of the Privacy Act), and subject to compliance with the procedural provisions relating to access to and correction of personal information (see Part V of the Privacy Act).

Principle 7: Correction of personal information

Data subjects are entitled to request correction of personal information held by an agency.

Principle 8: Accuracy, etc, of personal information to be checked before use

Agencies that hold personal information shall not use that information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading, having regard to the purpose for which the information is proposed to be used.

Principle 9: Agency not to keep personal information for longer than is necessary

Principle 10: Limits on use of personal information

Personal information obtained for one purpose must not be used for any other purpose, except in limited circumstances.

Principle 11: Limits on disclosure of personal information

Generally, agencies must not disclose personal information unless the disclosure is one of the purposes for which the information was collected or disclosure is permitted on the basis of one of the other permitted grounds for disclosure set out in Principle 11.

Principle 12: Unique identifiers

Agencies must only assign unique identifiers to individuals in certain limited circumstances. Agencies must not require individuals to disclose any unique identifiers unless disclosure is for a purpose (or is directly related to a purpose) for which the unique identifier was assigned.

While the territorial effect of New Zealand's Privacy Act is generally confined to the handling of personal information by agencies in New Zealand, section 10 of the Privacy Act provides for extended jurisdiction in certain limited circumstances. For example, for the purposes of the use and disclosure principles (Principles 10 and 11 respectively), information held by an agency includes information that is held outside New Zealand by that agency, where that information has been transferred out of New Zealand by that agency or another agency.

The Privacy Act does not confer legal rights on individuals that are enforceable in a court of law, except where an individual seeks to exercise his or her access right in respect of personal information held by a public sector agency.[176]

Instead, the Privacy Act's information privacy principles are enforceable via the Privacy Act's complaints procedure. Where a complaint is made to the Privacy Commissioner, the Privacy Commissioner may investigate the complaint and if having done so determines that the complaint has substance, the Privacy Commissioner is required to use best endeavours to try to secure a settlement between the parties. If a settlement cannot be reached, the Privacy Commissioner may refer the matter to the Director of Human Rights Proceedings who will decide whether proceedings should be instituted before the Human Rights Review Tribunal. An aggrieved individual is also entitled to bring the matter before the Human Rights Review Tribunal, provided that the complaint has already been considered by the Privacy Commissioner. There is a right of appeal from the Human Rights Review Tribunal to the High Court of New Zealand.

It is important to note that because alleged contraventions of the Privacy Act are generally resolved at the Privacy Commissioner stage, many of the provisions that underpin the Privacy Act are yet to be tested in the New Zealand courts.

(ii) Common law tort of invasion of privacy

The New Zealand Court of Appeal has (by majority decision) recently given recognition to a tort of invasion of privacy. Previously there had been some doubt as to the existence of the tort in New Zealand. The two elements that are generally accepted as needing to be satisfied for the tort to be established are as follows:[177]

(A) the existence of facts in respect of which there is a reasonable expectation of privacy; and

(B) publicity given to those private facts that will be considered highly offensive to an objective reasonable person.

There is a defence enabling publication to be justified by legitimate public concern in the information.

New Zealand's tort of invasion of privacy is still in its infancy and its bounds remain unclear. Cases applying such a tort have arisen less than once a year since its recognition. It has yet to be decided whether:

176 *Privacy Act 1993*, s 11.

177 *Hosking v Runting* [2005] 1 NZLR 1.

- the tort protects corporations as well as natural persons[178];
- there are defences other than public concern; and
- there are remedies other than an injunction or damages.

The tort was one of the issues considered by the New Zealand Law Commission in its review of the law of privacy completed in 2011. The Commission recommended that the development of the tort continue to be left to the common law. The government has yet to respond to the Commission's recommendations[179]

Since the present case does not squarely engage the tort as currently articulated, we do not propose to consider the tort further in this advice.

Application to the present case

(i) Scope of our advice

The Privacy Act's information privacy principles will regulate each collection, use and disclosure of personal information that occurs as part of the proposed operation of the APAC Coalition. The case study set out in the Report contemplates numerous acts of collection, use and disclosure, each done by the various stakeholders involved in the Coalition.

In order to consider the position of each of ICMEC, APAC Coalition Members and the public prosecutor under New Zealand privacy laws, we would need to be able to analyse each of the acts of collection, use and disclosure contemplated by the case study, so as to be able to form a view as to the extent to which the Privacy Act presents any obstacles to the operation of the APAC Coalition.

Our analysis of the application of the privacy principles contained in New Zealand's Privacy Act in this paper is limited to the particular question of whether there are any legal obstacles to the disclosure by APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC, the other APAC Coalition Members and the public prosecutor (the **disclosure question**).

It is important to remember that from a data privacy perspective, ICMEC only needs to be concerned about every disclosure of information about natural persons and not disclosure about a corporation or other legal entity.

(ii) Advice

The relevant Privacy Act provisions

"Disclosure" is defined as the making available of information to the public in general or to limited classes of people (as contemplated by the Coalition).[180]

From a Privacy Act perspective, the disclosure question principally falls to be decided under Principle 11, which regulates the disclosure of personal information. Principle 8 (accuracy etc. of personal information to be checked before use) is also relevant, as is section 7, which is the savings provision of the Privacy Act.

---

178 Although this is unlikely given the Australian decision of *ABC v Lenah Game Meats Pty Ltd* 185 ALR 1 (HCA).

179 http://www.lawcom.govt.nz/project/review-privacy.

180 Spiller, Peter *Butterworths New Zealand Law Dictionary* (6th ed, LexisNexis NZ Ltd, Wellington, 2005).

We also briefly discuss Principles 2 and 10.[181] Principle 2 is relevant to the collection of account holder personal information by the persons to whom it is disclosed. Principle 10 is relevant to the use of account holder personal information to relate a particular transaction to an account holder and thereby pinpoint the individual whose identity the relevant APAC Coalition Member proposes to disclose to law enforcement, ICMEC and fellow APAC Coalition Members.

Which personal information is being disclosed?

The information that APAC Coalition Members propose to disclose will include at least the identity of the account holder(s). Other information about account holders may also be disclosed, including the relevant account holder's address, other contact details and perhaps even activity on the relevant account holder's account. An individual's identity and contact details are undoubtedly personal information within the meaning of the Privacy Act; activity on an account holder's account will typically constitute personal information too.

To whom will the personal information be disclosed?

The disclosure question posed in the Report contemplates disclosure by an APAC Coalition Member to ICMEC, the other APAC Coalition Members and the public prosecutor.

In New Zealand, the appropriate law enforcement authority for APAC Coalition Members to disclose account holder details to will ordinarily be the Censorship Compliance Unit of the Department of Internal Affairs or the Police. While both the Censorship Compliance Unit and the Police are empowered to investigate and prosecute contraventions of the Classification Act, the Censorship Compliance Unit appears to take the lead role in most cases. The Censorship Compliance Unit's practice is to involve the Police where there is any danger or suspicion of child abuse.[182] Both the Police and the Department of Internal Affairs (the Government department of which the Censorship Compliance Unit forms part) are 'public sector agencies' within the meaning of the Privacy Act. Public sector agencies are in turn a subset of 'agencies' required to comply with the legislation.

Is the disclosure permitted on the basis of one of the permitted grounds for disclosure in Principle 11?

Under Principle 11, an agency that holds personal information may not disclose that information unless the agency believes, on reasonable grounds, that the disclosure falls within one of the specified permitted grounds for disclosure. We discuss the grounds we consider to be most relevant to the APAC Coalition below.

Principle 11(a) – Disclosure for a purpose (or directly related to a purpose) in connection with which the information was obtained

Disclosure of personal information is permitted where the disclosure is one of the purposes, or is directly related to the purposes, in connection with which the information was obtained.[183]

---

181 While there is an argument that disclosure is one form of use of personal information (which is separately regulated by Principle 10), in practice, both the Privacy Commissioner and the Tribunal have opted to deal with every case of disclosure under Principle 11 rather than Principle 10. *Brookers Human Rights Law*, PR3.11.

182 Mr Paul Duke, Department of Internal Affairs, "New Zealand Censorship Compliance Unit", accessible here.

183 Principle 11(a).

This permitted ground of disclosure applies to the situation where disclosure was always intended when the information was obtained.[184] This may be because the data subject was notified of the purposes for which his or her personal information was collected (in accordance with Principle 3(1)(b)), or because of the context in which the agency collected the personal information.

The personal information sought to be disclosed in the present case is the identity of the alleged offender and possibly account transaction details. We anticipate that the primary purpose for which APAC Coalition Members collect information about their account holders' identities and transactions is to allow each APAC Coalition Member to provide their services to those people. Another purpose of obtaining identifying information might be to comply with laws requiring financial institutions to verify the identity of their account holders. Section 6 of the *Financial Transactions Reporting Act 1996*[185] is an example of such a law.

In these circumstances, there might be difficulties with APAC Coalition Members seeking to rely on this permitted ground of disclosure under Principle 11. Disclosure of account holder information and account transaction details to ICMEC, fellow Coalition Members, the Censorship Compliance Unit or the Police for enforcement action is unlikely to be considered to be a purpose that is directly related to the service provision and compliance with law purposes in connection with which the information was collected.

The proposed disclosure of account holder information to law enforcement agencies might be less problematic, particularly where the disclosure is made under the same legislation that required the collection of identifying information in the first place. See further section 3.5.2 below for a discussion of the disclosure requirements under the Financial Transactions Reporting Act.

Principle 11(d) - Disclosure is authorised by the individual concerned

Disclosure of personal information is also permitted under Principle 11(d) where it is authorised by the individual concerned. From a compliance point of view, obtaining the required authorisation is one of the more robust permitted grounds of disclosure that APAC Coalition Members could seek to rely upon.

Authorisation under the Privacy Act has been held to require a positive act.[186] One of New Zealand's privacy commentators has said that "[t]he concept of authorisation is arguably stronger than that of consent … [it] more clearly denotes a deliberate act".[187] Another commentator put it this way:[188]

> *It is very doubtful that fine print in a form signed months or years earlier would provide an agency with reasonable grounds to believe that a person had "authorised" a certain action that then came as a surprise to that person.*

---

184 *Brookers Human Rights Law,* PR3.11.

185 http://www.legislation.govt.nz/act/public/1996/0009/latest/DLM373804.html?search=ts_act_financial+transactions_resel&p=1&sr=1

186 *Case No 2976* (Privacy Commissioner's Case Notes 1994 – 2005), http://privacy.org.nz/case-note-2976-1996-nzprivcmr-1-couple-complain-bank-conducted-unauthorised-credit-check-and-disclosed-employment-details/?highlight=2976.

187 Roth, PVA6.5(e).

188 *Brookers Human Rights Law,* PR2.02.

Implied authorisation has been found to exist in a small number of cases under the Privacy Act,[189] but these are very fact-specific and not capable of generalisation.

If APAC Coalition Members wish to rely on the permitted ground of disclosure in Principle 11(d), we recommend that they obtain the informed, written consent of their account holders to the use of their personal information as contemplated by the APAC Coalition framework. This informed consent should clearly set out the circumstances in which disclosures to law enforcement agencies, ICMEC and other Coalition Members will be made, as well as the nature of the personal information that will be disclosed on each occasion. A record should be kept of when authorisation was given, on what terms and whether it has been withdrawn subsequently. Procedures should also be established to regularly review authorisations so that they are not rendered irrelevant by the passage of time.

Principle 11(e)(i), (ii), (iv) - Disclosure is necessary to avoid prejudice to the maintenance of law/for the enforcement of a law imposing a pecuniary penalty/for the conduct of proceedings before any court or tribunal

It is possible that an APAC Coalition Member's disclosure of the alleged Offender's details to law enforcement agencies such as the Censorship Compliance Unit or the Police falls within Principle 11(e). Principle 11(e) permits disclosure where an agency believes, on reasonable grounds, that non-compliance is necessary:

- to avoid prejudice to the maintenance of law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences (paragraph 11(e)(i));
- for the enforcement of a law imposing a pecuniary penalty (in this case, the Classification Act offences) (paragraph 11(e)(ii)); and
- for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation) (paragraph 11(e)(iv)).[190]

The most relevant of the above permitted grounds for disclosure is likely to be the maintenance of law ground in Principle 11(e)(i). To be able to rely on this ground, an APAC Coalition Member will need to meet the high standard of showing that non-compliance with the non-disclosure rule in Principle 11 was necessary, and that there was the requisite nexus between the Coalition Member's non-compliance and the law enforcement objectives described above. This can be a high threshold to meet, as illustrated by the following test stated in respect of the permitted ground of disclosure in Principle 11(e)(i):[191]

> *…for [the permitted ground of disclosure in Principle 11(e)(i)] to apply there must be a very direct connection between the disclosure and prejudice to the maintenance of the law. The particular prejudice should be clear or particularised. We think general assumptions about the possible consequences of a disclosure will not be sufficient to satisfy the provision.*

While the law enforcement permitted grounds of disclosure in Principle 11(e) are not limited in their application to disclosure to law enforcement agencies, in the present case we doubt whether APAC Coalition Members could rely on them in respect of disclosures of account

189 See for example, *L v L* (Decision No 15/2001, CRT 11/01, 26 July 2001); *L v J* (1999) 5 HRNZ 616 (which dealt with Rule 11 of the Health Information Privacy Code 1994).

190 Principle 11(e)(iii) also permits disclosure where this is necessary for the protection of the public revenue.

191 *K v Police Commissioner* (unreported, Complaints Review Tribunal, Decision No 33/99, CRT 17/99, 26 November 1999).

holder details to ICMEC and their fellow Coalition Members. This is principally because neither ICMEC nor the APAC Coalition Members have any mandate to investigate or enforce the objectionable publication offences in the Classification Act, and so disclosure to those recipients cannot be considered "necessary". In this regard, we note that prosecutions under the Classification Act can only be commenced with the leave of the Attorney-General,[192] although his power can ultimately be delegated to members of the Police of Inspector rank and above.[193]

Savings provision, s 7 – Disclosure is pursuant to another enactment

As further discussed in paragraph 3.5.2 below, APAC Coalition Members might sometimes be obliged to report the unlawful activities of their account holders under the Financial Transactions Reporting Act.

Disclosure of personal information under another enactment will not result in a contravention of Principle 11. This is because the savings provision in s 7(1) of the Privacy Act provides that nothing in Principle 11 derogates from an enactment that authorises or requires personal information to be made available.

Conclusion regarding the application of the exceptions to the non-disclosure rule in Principle 11

Where an APAC Coalition Member is required to disclose an account holder's suspected unlawful activities under the Financial Transactions Reporting Act or any other enactment, there will be no contravention of Principle 11.

Otherwise an APAC Coalition Member will need to establish that one of the exceptions to the non-disclosure rule in Principle 11 applies. From a compliance point of view, (so long as the appropriate authorisation can be obtained), one of the more robust exceptions for an APAC Coalition Member to rely on is Principle 11(d), which permits disclosure where it is authorised by the individual concerned. Where the disclosure is to law enforcement agencies, one or more of the exceptions in Principle 11(e) might be available. Reliance on the purpose exception in Principle 11(a) is likely to be more difficult, at least until APAC Coalition Members clearly communicate to their account holders their participation in the Coalition and the potential disclosures of personal information that such participation could involve.

Principle 8 and the use of personal information about an account holder's alleged involvement in unlawful dealings in child pornography

APAC Coalition Members also need to consider their obligations under Principle 8 under the APAC Coalition framework.

Principle 8 provides that an agency must not use personal information it holds without taking such steps (if any) as are reasonable in the circumstances to ensure that the information is accurate, up to date, complete, relevant, and not misleading, having regard to the purpose for which the information is proposed to be used. Construed purposively, Principle 8's concept of 'use' includes disclosure of personal information.

The APAC Coalition proposes disclosure of an account holder's identity, and potentially transaction details, in the following two circumstances:

192 *Films, Videos, and Publications Classification Act 1993*, s 144(1).

193 *Films, Videos, and Publications Classification Act 1993*, s 144(2), 145(1).

- to identify alleged offenders to law enforcement agencies so that they can investigate and possibly take enforcement action against the individual;

- in the event that no law enforcement action is taken, to fellow APAC Coalition Members with the request that all accounts and services provided by the APAC Coalition Members to the alleged Offender be closed down.

In both of these cases, an individual is likely to suffer significant harm in the event that the information used by APAC Coalition Members to form a view that an account holder is likely to be dealing in child pornography turns out to be wrong. As a result, Principle 8 will require a proportionally high standard of data quality. APAC Coalition Members will need to develop robust procedures to ensure that they can demonstrate to the Privacy Commissioner or other decision-maker that they have taken reasonable steps to ensure the personal information used is accurate, up to date, complete, relevant and not misleading. One instance where particular care will need to be taken is where the account into which a payment for child pornography has been received is a joint account. APAC Coalition Members should not merely assume the involvement of both account holders in the unlawful activity. Careful checks should be undertaken prior to taking any steps adverse to the data subject, such as terminating their services. It may even be appropriate to give account holders an opportunity to respond to the allegation before taking the disclosure and termination steps contemplated by the APAC Coalition framework.

Other Privacy Act considerations related to the proposed disclosure of account holder identities

Principle 10 – The use limitation principle

Principle 10 is relevant to an APAC Coalition Member's use of account holder personal information to relate a test or undercover transaction to an account holder, and thereby pinpoint the individual whose identity the relevant APAC Coalition Member proposes to disclose to law enforcement, ICMEC and fellow APAC Coalition Members.

Principle 10 is colloquially known as the use limitation principle. It provides that an agency that holds personal information obtained in connection with one purpose must not use that information for any other purpose unless the agency believes, on reasonable grounds, that one of the permitted grounds of use applies.

The application of Principle 10 to the present case involves similar considerations as those set out in relation to Principle 11 above. While the permitted grounds of use in Principle 10 are not identical to the permitted grounds of disclosure in Principle 11, there is a significant degree of overlap. Relevantly for the present case, the data subject authorisation and maintenance of law grounds of disclosure in Principle 11 have counterparts in Principle 10. It is these grounds of use that are likely to be most relevant to APAC Coalition Members seeking to use their account holders' personal information to relate a particular transaction to an account holder.

Principle 2 – Source of personal information

A further point that ICMEC and APAC Coalition Members need to consider is that an APAC Coalition Member's disclosure of account holder personal information to law enforcement agencies, ICMEC and fellow APAC Coalition Members is only one half of the equation. The other half is whether those persons can collect that information.

Principle 2 provides that agencies must collect personal information directly from the data subject, except in certain limited circumstances. These circumstances relevantly include where the agency believes, on reasonable grounds:

- that the individual concerned authorises collection of the information from someone else (Principle 2(2)(b));
- that non-compliance is necessary (Principle 2(2)(d)):
    - to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences;
    - for the enforcement of a law imposing a pecuniary penalty;
    - for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);
- that compliance would prejudice the purposes of the collection (paragraph 2(2)(e)); or
- that compliance is not reasonably practicable in the circumstances of the particular case (Principle 2(2)(f)).

Each recipient of disclosed personal information under the APAC Coalition framework will need to assess whether they fall within the bounds of one or more of the above exceptions.

The maintenance of law exception in Principle 2(2)(d)(i) has been held to apply in a situation broadly analogous to the present case. In *Case No 6314*, the Accident Rehabilitation and Compensation Insurance Corporation (**ARCIC**) asked a private investigator to investigate a claimant who was receiving weekly compensation and other allowances. The private investigator posed as a potential guest at the claimant's bed and breakfast accommodation and asked the claimant's wife about the day-to-day operation of the business with a view to collecting information about the claimant's use of home helpers provided by ARCIC. The Privacy Commissioner accepted the ARCIC's submission that it had reasonable grounds to believe that the maintenance of law exception in Principle 2(2)(d)(i) applied in the circumstances:

> *I agreed that where fraudulent activity was suspected it was not reasonable to expect [ARCIC] to approach the claimant first. I accepted that collecting information from people other than the suspect could be justified where the information was sought to confirm or refute a suspicion of fraudulent actions.*

As we have seen with the use and disclosure principles (Principles 10 and 11 respectively), law enforcement agencies who have a mandate to prevent, detect, investigate, prosecute or punish Classification Act offences will typically have a stronger case for relying on the maintenance of law exception in Principle 2(2)(d)(i). That is not to suggest that ICMEC and APAC Coalition Members are prevented from relying on that exception in any appropriate case.

ICMEC and APAC Coalition Members might also seek to rely on the exceptions in Principle 2(2)(e) (compliance would prejudice the purpose of collection) and Principle 2(2)(f) (compliance is not reasonably practicable in the circumstances). Most commonly, it will not

be practicable to obtain the information directly from the individual concerned if the agency does not, at the time of the collection, know the identity of that individual or does not know how to get in touch with them. These features will typically exist in the present case.

The Privacy Act and Trans-border Data Flows

Unlike some other jurisdictions, New Zealand's Privacy Act does not contain any express prohibition on the transfer of personal information outside New Zealand. Instead, the Privacy Act regulates:

- the circumstances in which the transfer is permissible; and
- the entities that will remain responsible under New Zealand's Privacy Act 1993 for personal information held outside New Zealand (if any).

Circumstances in which the transfer is permissible

Cross-border transfers of personal information are generally regulated by the disclosure principle in New Zealand's Privacy Act (principle 11). The disclosure principle prohibits the disclosure of personal information except where a permitted ground for disclosure applies. These permitted grounds for disclosure include where the regulated agency believes, on reasonable grounds, that:

- the disclosure is one of the purposes for which the information was collected or is directly related to one of those purposes; or
- the disclosure is authorised by the individual concerned.

Responsibility under New Zealand law for personal information held outside New Zealand

A regulated agency that *itself* holds personal information outside New Zealand is required to comply with several of the information privacy principles (IPPs) in New Zealand's Privacy Act. Specifically, section 10 of the Privacy Act provides that:

- the IPPs relating to storage, security, retention, use and disclosure (IPPs 5 and 8-11) apply to personal information held outside New Zealand by a regulated agency where that information has been transferred out of New Zealand by that agency or any other agency; and
- the IPPs relating to access and correction of personal information (IPPs 6 and 7) apply to personal information held outside New Zealand by a regulated agency.

The concept of what it means for a regulated agency to 'hold' personal information is an important one when considering the application of section 10. Under section 3(4) of the Privacy Act, where an agency:

- holds information (i) solely as agent, (ii) for the sole purpose of safe custody, or (iii) for the sole purpose of processing the information on behalf of another agency; and
- does not use or disclose the information for its own purposes,

the information is deemed to be held by the agency on whose behalf that information is held or processed.

Other relevant matters

New Zealand's regulation of trans-border data flows was considered by the Law Commission as part of a general review of New Zealand's privacy laws. The final report was issued in August 2011. The recommendations are awaiting a government response. If enacted, there may be changes which affect this advice.

The Privacy (Cross-border Information) Amendment Act 2010 was enacted in September 2010. This empowers the Privacy Commissioner to prohibit the transfer of personal information in circumstances where the personal information appears to be routed through New Zealand to circumvent the privacy laws of the country from which the information originated. New Zealand's privacy laws have not yet been assessed as 'adequate' by the European Union, but the Privacy Commissioner expects that the enactment of the Privacy (Cross-border Information) Amendment Act will enable New Zealand to obtain a formal finding of adequacy from the European Union. In April 2011, the EU Article 29 Data Protection Working Party issued an opinion (11/2011) recognising that New Zealand's privacy law meets international best practice.

Legislation establishing a legal framework for trusted third parties

There is no legislation in New Zealand establishing a legal framework for trusted third parties.

(c) Criminal law aspects

The legal framework

It is a crime in New Zealand to aid or abet any person in the commission of an offence, and to incite, counsel or procure a person to commit an offence.[194] Any person – either natural or legal – who participates in these ways is a party to and guilty of the substantive offence.[195]

There are two parts to the *mens rea* (mental element) required to establish secondary liability under the Crimes Act:[196]

- knowledge of the essential matters that constitute the offence committed by the principal party; and
- an intention or purpose to help or encourage the principal party to do the acts that constitute the offence.

The *actus reus* (physical element) depends on the nature of the secondary participation alleged.

There is precedent in New Zealand that a purchaser can aid or abet the offence of unlawful selling.[197] This is a specific instance of the general principle that where an offence is specifically directed at one party to a bilateral transaction, the other party to the transaction will ordinarily be liable as a secondary party unless the offence is distinctly intended for the latter's protection.[198]

However, other New Zealand cases addressing the criminal liability of purchasing parties to a transaction have questioned whether secondary parties should be held liable, particularly where it is a

194 *Crimes Act 1961,* s 66(1).
195 *Crimes Act 1961,* s 66(1).
196 Adams on Criminal Law, paragraph CA6.19.
197 *Angland v Hosken* [1935] NZLR 71; *Hedley v Hamlin Kallil* [1936] NZLR 732.
198 *Giorgianni v R* (1985) 156 CLR 473 (HCA) per Mason J; *Scott v Killian* (1985) 40 SASR 37; *R v Maroney* (2000) 114 A Crim R 364.

necessary part of the substantive offence that the offending material is supplied "to any other person".[199]

Application to the present case

Given the precedent discussed above, there is a risk that a civilian tester may be held liable as a secondary party to the substantive Classification Act offences committed by the Offender when the Offender grants access to the Offender's Site or otherwise makes available the child pornography material. Depending on how the Offender's Site operates, these substantive offences could include:

(i) the offences of supplying or distributing an objectionable publication to another person;[200] and

(ii) the offence of displaying or exhibiting an objectionable publication to any other person in expectation of payment or otherwise for gain.[201]

Where charged, the tester may be in a position to rely on a Classification Act defence, provided that both the form[202] and nature of the charge permit (since not all Classification Act offences have statutory defences).

From a practical perspective, we consider that the risk of ICMEC or APAC Coalition Members being prosecuted as secondary participants to Classification Act offences is relatively remote.

First, we anticipate that there will often be difficulties in making out the mens rea (mental element) required to establish secondary liability. The requisite mens rea is generally described as an intention to help or encourage the principal party to do the acts that constitute the offence.

Second, prosecutions under the Classification Act can only be commenced with the leave of the Attorney-General,[203] which power can ultimately be delegated to members of the Police of Inspector rank and above.[204] The Solicitor-General's Prosecution Guidelines[205] list a number of factors that appear to militate against a person in the position of ICMEC or Coalition Members being charged as a secondary participant. In the first instance, we question whether a prosecution of ICMEC or a Coalition Member would be in the "public interest" given the overriding objectives of the Coalition. Public interest is the factor that is largely determinative of the decision to prosecute. Other factors include:

- Whether the conduct in question really warrants the intervention of the criminal law;
- The degree of culpability of the alleged offender;
- Whether the prosecution might be counter-productive; and
- Whether the consequences of any resulting conviction would be unduly harsh or oppressive.

It may also assist ICMEC or the relevant Coalition Member that they may be able to give evidence against the alleged Offender which may not otherwise be available to law enforcement agencies.

---

199 *R v Ngamoki* 7/11/97, Heron J, HC Palmerston North T5/97.

200 *Films, Videos, and Publications Classification Act 1993*, s 123(1)(e).

201 *Films, Videos, and Publications Classification Act 1993*, s 123(1)(f).

202 It is possible to be convicted upon a count charging the tester with having committed the crime, or upon a count alleging how be became a party to it. *Crimes Act 1961*, s 343.

203 *Films, Videos, and Publications Classification Act 1993*, s 144(1).

204 *Films, Videos, and Publications Classification Act 1993*, s 144(2), 145(1).

205 http://www.crownlaw.govt.nz/uploads/ProsecutionGuidelines.PDF.

However, in order to eliminate the risk of secondary liability for ICMEC and APAC Coalition Members altogether, we recommend that undercover transactions only be taken by or with the authorisation of law enforcement officers.

We also recommend that ICMEC discusses the proposed operation of the APAC Coalition framework with law enforcement authorities prior to establishing the framework. New Zealand's *Policing Act 2008*[206] acknowledges the role of private sector bodies in assisting the Police in the performance of their roles.[207] If ICMEC can reach an understanding with the law enforcement agencies in New Zealand that allows them to assist in the identification of Offenders without the threat of direct or secondary liability, risk can be removed. Such an understanding would also remove risk of critical or adverse issues between other enforcement agencies and ICMEC or APAC Coalition Members.

(d) Banking secrecy rules

The legal framework

(i) Bankers' duty of confidence

New Zealand banks and financial institutions owe duties of confidence to their (whether those customers are legal or natural persons) in respect of information arising in the course of banker-customer relationships. These duties are founded in an implied term of the banker-customer contract and in equity. A banker's contractual and equitable duties of confidence are largely co-extensive. The main difference between them is when those duties begin and end.[208]

Tournier v National Provincial and Union Bank of England is the leading case in New Zealand on bankers' duties of confidence. In that case, Banker J explained the nature and extent of a banker's contractual duty of confidence as follows:[209]

> *[T]he duty is a legal one arising out of contract, and … the duty is not absolute but qualified…. On principle I think that the qualifications can be classified under four heads:*
>
> *(i) where disclosure is under compulsion by law;*
>
> *(ii) where there is a duty to the public to disclose;*
>
> *(iii) where the interests of the bank require disclosure; and*
>
> *(iv) where the disclosure is made by the express or implied consent of the customer.*

Each of these exceptions will be discussed in more detail, and applied to the present case, in section 3.5.2 below.

(ii) The Privacy Act

---

206 http://www.legislation.govt.nz/act/public/2008/0072/latest/DLM1102125.html?search=ts_act_policing_resel&p=1&sr=1.

207 *Policing Act 2008*, s 10.

208 The equitable duty arises before the banker and customer contract is established, whereas the contractual duty does not commence until the relationship of banker and customer is established.

209 *Tournier v National & Provincial & Union Bank of England* [1924] 1 KB 461, at 471 and 472.

The Privacy Act's provisions that regulate the disclosure of personal information constitute an additional layer of regulation for banks where the information in question is 'personal information' within the meaning of the Privacy Act (see further section 3.2 above). Some of the exceptions to the use and disclosure principles in the Privacy Act can be viewed as legislative confirmation of the *Tournier* exceptions to a banker's contractual duty of confidence.[210]

(iii) Code of Banking Practice

The New Zealand Bankers' Association has developed the *Code of Banking Practice*, which is a self-regulatory code of conduct that sets out good banking practices.[211] Compliance with the Code is voluntary, but a number of the major banks in New Zealand have agreed to observe it. These banks include ANZ, ASB Bank, Bank of New Zealand, Citibank, HSBC, Kiwibank, TSB Bank and Westpac.

Part 2.1 of the Code addresses customer privacy and provides in relevant part:

> *(i) We have a strict duty to protect the confidentiality of all our Customers and former Customers' affairs. We are also obliged in our dealings with our personal Customers to observe and comply with the Privacy Act 1993.*
>
> ...
>
> *(ii) Certain laws require us to disclose your confidential information, for example, under the Tax Administration Act 1994 the Inland Revenue Department may request certain information from us. Section 11.2 of this Code lists examples of some additional laws that may require us to disclose your confidential information.*

Section 11.2 refers to the Financial Transactions Reporting Act, among other enactments.

The Code of Banking Practice is instructive of the approach that major New Zealand banks take toward the disclosure of their customers' confidential information. Relevantly, no express reference is made to the second *Tournier* exception as a ground for disclosure of customer information.

Application to the present case

(i) The first *Tournier* exception – disclosure under compulsion by law

The implied contractual duty of confidence is overridden by the duty of both bank and customer to submit to any other rule of law that requires disclosure.[212]

There are a significant number of New Zealand laws under which banks are obliged to disclose information about their customers. Of particular relevance to the present case are the Financial Transactions Reporting Act and the AML CFT Act.

---

210 Roth, BNF.2.

211 http://www.nzba.org.nz/banking-standards/#cobp.

212 *Tournier v National & Provincial & Union Bank of England* [1924] KB 461, at 473. Where the information concerned is information about an identifiable individual, this exception is endorsed by Principle 11(e) of the Privacy Act, and s 7 of the Privacy Act, which is the Privacy Act's savings provision.

Under the Financial Transactions Reporting Act, a financial institution[213] must make a suspicious transaction report[214] to the Commissioner of Police where:[215]

- any person conducts or seeks to conduct any transaction through a financial institution; and
- the financial institution has reasonable grounds to suspect:
    - that the transaction or proposed transaction is or may be relevant to the investigation or prosecution of any person for a money laundering offence; or
    - that the transaction or proposed transaction is or may be relevant to the enforcement of the *Criminal Proceeds (Recovery) Act 2009*.

The proceeds of crime ground of suspicion is likely to be the most relevant ground of suspicion in the present case.

The Proceeds of Crime Act 1991 was repealed and replaced with the *Criminal Proceeds (Recovery) Act 2009* on 1 December 2009. One important difference between the two Acts is that the new Act is relevant not just to the proceeds of serious offences, but also where property, proceeds, or benefits of a value of $30,000 or more have, directly or indirectly, been acquired or derived as a result of criminal offending.[216]

Applied to the present case, the Financial Transactions Reporting Act will require APAC Coalition Members, who are 'financial institutions' as defined in the Act, to report a transaction to the Commissioner of Police if the Member suspects that payments for child pornography received by its account holders are:

- the proceeds of a knowledge-based objectionable publication offence under the Classification Act (knowledge-based offences being 'serious offences'); or
- proceeds to the value of $30,000 or more that have, directly or indirectly, been acquired or derived from criminal offending.

An APAC Coalition Member's reliance on this reporting obligation in the Financial Transactions Reporting Act is likely to be of limited assistance in facilitating the disclosure of account holders' identities as contemplated by the APAC Coalition framework.

In the first instance, this is because the Financial Transactions Reporting Act only permits disclosure to the Commissioner of Police; it does not permit disclosure to other Coalition Members as contemplated by the APAC Coalition framework.

Secondly, APAC Coalition Members are likely to face some difficulty in assessing whether a particular payment for child pornography triggers the reporting obligation in the Financial Transactions Reporting Act. Coalition Members will not be well-placed to determine whether

---

213 The Financial Transactions Reporting Act defines "financial institutions" to include banks, and any person whose business consists of providing financial services that involve the transfer or exchange of funds, including payment services.

214 A suspicious transaction report must contain the details specified in the Financial Transactions Reporting Act, including the identity of the persons conducting the transaction, where those details are known the person conducting the report. *Financial Transactions Reporting Act 1996*, s 15(2)(b).

215 *Financial Transactions Reporting Act 1996*, s 15(1). The Commissioner of Police has issued guidelines under s 24 of the Financial Transactions Reporting Act to help financial institutions identify transactions that may give rise to either of the two grounds of suspicion set out above. The guidelines are http://www.nzba.org.nz/banking-standards/#cobp.

216 *Criminal Proceeds (Recovery) Act 2009*, s 6.

a knowledge-based or strict liability offence has been committed, or whether the $30,000 threshold for criminal proceeds has been met, working on the assumption that a single payment to access child pornography online is likely to be significantly less than $30,000. The application of the $30,000 threshold in the Criminal Proceeds (Recovery) Act 2009 is yet to be considered by the New Zealand Courts. However, in our view, the language of the definition of "significant criminal activity" permits aggregation of proceeds arising out of an activity. The definition provides:

> *In this Act, unless the context otherwise requires,* ***significant criminal activity*** *means an activity engaged in by a person that if proceeded against as a criminal offence would amount to offending - …*
>
> (b) from which property, proceeds, or benefits of a value of $30,000 or more have, directly or indirectly, been acquired or derived.

(ii) The second *Tournier* exception – duty to the public to disclose

There is also an argument that APAC Coalition Members could rely on the second *Tournier* exception to disclose account holder information. Atkin LJ has suggested that a bank might have a duty to the public to disclose confidential information in cases where the public needs to be protected against "fraud or crime".[217] However, the public interest in disclosure will need to be weighed against the strong countervailing public interest "that confidences should be respected".[218]

The difficulty with reliance on the second *Tournier* exception is that it is notoriously uncertain. It has been said that "all the banking law texts agree that [the second *Tournier* exception] has been the least used and is the least easily comprehended of the *Tournier* exceptions."[219] Further, a leading banking law text in New Zealand states that: [220]

> *The only sound advice that may be given is that, in relation to information about customers that are not individuals, the banker should exercise extreme restraint before disclosing information pursuant to the supposed duty to the public. In relation to information about identifiable individuals, the banker should release information only in compliance with the relevant exceptions to the statutory prohibition against disclosure under s 6, principles 10 and 11, of the Privacy Act 1993.*

We therefore consider that it would be a risky course for APAC Coalition Members to rely on the second *Tournier* exception in support of their disclosure of account holder information for accounts into which payments for accessing an Offender's Site are received.

(iii) The third *Tournier* exception - interests of the bank require disclosure

The third *Tournier* exception applies where the bank is suing or defending an action in relation to a customer or third party such as a guarantor. It is not relevant to the present case.

(iv) The fourth *Tournier* exception - disclosure is made by the express or implied consent of the customer

---

217 *Tournier,* per Atkin LJ at 486.

218 *Attorney-General v Guardian Newspapers Ltd (No 2)* [1988] 3 WLR 776 at 782 per Keith LJ; cf p 807, per Goff LJ.

219 *R v Curtis* CA 346-93, 3 December 1993.

220 *Tyree's Banking Law in New Zealand* para 4.5.4.

The fourth *Tournier* exception permits disclosure of customer information where the customer has expressly consented to the disclosure, provided that the bank discloses only information that is and within the bounds of the customer's consent.[221] More specifically, it is stated in *Tournier* that "to the extent to which [the consent] is given, the bank will be justified in acting."[222] We infer from this statement that a customer's consent will never extend to the disclosure of incorrect information. Principle 7 (permitting an individual to request correction of personal information held by a bank) and principle 8 (requiring a bank to take reasonable steps to ensure that information to be used is accurate, up to date, complete, relevant and not misleading) of the Privacy Act reinforce the obligations of banks in this regard. A bank can also infer implied consent where it can demonstrate that the customer is aware of the banking practice that gives rise to the disclosure.

From a compliance point of view, the fourth *Tournier* exception is likely to be one of the more robust exceptions that APAC Coalition Members could seek to rely upon. Since the corresponding Privacy Act exception requires express authorisation by the individual concerned,[223] it is submitted that APAC Coalition Members should similarly obtain express authorisation from their corporate customers to disclose account holder information as contemplated by the APAC Coalition framework.

(e) Termination of contract/general contract law

The legal framework

In New Zealand, a contract can be terminated for breach:

(i) in accordance with its terms; and

(ii) where the *Contractual Remedies Act 1979* otherwise permits.

The *Contractual Remedies Act 1979* applies only to contracts that are governed by New Zealand law, and only to the extent that the Act's remedies are not inconsistent with the terms of the contract. Assuming those prerequisites are met, the *Contractual Remedies Act 1979* provides that a party to a contract may cancel the contract if the other party breaches an essential term, or where the effect of the breach is to substantially change the benefit or burden of the contract.

New Zealand's illegal contracts legislation[224] generally provides that illegal contracts, such as those that are contrary to public policy, have no effect.[225] However, this legislation does not come into play in the present case because no illegality arises from the creation or performance of the contract itself.

Application to the present case

The question of whether an APAC Coalition Member can terminate a contract with one of its customers, as contemplated by the APAC Coalition framework, will turn on the construction of the relevant contract between the APAC Coalition Member and the customer, and the application of the *Contractual Remedies Act 1979*. Each APAC Coalition Member will need to separately assess their position vis-à-vis the particular customer concerned.

---

221 *Tyree's Banking Law in New Zealand,* para 4.5.4.

222 *Tournier,* per Atkin LJ at 486.

223 See further section 3.2.2, p22 above.

224 *Illegal Contracts Act 1970.*

225 *Illegal Contracts Act 1970,* s 6.

It is preferable that each APAC Coalition Member includes an express term in its customer contracts empowering the Member to terminate services provided to a customer where the Member forms a suspicion that the customer's account has been used to for allegedly unlawful activities. Care needs to be taken in the drafting of any such term so that an APAC Coalition Member can safely rely on the term in circumstances where its suspicion may not be reasonably held, and/or the child pornography material in question turns out not to be an objectionable publication within the meaning of the Classification Act.

(f) Other obstacles

Defamation and malicious falsehood

ICMEC and APAC Coalition Members should also be aware of the real risk of liability under the torts of defamation and/or malicious falsehood in the event that account holders are incorrectly identified as being in receipt of payments for allegedly objectionable publications, or that the allegation made against the account holder is otherwise unfounded.

Even where the allegation is well-founded, aggrieved account holders may nonetheless commence defamation and/or malicious falsehood proceedings against ICMEC and APAC Coalition Members. It may be that ICMEC and APAC Coalition Members can rely on the defences of truth and/or qualified privilege in respect of at least some of their publications if limited to enforcement agencies, for example. However, it is fair to say that the outcome of defamation proceedings in New Zealand (as in many other jurisdictions around the world) cannot always be predicted with certainty.

A further point to bear in mind is that defamation/malicious falsehood liability is magnified by any proposed publication to ICMEC and fellow APAC Coalition Members. This is relevant to the size of any civil damages award that might be made in the event that the plaintiff prevails and no complete defence can be made out.[226]

[226] The tort of defamation only attracts civil liability in New Zealand. Libel and slander have not been criminal offences since the enactment of the *Defamation Act 1992*.

SCHEDULE 1

INFORMATION PRIVACY PRINCIPLES

Principle 1 Purpose of collection of personal information

Personal information shall not be collected by any agency unless—

(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) The collection of the information is necessary for that purpose.

Principle 2 Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds, —

(a) That the information is publicly available information; or

(b) That the individual concerned authorises collection of the information from someone else; or

(c) That non-compliance would not prejudice the interests of the individual concerned; or

(d) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(e) That compliance would prejudice the purposes of the collection; or

(f) That compliance is not reasonably practicable in the circumstances of the particular case; or

(g) That the information—

(i) Will not be used in a form in which the individual concerned is identified; or

(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

Principle 3 Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

(a) The fact that the information is being collected; and

(b) The purpose for which the information is being collected; and

(c) The intended recipients of the information; and

(d) The name and address of—

(i) The agency that is collecting the information; and

(ii) The agency that will hold the information; and

(e) If the collection of the information is authorised or required by or under law, —

(i) The particular law by or under which the collection of the information is so authorised or required; and

(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) The rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds, —

(a) That non-compliance is authorised by the individual concerned; or

(b) That non-compliance would not prejudice the interests of the individual concerned; or

(c) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That compliance would prejudice the purposes of the collection; or

(e) That compliance is not reasonably practicable in the circumstances of the particular case; or

(f) That the information—

(i) Will not be used in a form in which the individual concerned is identified; or

(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4 Manner of collection of personal information

Personal information shall not be collected by an agency—

(a) By unlawful means; or

(b) By means that, in the circumstances of the case, —

(i) Are unfair; or

(ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5 Storage and security of personal information

An agency that holds personal information shall ensure—

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) Loss; and

(ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6 Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) To have access to that information.

(2) Where, in accordance with sub-clause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5 of this Act.

Principle 7 Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled—

(a) To request correction of the information; and

(b) To request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8 Accuracy, etc, of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9 Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10 Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds, —

(a) That the source of the information is a publicly available publication; or

(b) That the use of the information for that other purpose is authorised by the individual concerned; or

(c) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to—

(i) Public health or public safety; or

(ii) The life or health of the individual concerned or another individual; or

(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) That the information—

(i) Is used in a form in which the individual concerned is not identified; or

(ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) That the use of the information is in accordance with an authority granted under section 54 of this Act.

Principle 11 Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) That the source of the information is a publicly available publication; or

(c) That the disclosure is to the individual concerned; or

(d) That the disclosure is authorised by the individual concerned; or

(e) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to—

(i) Public health or public safety; or

(ii) The life or health of the individual concerned or another individual; or

(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) That the information—

(i) Is to be used in a form in which the individual concerned is not identified; or

(ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

Principle 12 Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of subpart YB of the Income Tax Act 2007.

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

THE PHILIPPINES

1. EXECUTIVE SUMMARY

No.	Section	Content
1.	**Data Protection**	In November 2009, the Philippine Congress passed into law Republic Act No. 9775, otherwise known as the "Anti Child Pornography Act of 2009". This is considered landmark legislation in that it provides specific rules with respect to data that can be provided and made accessible to the public. More particularly, the law imposes certain duties on Internet service providers and Internet content hosts with respect to monitoring, reporting on, and preventing access to and transmittal of child pornography or child pornography materials.
2.	**Criminal Law**	While it has been a long declared policy of the state to promote and protect the physical, moral, spiritual and social well being of our youth. (Article II, Section 13 of the 1987 Constitution), laws specifically addressing the problem of child abuse and exploitation in the Philippines have not always been in place. At one time, even the Supreme Court had occasion to observe that there is "a lack of criminal laws which will adequately protect street children from exploitation by paedophiles, pimps, and, perhaps, their own parents or guardians who profit from the sale of young bodies." In 1992, Republic Act No. 7610, otherwise known as the "Special Protection of Children against Abuse, Exploitation and Discrimination Act", was enacted for the protection of children against abuse, commercial sexual exploitation, trafficking, and employment in illicit activities. More recently, to address the changes in the nature and means of accessing and disseminating child pornography, the Philippine Congress passed into law the Anti-Child Pornography Act of 2009 (Republic Act No. 9775), The law defines "child pornography" as "any representation, whether visual, audio, or written combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities" The law criminalises the mere possession of any form of child pornography.

No.	Section	Content
3.	**Banking Secrecy Laws**	Bank secrecy laws appear to be rigid and inflexible. Yet, Republic Act No. 9775 requires banks to report any suspected child pornography materials or transactions to the proper authorities. It is unclear how this exception to the numerous law and regulations on the secrecy of bank deposits is supposed to be undertaken. Also, the relaxation of banking secrecy laws based only on probable cause, instead of a final court order of attachment on the basis that the funds in the bank are fruits of the crime of child pornography may not be easily achieved, given that its laudable purpose must be tempered against the Philippines' interests in the credibility and speedy growth of its banking system.

2. FULL JURISDICTION REPORT

2.1 International Legal Framework

At the outset, when dealing with international treaties, the Philippines adheres to the principle of incorporation enunciated in Section 2, Article II of the its Constitution. Such Constitutional principle declares that "the Philippines adopts the generally accepted principles of international law as part of the law of the land".

As regards the power to enter into treaties or international agreements, the Constitution vests the same in the President, subject only to the concurrence of at least two-thirds vote of all the members of the Senate.

The Philippine Supreme Court has had several occasions to rule that the above-mentioned doctrine of incorporation is applied whenever local courts are confronted with situations in which there appears to be a conflict between a rule of international law and the provisions of the constitution or statute of the local state.

(a) List of international legal acts analysed (together with footnotes containing an Internet link to each) in relation to the following issues (or otherwise as appropriate):

(i) SEXUAL EXPLOITATION OF CHILDREN

(A) Convention on the Rights of a Child (CRC)

The Convention on the Rights of a Child was entered into force on 2 September 1990. The Convention on the Rights of a Child has 140 signatories and as of 25 May 2009, 193 States have become parties thereto. The Philippines became a signatory on 26 January 1990 and ratified it on 21 August 1990. The Convention on the Rights of a Child protects the rights of children by setting standards in health care, education, and legal, civil and social services. Among others, it orders that State Parties must protect the child from all forms of sexual exploitation and abuse. The Convention on the Right of a Child provides, in salient part:

Article 19

I. States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or **exploitation**, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child.

II. Such protective measures should, as appropriate, include effective procedures for the establishment of social programmes to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, as appropriate, for judicial involvement.

Article 34

States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:

I The inducement or coercion of a child to engage in any unlawful sexual activity;

II The exploitative use of children in prostitution or other unlawful sexual practices;

III The exploitative use of children in pornographic performances and materials.

(Emphasis supplied.)

(B) The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

Pursuant to the purposes of the Convention on the Rights of the Child, measures were extended to ensure protection for children from the sale of children, child prostitution, and child pornography. Thus, the Optional Protocol was entered into force on 18 January 2002. 116 States are signatories to the Optional Protocol and since 25 May 2009, 131 States have become parties thereto. On 8 September 2000, the Philippines signed the Convention and ratified it on 28 May 2002. The Optional Protocol sought to (i) address the growing availability of child pornography on the Internet and other evolving technologies; (ii) raise public awareness; and (iii) reduce consumer demand for the sale of children, child prostitution, and child pornography. The Optional Protocol provides, in relevant part:

Article 1

States Parties shall prohibit the sale of children, **child prostitution and child pornography** as provided for by the present Protocol.

Article 2

For the purposes of the present Protocol:

I. Sale of children means any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration;

II. **Child prostitution means the use of a child in sexual activities for remuneration or any other form of consideration**;

III. **Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.**

Article 3

I. Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis:

II. In the context of sale of children as defined in article 2:

III. **Offering, delivering or accepting, by whatever means, a child for the purpose of:**

(a) Sexual exploitation of the child;

(b) Transfer of organs of the child for profit;

(c) Engagement of the child in forced labour;

(d) Improperly inducing consent, as an intermediary, for the adoption of a child in violation of applicable international legal instruments on adoption;

IV. **Offering, obtaining, procuring or providing a child for child prostitution, as defined in article 2;**

V. **Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in article 2.**

(Emphasis supplied)

(C) Convention (No. 182) concerning the prohibition and immediate action for the elimination of the worst forms of child labour

The Worst Forms of Child Labour Convention was entered into force on 17 June 1999. As of 25 May 2009, 169 States have ratified it. The Philippines ratified the Worst Forms of Child Labour Convention on 28 November 2000. This convention commits to take immediate action to prohibit and eliminate the worst forms of child labor. It recognizes that child labor is to a great extent caused by poverty and the solution is to alleviate poverty and grant universal education through sustained

economic growth and social progress. The Worst Forms of Child Labour Convention provides, in relevant part:

Article 1

Each Member which ratifies this Convention shall take immediate and effective measures to secure the prohibition and elimination of the worst forms of child labour as a matter of urgency.

Article 3

For the purposes of this Convention, the term *the worst forms of child labour* comprises:

I. All forms of slavery or practices similar to slavery, such as the sale and **trafficking of children**, debt bondage and serfdom and forced or compulsory labour, including forced or compulsory recruitment of children for use in armed conflict;

II. **The use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances;**

III. **The use, procuring or offering of a child for illicit activities, in particular for the production and trafficking of drugs as defined in the relevant international treaties;**

IV. **Work which, by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of children.**

(Emphasis supplied)

(D) International Convention for the Suppression of the Traffic in Women and Children

This treaty was originally concluded in Geneva on 30 September 1921 and entered into force on 15 June 1922. This treaty was amended by the Protocol signed at Lake Success, New York, on 12 November 1947. The Philippines acceded to the treaty on 30 September 1954 and currently, 46 states have signed this treaty. Article 2 of the treaty provides that, "The High Contracting Parties agree to take all measures to discover and prosecute persons who are engaged in the traffic in children of both sexes..." Under Article 4, in cases where there are no extradition Conventions in force between them, the Parties are obliged to take all measures within their power to extradite or provide for the extradition of persons accused or convicted of the offense.

(E) Convention on Cybercrime

The Convention on Cybercrime was opened for signature on 23 November 2001. As of 25 May 2009, 26 States have ratified or acceded to the Convention. The Philippines has been invited to accede to the Convention on Cybercrime but has not signed nor ratified the same. The Convention on Cybercrime recognizes that the revolution in information technology has resulted in new types of crimes, with additional cross-border implications that make it more difficult to seize the perpetrators. The Convention on Cybercrime seeks to, inter alia, address cyberspace offenses that violate human dignity and the protection of minors. Article 9 therein seeks to

strengthen protective measures for children, including protection against sexual exploitation, by updating criminal law provisions to limit the use of computer systems in the commission of sexual offenses against children.

Article 9 – Offences related to child pornography

(F) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

I. Producing child pornography for the purpose of its distribution through a computer system;

II. Offering or making available child pornography through a computer system;

III. Distributing or transmitting child pornography through a computer system;

IV. Procuring child pornography through a computer system for oneself or for another person;

V. Possessing child pornography in a computer system or on a computer-data storage medium.

(G) For the purpose of paragraph (F) above, the term "child pornography" shall include pornographic material that visually depicts:

I. A minor engaged in sexually explicit conduct;

II. A person appearing to be a minor engaged in sexually explicit conduct;

III. Realistic images representing a minor engaged in sexually explicit conduct.

(H) For the purpose of paragraph (G) above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

(b) HUMAN TRAFFICKING

(i) R190 Worst Forms of Child Labor Recommendation, 1999 (see notes above)

(ii) Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others

According to Article 1, Parties to the Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others agree to punish any person who, to gratify the passions of another when such person: (1) procures, entices or leads away, for purposes of prostitution, another person, even with the consent of that person; (2) exploits the prostitution of another person, even with the consent of that person.

Under Article 2, Parties to the Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others further agree to punish any person who: (1) keeps or manages, or knowingly finances or takes part in the financing of a brothel; and, (2) knowingly lets or rents a building or other place or any part thereof for the purpose of the prostitution of others.

Under Article 6, signatories to the convention are obliged to repeal or abolish any law, regulation or administrative provision by virtue of which persons who engage in or are suspected of engaging in prostitution are subject either to special registration or to the possession of a special document or to any exceptional requirements for supervision or notification.

(c) MONEY LAUNDERING

(i) United Nations Convention Against Transnational Organized Crime

The Convention Against Transnational Organized Crime was entered into force on 29 September 2003. As of 25 May 2009, 147 States are signatories and 148 States have become parties to the Convention. The Philippines signed the Convention on 14 December 2000 and ratified it on 28 May 2002. This Convention aims to promote cooperation to prevent and combat transnational organized crime more effectively.

Under the Convention Against Transnational Organized Crime, "organized criminal group" is defined as a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences. The Convention Against Transnational Organized Crime also criminalises the laundering of property or proceeds of a crime for the purpose of concealing or disguising the illicit origin of the property or of helping any person involved in the commission of the crime. The same convention also enumerates the measures that each State Party must take so that they may combat money laundering.

(ii) Article 6 – Criminalization of the laundering of proceeds of crime

Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(A) I. The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;

II. The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

(B) Subject to the basic concepts of its legal system:

I. The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

II. Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

(iii) Article 7 – Measures to combat money-laundering

(A) Each State Party:

I. Shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer identification, record-keeping and the reporting of suspicious transactions;

II. Shall, without prejudice to articles 18 and 27 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money laundering.

(B) States Parties shall consider implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across their borders, subject to safeguards to ensure proper use of information and without impeding in any way the movement of legitimate capital. Such measures may include a requirement that individuals and businesses report the cross-border transfer of substantial quantities of cash and appropriate negotiable instruments.

(C) In establishing a domestic regulatory and supervisory regime under the terms of this article, and without prejudice to any other article of this Convention, States Parties are called upon to use as a guideline the relevant initiatives of regional, interregional and multilateral organizations against money-laundering.

(D) States Parties shall endeavour to develop and promote global, regional, sub regional and bilateral cooperation among judicial, law enforcement and financial regulatory authorities in order to combat money-laundering.

(d) MUTUAL LEGAL ASSISTANCE TREATIES

Mutual legal assistance treaties, or MLATs, are treaties that generally impose reciprocal obligations on party states to cooperate in the investigation and prosecution of crime. These treaties usually provide for an effective means of sharing information and evidence related to criminal investigations and prosecutions.

Presently, the Philippines has MLATs with the following states: United States of America, Republic of China, Swiss Confederation, Hong Kong, Korea, Spain and Australia. These treaties grant and provide to the party states assistance in all matters relating to investigations or proceedings in respect of criminal matters. The treaty of the Philippines with the United States of America is more comprehensive since the request for assistance could cover anything in connection with the prevention, investigation, and prosecution of criminal offenses and in proceedings related to criminal matters. Also, Article 3 of the RP-US MLAT provides that assistance should be provided without any regard to any double criminality standard. This means that the requested state, or the state being asked to render assistance, should comply with its obligations even if the investigation or prosecution is for an act or omission that is not considered an offense or crime within its jurisdiction.

The use of the MLATs with respect to child pornography has not been tested. Even at the domestic level, there is slow action on the part of law enforcers and the judiciary on child pornography cases.

Article 1 of both treaties with Australia and the United States of America provides mutual assistance in criminal matters which includes taking the testimony or statements of persons located in the requested state; providing documents, records, and items of evidence; serving documents; locating or identifying persons or items; transferring persons in custody for testimony or other purposes; executing requests for searches and seizures; assisting in proceedings related to forfeiture of assets, restitution, and collection of fines; and any other form of assistance not prohibited by the laws of the Requested State. Thus, the MLATs of the Philippines with Australia and the United States not only provide efficient and effective means of gathering information on criminal matters but also offer ways of denying criminals the fruits and instrumentalities of their crimes.

Aside from the MLAT's mentioned above, the Philippines has extradition treaties with several countries including Australia, Canada, United States of America, Hong Kong, Federated States of Micronesia, Thailand, Indonesia, Korea, India, Spain, Italy and Switzerland. In general, these treaties contain a dual criminality clause that provides that extraditable offenses are those that are considered offenses in both the requesting and requested states. However, the treaties with Hong Kong, Thailand and Indonesia have a list of extraditable offenses in lieu of a dual criminality clause. The treaty with Hong Kong is the only one with a specific provision on stealing, abandoning, exposing or unlawfully detaining a child; or any other offenses involving the exploitation of children.

(e) LIST OF GENERAL DEFINITIONS OF INTERNATIONAL LAW USED.

Under the Convention on Cybercrime, child pornography refers to pornographic material that visually depicts:

(i) A minor engaged in sexually explicit conduct;

(ii) A person appearing to be a minor engaged in sexually explicit conduct;

(iii) Realistic images representing a minor engaged in sexually explicit conduct.

A minor is defined as all persons under 18 years of age.

Under the Optional Protocol, child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

2.2 Questions and Answers relevant to the APAC Coalition

(a) Are there laws specifically addressing child pornography in the Philippines?

Republic Act No. 9775 (the "Anti-Child Pornography Act of 2009") punishes any person that shall: (a) hire, employ, use, persuade, induce or coerce a child to perform in the creation or production of child pornography; (b) produce, direct, manufacture or create any form of child pornography and child pornography materials; (c) sell, offer, advertise and promote child pornography and child pornography materials; (d) possess, download, purchase, reproduce or make available child pornography materials with the intent of selling or distributing them; (e) publish, post, exhibit, disseminate, distribute, transmit or broadcast child pornography or child pornography materials; (f) knowingly possess, view, download, purchase or in any way take steps to procure, obtain or access for personal use child pornography materials; and (g) attempt to commit child pornography by luring or grooming a child.

In addition, there is an earlier law, Republic Act No. 7610, as amended, Section 9 of which penalizes any person who shall "hire, employ, use, persuade, induce or coerce a child to perform in obscene exhibitions and indecent shows, whether live or in video, or model in obscene publications or pornographic materials or to sell or distribute the said materials." Section 12-D of the same act also prohibits any child from being engaged in the worst forms of child labor, which includes "the use, procuring, offering or exposing of a child for prostitution, for the production of pornography or for pornographic performances."

Both acts define "child" to include not only persons below eighteen (18) years of age but also those who are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation or discrimination because of a physical or mental disability or condition.

Moreover, Republic Act No. 9208 (the "Anti-Trafficking of Persons Act of 2003") makes it unlawful for any person, natural or juridical, to commit any of the following acts:

(i) to recruit, transport, transfer, harbor, provide, or receive a person by any means, including those done under the pretext of domestic or overseas employment or training or apprenticeship, for the purpose of prostitution, pornography, sexual exploitation, forced labor, slavery, involuntary servitude or debt bondage;

(ii) to introduce or match for money, profit, or material, economic or other consideration, any person or any Filipino woman to a foreign national, for marriage for the purpose of acquiring, buying, offering, selling or trading him/her to engage in prostitution, pornography, sexual exploitation, forced labor, slavery, involuntary servitude or debt bondage;

(iii) to offer or contract marriage, real or simulated, for the purpose of acquiring, buying, offering, selling, or trading them to engage in prostitution, pornography, sexual exploitation, forced labor or slavery, involuntary servitude or debt bondage;

(iv) to undertake or organize tours and travel plans consisting of tourism packages or activities for the purpose of utilizing and offering persons for prostitution, pornography or sexual exploitation;

(v) to maintain or hire a person to engage in prostitution or pornography;

(vi) to adopt or facilitate the adoption of persons for the purpose of prostitution, pornography, sexual exploitation, forced labor, slavery, involuntary servitude or debt bondage;

(vii) to recruit, hire, adopt, transport or abduct a person, by means of threat or use of force, fraud, deceit, violence, coercion, or intimidation for the purpose of removal or sale of organs of said person; and

(viii) to recruit, transport or adopt a child to engage in armed activities in the Philippines or abroad.

(b) What is the definition of illegal child pornography in the Philippines, looking at both domestic and international law?

The Anti-Child Pornography Act of 2009 defines child pornography as "any representation, be it visual, audio or written, combination thereof, by electronic, mechanical, digital, optical, magnetic or other means, of a child engaged in real or simulated explicit sexual activities."

This definition appears broader than that provided in the Convention on Cybercrime, which limits the scope of child pornography to any visual representation of a child engaged in real or simulated sexually explicit, indecent, or obscene conduct.

In the event that a broader, more progressive definition is crafted in international law, the Philippines would undoubtedly undertake earnest efforts to harmonize domestic and international law in order to give effect to both.

(c) Are there legal obstacles to the undertaking of a test or an undercover transaction by a law enforcement agency on behalf of the national hotline to the Offender's account?

Under the current statutory framework, there is no prohibition against a law enforcement agency to undertake a test or undercover transaction. However, law enforcement agencies must be mindful of the Constitutional right of all persons to be secure in their persons, houses, papers and effects against unreasonable seizures and the right to the privacy of communication and correspondence.

In line with this, it is unlawful under Philippine law for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word by using a device commonly known as a dictaphone or dictagraph or detectaphone or walkie-talkie or tape recorder, or however otherwise described. It is likewise unlawful for any person, to knowingly possess any tape record, wire record, disc record, or any other such record, or copies thereof, of any communication or spoken word secured or to replay the same for any other person or persons; or to communicate the contents thereof, either verbally or in writing, or to furnish transcriptions thereof, whether complete or partial, to any other person. Any communication or spoken word, or the existence, contents, substance, purport, effect, or meaning of the same or any part thereof, or any information contained, obtained or secured by any person of such unauthorized taping shall not be admissible in evidence in any judicial, quasi-judicial, legislative or administrative hearing or investigation. The only exception to the non-admissibility rule of unauthorized taping communications shall be when a government officer, authorized by a written order of the Court, does the same due to crimes of treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping, punishing espionage and other offenses against national security.

The Supreme Court has ruled that the nature of the conversations is immaterial to a violation of the statute. It held that: "The substance of the same need not be specifically alleged in the information. What R.A. 4200 penalizes are the acts of secretly overhearing, intercepting or recording private communications by means of the devices enumerated therein. The mere allegation that an individual made a secret recording of a private communication by means of a tape recorder would suffice to constitute an offense under Section 1 of R.A. 4200. As the Solicitor General pointed out in his Comment before the respondent court: "Nowhere (in the said law) is it required that before one can be regarded as a violator, the nature of the conversation, as well as its communication to a third person should be professed."

Furthermore, to the extent that there will be an inquiry into the bank accounts of the Offender, bank deposits are absolutely confidential. No person (whether a government official or private entity) may examine bank deposits, and bank officials are prohibited from disclosing any information concerning deposits, except under the following circumstances:

(i) Upon written permission of the depositor; or

(ii) In cases of impeachment; or

(iii) Upon order of a competent court in cases of bribery or dereliction of duty; or

(iv) In cases where the money deposited or invested is the subject matter of litigation.

(d) Are there legal obstacles to the undertaking of a test or an undercover transaction by an entity other than a law enforcement agency (for example, a credit card company or an online payments facilitator) on behalf of the national hotline to the Offender's account?

In the absence of a court order, to the extent that the undercover transaction or test requires an inquiry into the Offender's bank account in the Philippines, the transaction is prohibited by Philippine law on the secrecy of bank deposits. In addition, to the extent that the test or undercover transaction requires the disclosure of electronic documents or information, this is prohibited by the Electronic Commerce Act of 2000 (Republic Act No. 8792).

However, Section 10 of the Anti-Child Pornography Act of 2009 provides that "photo developers, information technology professionals, credit card companies and banks and any person who has direct knowledge of any form of child pornography activities shall have the duty to report any suspected child pornography materials or transactions to the proper authorities within seven (7) days from discovery thereof." The implementing rules and regulations for the Anti-Child Pornography of 2009 merely tracks the language of Section 10 of the Anti-Child Pornography Act of 2009 and does not provide the operational details as how this provision should be implemented in light of existing privacy and data protection laws. The implementing rules and regulations provide that credit card companies and banks found guilty of wilfully and knowingly failing to comply with the notice requirements to the proper authorities shall suffer the penalty of a fine of not less than P1,000,000.00 but not more than P2,000,000.00 for the first offense. In the case of a subsequent offense, the penalty shall be a fine of not less than P2,000,000.00 but not more than P3,000,000.00 and revocation of its license to operate and immediate closure of the establishment.

(e) Are there legal obstacles to the collaboration of APAC Coalition Members in relation to the test or the undercover transaction?

Same as 2.2(d). It should be noted, though, that under Section 6 of the Anti-Child Pornography Act of 2009, complaints on cases of any form of child pornography may be filed by, among others, "at least three (3) concerned responsible citizens residing in the place where the violation occurred", or "any person who has personal knowledge of the circumstances of the commission of (the) offense."

(f) Are there legal obstacles to the disclosure by the APAC Coalition Members of the identity of the holder of the merchant's account and/or the Offender to ICMEC, the other APAC Coalition Members and the public prosecutor?

Same as 2.2(d) and 2.2(e).

(g) Are there legal obstacles to the termination of the provision of services to the Offender by APAC Coalition Members?

There are no legal obstacles, subject to the provisions of the contract.

(h) Recommendations

(i) Building the APAC Coalition and Conduct

As a country plagued with the social dilemma of child abuse and exploitation, the Philippine government may be keen on developing and building the APAC Coalition. Non-government

organizations ("NGOs") may likewise be involved in this endeavour. NGOs are viewed as strategic partners of the government in the social and moral concerns of the country. This is due to the perceived credibility and respect accorded to NGOs and its staff, who often have direct and personal contact with the local community members. NGOs are likewise more flexible and open in exploring innovative approaches to combat child abuse and exploitation. NGOs are skilled in lobbying and advocating their ideas and opinions to the government bodies, often serving as a primordial link to the reality occurring at the grassroots.

It also bears mention that Section 22 of the Anti-Child Pornography Act of 2009 specifically recognizes child pornography as a transnational crime. The Department of Justice is authorized to cooperate with a foreign state in the investigation or prosecution of any form of child pornography by: "(1) conducting a preliminary investigation against the offender and, if appropriate, to file the necessary charges in court; (2) giving information needed by the foreign state; and (3) to apply for an order of forfeiture of any proceeds or monetary instrument or properly located in the Philippines used in connection with child pornography in the court."

(ii) Monitoring of Legal Developments

All laws are passed upon by the Congress of the Philippines, consisting of the House of Representatives and the Senate. Bills of such nature, i.e., data protection, criminal laws, and banking secrecy laws, may originate from either House. These bills may be publicly accessed and monitored.

2.3 Analysis of Relevant Cases

In Karen Salvacion v. Central Bank of the Philippines (G.R. No. 94723, 21 August 1997), an American tourist, coaxed and lured petitioner Salvacion, then 12 years old, to go with him to his apartment. Therein, the accused detained Salvacion for four days and raped her several times. A case for Serious Illegal Detention and four counts of rape charges were filed against the American tourist. A Civil Case for damages with preliminary attachment was also filed against him. On the scheduled day of hearing for Bartelli's petition for bail the latter escaped from jail, thereby causing all criminal cases filed against him to be archived pending his arrest. Meanwhile, the issuance of the writ of preliminary attachment was granted for the petitioners and the writ was issued. However, China Banking Corporation failed to honor Notice of Garnishment served by the Deputy Sheriff. China Banking Corporation invoked Section 113 of the Central Bank Circular No. 960 to the effect that the dollar deposits of defendant Greg Bartelli are exempt from attachment, garnishment, or any other order or process of any court, legislative body, government agency or any administrative body whatsoever.

The Supreme Court held that the questioned Section 113 of the Central Bank Circular No. 960 which exempted from attachment, garnishment, or an order or process of any court, legislative body, government agency or any administrative body whatsoever, is applicable to a foreign transient. Otherwise, injustice would result especially to a citizen aggrieved by foreign guests and negate Article 10 of the New Civil Code, which provides that "in case of doubt in the interpretation or application of laws, it is presumed that the lawmaking body intended right and justice to prevail. The provisions of Section 113 of CB Circular No. 960 and PD No. 1246 insofar as it amends Section 8 of R.A. No. 6426 were held to be inapplicable to the case because of its peculiar circumstances. Respondents were required to comply with the writ of execution and to release to the petitioners the dollar deposits of accused in such amount as would satisfy the judgment. The said case is critical in that the Supreme Court construed a legal provision in such a manner so as to see that it protects and upholds the interest of the child.

2.4 Analysis of Domestic and International Statutory Law

(a) Key Problems

The Philippines does not appear to suffer from a shortage of laws intended to address the problems of child exploitation and pornography. There, in fact, appears to be a surfeit of legislation. The Philippines has a number of overlapping legislation on the trafficking of children, child exploitation, and child pornography. This suggests that there may be two key areas of concern – awareness and implementation.

Lack of Awareness. There seems to be a lack of awareness or understanding on the part of law enforcers and the general public of the laws on the sale of children, child prostitution, and child pornography. The Anti-Child Pornography Act of 2009 attempts to address this shortcoming by placing responsibility on civil society, i.e., mall owners and operators, ISPs, Internet content hosts. The law requires ISPs to install filtering software that will block access to web sites that contain child pornography. In addition, all operators and business establishments have to know and report any violation of the law in their premises.

Weak Enforcement. Weak or inconsistent enforcement also impede progress in deterring these crimes. Government officials all the way down to the grassroots levels should be vigilant and involved in enforcement. In this regard, the Anti-Child Pornography Act of 2009 authorizes the local government unit (LGU) of the city or municipality where an Internet café or kiosk is located to monitor and regulate the establishment and operation of the same in order to prevent violation of the provisions of the law.

The Anti-Child Pornography Act of 2009, however, is not without its own problems. First, it does not provide for educating law enforcers and government regulators to make them technology savvy. As the definition of "child pornography" expands from the traditional forms like videos or photographs to include digitally-created images and other representations, police and other law enforcers need better training on how to detect, apprehend, and prosecute the perpetrators. Similarly, training for prosecutors, lawyers, and judges on electronic commerce and cybercrime should be instituted.

Furthermore, the Anti-Child Pornography Act of 2009, by legislating access to the Internet, filtering of content and similar limitations, have raised concerns on its possible impact on the right to privacy, information and communication.

2.5 Domestic Legal Framework

(a) Definition of illegal child pornography;

To meet the challenges of the new landscape for child pornography brought about by the prevalence of the Internet, mobile phones, and related technology, the Philippine Congress passed into law Republic Act No. 9775, otherwise known as the "Anti-Child Pornography Act of 2009" on 19 November 2009. The said law makes it criminal for any person to: (a) hire, employ, use, persuade, induce or coerce a child to perform in the creation or production of child pornography; (b) produce, direct, manufacture, or create any form of child pornography and child pornography materials; (c) sell, offer, advertise, and promote child pornography and child pornography materials; (d) possess, download, purchase, reproduce, or make available child pornography materials with the intent of selling or distributing them; (e) publish, post, exhibit, disseminate, distribute, transmit, or broadcast child pornography or child pornography materials; (f) knowingly possess, view, download, purchase, or in any way take steps to procure, obtain or access for personal use child pornography materials; and (g) attempt to commit child pornography by luring or grooming a child.

(b) Privacy and data protection rules;

The Supreme Court has recognized the existence of a right to privacy as "accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection. It is expressly recognized in Section 3(1) of the Bill of Rights:

Section 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law."

Other zones of privacy are likewise recognized and protected in Philippine laws. The Civil Code provides that "[e]very person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons" and punishes as actionable torts several acts by a person of meddling and prying into the privacy of another. It also holds a public officer or employee or any private individual liable for damages for any violation of the rights and liberties of another person, and recognizes the privacy of letters and other private communications.

Republic Act No. 8792 (the "Electronic Commerce Act") provides that any person who obtains access to any electronic key, electronic data message or electronic documents, book, register, correspondence, information or other material shall not convey to or share the same with any other person.

In addition, the Philippines has a long-line of jurisprudence on prior restraint or censorship. Succinctly, content-based regulation bears a heavy presumption of invalidity and is measured against the clear and present danger rule. Such legislation will pass constitutional muster only if justified by a compelling reason, and the restrictions imposed are neither overbroad nor vague. Besides, "central to the first amendment due process is the notion that a judicial rather than an administrative determination of the character of the speech is necessary … Courts alone are competent to decide whether speech is constitutionally protected."

Sections 9 to 12 of the Anti-Child Pornography Act of 2009, however, attempts to provide broad exceptions to the protection afforded by the foregoing laws.

Section 9. Duties of an Internet Service Provider (ISP). – All Internet service providers (ISPs) shall notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person: Provided, that no ISP shall be held civilly liable for damages on account of any notice given in good faith in compliance with this section.

Furthermore, an ISP shall preserve such evidence for purpose of investigation and prosecution by relevant authorities.

An ISP shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an Internet address which contains any form of child pornography.

All ISPs shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered.

An ISP that shall knowingly, willfully and intentionally violate this provision shall be subject to the penalty provided under Section 15(k) of this Act.

The National Telecommunications Commission (NTC) shall promulgate within ninety (90) days from the effective date of this Act -- the necessary rules and regulations for the implementation of this provision which shall include, among others, the installation of filtering software that will block access to or transmission of any form of child pornography.

Section 10. Responsibility of Mall Owners/Operators and Owners or Lessors of Other Business Establishments. – All mall owners/operators and owners or lessors of other business establishments shall notify the PNP or the NBI within seven (7) days from obtaining facts and circumstances that child pornography is being committed in their premises. Provided, That public display of any form of child pornography within their premises is a conclusive presumption of the knowledge of the mall owners/operators and owners or lessors of other business establishments of the violation of this Act: Provided, further, That a disputable presumption of knowledge by mall owners/operators and owners or lessors of other business establishments should know or reasonably know that a violation of this Act is being committed in their premises.

Photo developers, information technology professionals, credit card companies and banks and any person who has direct knowledge of any form of child pornography activities shall have the duty to report any suspected child pornography materials or transactions to the proper authorities within seven (7) days from discovery thereof.

Any willful and intentional violation of this provision shall be subject to the penalty provided under Section 15(l) of this Act.

Section 11. Duties of an Internet Content Host. – An Internet content host shall:

(i) Not host any form of child pornography on its Internet address;

(ii) Within seven (7) days, report the presence of any form of child pornography, as well as the particulars of the person maintaining, hosting, distributing or in any manner contributing to such Internet address, to the proper authorities; and

(iii) Preserve such evidence for purposes of investigation and prosecution by relevant authorities.

An Internet content host shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an Internet address that contains any form of child pornography.

An Internet content host who shall knowingly, willfully and intentionally violate this provision shall be subject to the penalty provided under Section 15(j) of this Act: Provided, That the failure of the Internet content host to remove any form of child pornography within forty-eight (48) hours from receiving the notice that any form of child pornography is hitting its server shall be conclusive evidence of willful and intentional violation thereof.

Section 12. Authority to Regulate Internet Café or Kiosk. – The local government unit (LGU) of the city or municipality where an Internet café or kiosk is located shall have the authority to monitor and regulate the establishment and operation of the same or similar establishments in order to prevent violation of the provisions of this Act.

(c) Legislation establishing a legal framework for trusted third parties;

There is currently no specific law in the Philippines governing the collection and processing of personal data by trusted third parties. The Department of Trade and Industry ("DTI"), in an attempt to cure the lack of clear rules on privacy and data protection, recently issued Department Administrative Order No.8 ("Guidelines") prescribing the guidelines and accreditation criteria for the protection of personal data information and communications systems in the private sector. The guidelines provide, in relevant part:

(i) The relevant Data Protection Certifier must first be accredited by the DTI Accreditation Office to ensure that they utilize commercially appropriate and internationally recognized standards. It must comply with the responsibilities and accreditation criteria set forth by the guidelines.

(ii) Personal data must be collected for specified and legitimate purposes that must be processed accurately, fairly and lawfully. Inaccurate data must be corrected, destroyed or their processing must be restricted. It must not be excessive in relation to the purpose and must be kept for no longer than is necessary.

(iii) The criteria for lawful processing are:

(A) It must be freely given

(B) It is required by the contract

(C) The processing shall be permitted only to fulfill the intention of the parties

(D) The data is necessary to protect important interest

(i) Personal data may be disclosed to a data processor provided that there is a written contract between them. Prior to commencing the data processing, the data processor must perform safety measure in accordance with this Guidelines and the Electronic Commerce Law.

(ii) The data subject has the following rights:

(A) To be informed and notified

(B) The right to have the data corrected or destroyed

(C) The right to object if the data will be used for commercial purposes

(i) Access to personal data is limited to authorized personnel. It shall not be made available to any person without the consent of the individual or in the absence of a court order.

(ii) Any person who obtained access to any personal data has the obligation of confidentiality under the Electronic Commerce Law.

(iii) Security measures must be taken by the data controller and data processor to prevent any accidental or unlawful destruction, alteration, and disclosure as well as against any unlawful processing. The data controller shall process the personal data and his authorized representative muse comply with the security measures that was placed and must follow strictly the instructions given by him. The obligation of confidentiality exists between the data controller and his employees and will continue in effect even if they terminated their employment.

As mentioned above, however, the Anti-Child Pornography Act of 2009 creates an exception for certain merchants and establishments to disclose information about their clients. Section 10 provides that "photo developers, information technology professionals, credit card companies and banks and any person who has direct knowledge of any form of child pornography activities shall have the duty to report any suspected child pornography materials or transactions to the proper authorities within seven (7) days from discovery thereof." In turn, Section 11 provides that an Internet content host may disclose "the particulars of the person maintaining, hosting, distributing or in any manner contributing"

to an Internet address where child pornography may be found, and even the "particulars of users who gained or attempted to gain access to an Internet address that contains any form of child pornography."

(d) Criminal Law Aspects

Apart from the Anti-Child Pornography Act of 2009, the Philippines has several legislations that criminalise the exploitation of children.

Section 9 of R.A. No. 7610, otherwise known as the "Special Protection of Children against Abuse, Exploitation and Discrimination Act", penalizes any person who shall hire, employ, use, persuade, induce, or coerce a child to perform in obscene exhibitions and indecent shows, whether live or on video, or model in obscene publications or pornographic materials or to sell or distribute the said materials. All establishments and enterprises which promote or facilitate child prostitution and other sexual abuse, child trafficking, obscene publications and indecent shows, and other acts of abuse shall be immediately closed and their authority or license to operate cancelled, without prejudice to the owner or manager thereof being subject to further prosecution.

Republic Act No. 9262, otherwise known as the "Anti-Violence Against Women and Their Children Act of 2004", punishes any act that attempts to compel or compels a woman or her child to engage in conduct which the woman or her child has the right to desist from or desist from conduct which the woman or her child has the right to engage in, or attempting to restrict or restricting the woman's or her child's freedom of movement or conduct by force or threat of force, physical or other harm or threat of physical or other harm, or intimidation directed against the woman or child. "Sexual violence" refers to an act that is sexual in nature, committed against a woman or her child. It includes, but is not limited to rape, sexual harassment, acts of lasciviousness, treating a woman or her child as a sex object, making demeaning and sexually suggestive remarks, physically attacking the sexual parts of the victim's body, forcing her/him to watch obscene publications and indecent shows or forcing the woman or her child to do indecent acts and/or make films thereof.

In addition, under the Philippines' Revised Penal Code, the following are criminal acts:

Obscene Publications - Article 201 (as amended by P.D. No. 960 and P.D. No. 969) punishes anyone who exhibits indecent or immoral plays, scenes, acts or shows, whether live or in film, which are prescribed by virtue hereof, shall include those which serve no other purpose but to satisfy the market for violence, lust or pornography.

Corruption of Minors - Article 340 punishes any person who shall promote or facilitate the prostitution or corruption of persons underage to satisfy the lust of another.

Under Philippine criminal law, a juridical entity cannot be held liable for a crime. The Supreme Court, in an obiter dictum, has stated that no criminal action may lie against an accused who is a corporation because of the lack of the essential element of malice. The other reason why a corporation cannot be held criminally liable is the impossibility of imprisoning a corporation. Thus, when corporations violate penal laws, these violations are deemed to have been done by the corporate officer who is held personally liable for the violations committed on behalf of or through the corporation. Essentially, in the field of criminal law, the veil of corporate fiction will not shield the individual officers or directors of the corporation from their criminal acts done through the corporation.

For this reason, the Anti-Child Pornography Act of 2009 provides that if "the offender is a juridical person, the penalty shall be imposed upon the owner, manager, partner, member of the board of directors and/or any responsible officer who participated in the commission of the crime or shall have knowingly permitted or failed to prevent its commissions".

The law, however, also provides for the confiscation and forfeiture of the proceeds, tools and instruments used in child pornography. Such confiscated and forfeited proceeds, tools and instruments may answer for the award for damages if the personal and separate properties of the Offender are insufficient. Whether or not this means victims must first exhaust the properties of the owner, manager, or responsible officer before proceeding against the offender-corporation is unclear.

(e) Banking Secrecy Rules

Local Currency Deposits

R.A. No. 1405 (Bank Deposits' Secrecy Law) provides that all deposits of whatever nature with banks in the Philippines are absolutely confidential. Inquiries and examination of such deposits are prohibited, and bank officials are proscribed from disclosing any information concerning such deposits, except under the following circumstances:

(i) Upon written permission of the depositor; or

(ii) In cases of impeachment; or

(iii) Upon order of a competent court in cases of bribery or dereliction of duty; or

(iv) In cases where the money deposited or invested is the subject matter of the litigation.

The Supreme Court also held that bank deposits are to be "absolutely confidential" except: (1) in an examination made in the course of a special or general examination of a bank that is specifically authorized by the Monetary Board after being satisfied that there is reasonable ground to believe that a bank fraud or serious irregularity has been or is being committed and that it is necessary to look into the deposit to establish such fraud or irregularity, (2) in an examination made by an independent auditor hired by the bank to conduct its regular audit provided that the examination is for audit purposes only and the results thereof shall be for the exclusive use of the bank, (3) upon written permission of the depositor, (4) in cases of impeachment, (5) upon order of a competent court in cases of bribery or dereliction of duty of public officials, or (6) in cases where the money deposited or invested is the subject matter of the litigation.

Foreign Currency Deposits

Republic Act No. 6426 (The Foreign Currency Deposit Act) provides that foreign currency deposits are absolutely confidential. Inquiries and examination of such deposits are prohibited, and bank officials are proscribed from disclosing any information concerning such deposits, except with the written consent of the depositor.

Section 55 of General Banking Law of 2000 (RA 8791) prohibits the disclosure by any director, official, employee or agent of any bank any information relative to the funds or properties in the custody of the bank belonging to private individuals, corporations or any other entity, except upon court order.

Again, the Anti-Child Pornography Act of 2009 purports to create an exception by providing that, "… banks … have the duty to report any suspected child pornography materials or transactions to the proper authorities within seven (7) days from discovery thereof." Such provision appears to be vague or overbroad, however, and may not withstand judicial scrutiny. It is well-established that exceptions against common right and general rules are construed as strictly as possible.

(f) Termination of Contract / General Contract Law

In the absence of a breach of contract that would entitle the APAC Coalition Members to rescind the contract, the basis for termination must be stipulated in the contract itself.

Termination is a jurisprudentially recognized mode of extinguishing the obligations of a party to a contract. In the case of Huibonhoa, et al. v. Court of Appeals, the Supreme Court explained the effects of termination on the obligations of the parties:

Termination is a remedy whereby the parties are released from further obligations from each other, although still entailing enforcement of the terms of the contract prior to the declaration of its cancellation.

Termination, unlike resolution, can simply be agreed upon by the parties. As was held in the case of Pryce Corporation v. PAGCOR:

[t]ermination refers to an "end in time or existence; a close, cessation or conclusion." With respect to a lease or contract, it means an ending, usually before the end of the anticipated term of such lease or contract that may be effected by mutual agreement or by one party exercising one of its remedies as a consequence of the default of the other. (Emphasis supplied)

The parities can mutually agree to terminate a contract even without the commission of any breach of their respective obligations. In contrast, resolution/rescission is predicated on the existence of a substantial breach committed by at least one party of his obligations.

THAILAND

1. EXECUTIVE SUMMARY AND FULL JURISDICTION REPORT

1.1 International legal framework

Thailand does not have a specific law pertaining to the entry into treaties and other international agreements. Therefore, the process for entering into treaties and international agreements in the case of Thailand generally relies on the practice under international law on the law of treaties. In addition, the treaty making process is also governed by the Constitution, Cabinet resolutions relating to entering into treaties, regulations of the Prime Minister's office relating to proposing matters to the Cabinet and orders of the Ministry of Foreign Affairs. In Thailand, like in many other jurisdictions, the Constitution, as the supreme law of the land, is the principal law which provides the rules and framework for treaty making. All Constitutions of the Kingdom of Thailand, including the current Constitution of 2007, have provided the principal rule relating to treaty making for the Kingdom of Thailand, namely that the King has the royal prerogative to enter into treaties. This royal prerogative is exercised through the Cabinet, as the executive branch of government. Therefore, the power to enter into treaties with other countries, including bilateral and multilateral treaties, is the power of the executive, i.e. the Cabinet, and not the National Assembly (or Parliament). In addition, before becoming party to an international treaty, a domestic process must be undertaken. Pursuant to the Cabinet Resolution of 30 December 2003, the government agency responsible for the subject matter under a treaty is required to propose the treaty to the Ministry of Foreign Affairs for consultation and opinion and then to the Cabinet for consideration and approval before entering into the treaty in order to determine whether new domestic laws need to be enacted and whether parliamentary approval needs to be sought.

Whilst the power to enter into treaties is the power of the Executive, there are, however, certain types of treaties that must be approved by the National Assembly to be effective. Under section 190 of the 2007 Constitution (a provision perceived by some commentators as having caused a paralysing effect on the Executive), a treaty that provides for a change in the Thai territories or the extraterritorial areas in which Thailand has sovereign right or jurisdiction under any treaty or through international law, or requires the enactment of an act for its implementation, or has wide scale effects on the economic or social stability of the country, or results in a significant obligation on the trade, investment or budget of the country, must be approved by the National Assembly. In such case, the National Assembly must complete its consideration within sixty (60) days as from the date of receipt of such matter.

As a country with a dualist legal system, obligations under an international treaty to which Thailand becomes a party are not automatically enforceable within the Kingdom. The provisions have to be incorporated into Thai laws for them to be enforceable domestically. In practice, whether new domestic laws need to be enacted would be examined prior to becoming party to a treaty. In a number of cases, domestic laws would already exist. However, if it were found that existing laws were insufficient to enact the provisions of the treaty, the government would make the necessary legislative changes in order for Thailand to be compliant with the international obligations to which it is bound.

1.2 Mutual Legal Assistance Treaties

Thailand's Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992)[227] provides a framework for cooperation with other countries in matters relating to criminal justice. It allows other countries to

[227] http://www.inter.ago.go.th/UN/UN%20(E)/English/MLAT/The%20Act%20on%20Mutual%20assistance%20in%20Criminal%20%20Matters%202535.pdf

request assistance from Thailand through diplomatic channels, even in the absence of any bilateral treaty. The Attorney General's powers under the act including ordering the taking of testimony and statements of witnesses and providing evidence to the requesting country.

Thailand has also entered into bilateral mutual assistance treaties with a number of countries including the United States, Canada, the United Kingdom, France, Norway, India, China, South Korea, Peru, Sri Lanka, Poland, Belgium and Australia.

1.3 Subjects of Direct Relevance

(a) Sexual exploitation of children

(i) United Nations Convention on the Rights of the Child (**CRC**)

The Convention which details the fundamental rights that all nations must guarantee for their children was ratified by Thailand in March 1992, with reservations in relation to three articles: Article 7 on birth registration, Article 22 on children seeking refugee status and Article 29 on education. Thailand's reservation regarding these Articles is that their application would be subject to national laws, regulations and prevailing practices in Thailand. In 1997, Thailand withdrew its reservation to Article 29.

Article 34 of the CRC commits signatories to act to prevent "the exploitative use of children in pornographic performances and materials." This Article 34 has been enacted into Thai law by Article 26(9) of the Child Protection Act 2003. Please refer to our report on the domestic legal framework for further details.

(ii) The Stockholm Declaration and Agenda for Action

Thailand adopted the Stockholm Declaration and Agenda for Action in 1996 and reaffirmed its commitment in Yokohama in 2001. The Stockholm Declaration has been recognised by the Committee on the Right's of the Child, the UN Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography and in the Optional Protocol to the CRC on the Sale of Children.

(iii) Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography

In January 2006, Thailand acceded to the Optional Protocol on the Sof Children, Child Prostitution and Child Pornography. Whilst no new laws in these areas have been enacted in Thailand since 2006, the Child Protection Act of 2003, the Prevention and Suppression of Prostitution Act of 1996 and the Amendments to the Criminal Code of 1997 all address, to some extent, the subject matter covered in the Optional Protocol, although Thai law has, to date, not implemented a legal definition of "pornography" or "child pornography" for the purposes of more effectively preventing and prosecuting criminal activity in this area. Please refer to our report on the domestic legal framework for further details.

(iv) Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (the ***ILO Convention***)

This convention, adopted by the International Labour Organisation in 1999 was ratified by Thailand on 16 February 2001 and came into effect in Thailand the following year (February

2002). [***Note: see page 34 of the Hong Kong full jurisdiction report for more details on the ILO Convention***]

As with the CRC and the Optional Protocol, only the Child Protection Act has been enacted into law in Thailand since Thailand's ratification of the ILO Convention. In addition, the Prevention and Suppression of Prostitution Act of 1996 and the Amendments to the Criminal Code of 1997 address some of the worst forms of child labour mentioned in the ILO Convention. Please see our report on the domestic legal framework for more details.

(v) Other ILO conventions

Thailand has also ratified a number of other conventions of the ILO including the Forced Labour Convention and the Abolition of Forced Labour Convention, and the Minimum Age Convention.

(b) Cybercrime

(i) The Council of Europe Convention on Cybercrime (CET No. 185)

Thailand is not a signatory to the Council of Europe Convention on Cybercrime (CET No. 185), to which a handful of non-EU member states have acceded. For instance, Japan signed the Convention on 23 November 2001 but has not ratified it.[228]

The United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) policy document on Internet Use for Business Development published in Bangkok in 2007 includes a set of training modules for policymakers – they relate to all aspects of e-commerce including the use of digital and electronic signatures and the need for legislative framework for public key infrastructures and certification authorities.

Module 3 relates to cybercrime and security. It lists those countries that have anti-cybercrime laws (note that it was published before Thailand enacted its cybercrime law) and mentions innovative practices for combating cybercrime around the world. It states that the transnational nature of cybercrime requires international cooperation on laws and jurisdiction.

The Asia Pacific Economic Cooperation has also endorsed action items to combat cyber crime and ASEAN member countries have agreed to create an ASEAN network Security Coordination Centre that will help combat cyber crime and cyber terrorism.

The 27th ASEAN Chiefs of Police (ASEANAPOL) Conference was held from 4 to 6 June 2007 which saw the signing of the ASEANAPOL Joint Communique and the INTERPOL-ASEASNAPOL Declaration on Cooperation by the ASEAN Chiefs of Police. The Joint Communiqué detailed resolutions to cooperate in tackling regional security issues such as terrorism, cybercrime, commercial crimes and transnational frauds.

The Singapore police force is heading up the implementation of the proposed framework for capacity building against cybercrime in ASEAN. Singapore held a second run of the Cyber Crime Investigation Workshop from 8 to 10 April 2008 which was attended by local and overseas participants from Brunei, Cambodia, Indonesia, Laos, Malaysia, Thailand as well as France, South Korea and USA. With the theme "Fighting Cybercrime Across Borders – Building Partnerships", the workshop involved a presentation by the ASEAN nations of their

228 http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

specific Cybercrime Capability Roadmaps as well as discussions and sharing of best practices in combating cybercrime.

The ASEAN-EU Programme for Regional Integration Support – Phase II (APRIS II) organised a workshop on cybercrime legislation in the ASEAN Member States on 27 and 28 November 2008 in collaboration with the Council of Europe, the ASEAN Secretariat, the ASEAN Telecommunications Regulators Council and the Malaysian Communications and Multimedia Commission.

The objectives of the workshop were to support the development of national legislation on cybercrime in ASEAN, based on the content of the 2001 (Budapest) Convention on Cybercrime, which is considered to be the main international standard in the domain, to identify capacity building needs, and to encourage inter-and intra-regional dialogue, cooperation and information sharing in line with the goals of the ASEAN-EU Strategic Partnership launched at the 2007 ASEAN-EU Commemorative Summit in Singapore.

(c) Data Protection

There are no international laws or conventions but there are cooperative efforts to coordinate in this area.

(i) EU Data Protection Directive 1995

This directive applies to EU members but is open to signature by non-EU countries. In 2008 the Convention's Consultative Committee recommended that non-EU member states with data protection legislation should be allowed to accede to the Convention. Seven countries in the Asia-Pacific have passed privacy legislation that is closely aligned with the broad EU approach – Thailand's draft legislation referred to in the Thailand domestic section of our report falls within this category.

(ii) APEC Privacy Framework 2005

The principles-based APEC Privacy Framework provides guidance to businesses in Thailand.[229] The nine principles are as follows:

(A) Preventing Harm;

(B) Notice;

(C) Collection Limitations;

(D) Uses of Personal Information;

(E) Choice;

(F) Integrity of Personal Information;

(G) Security Safeguards;

(H) Access and Correction; and

(I) Accountability.

[229] APEC Privacy Framework - http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html

Rather than implementing the principles-approach of the APEC Privacy Framework, as noted above, Thailand has favoured the drafting of privacy legislation, which is more closely aligned to the structure of the EU Data Protection Directive 1995.

(iii) ASEAN

ASEAN has declared its commitment to the establishment of an integrated ASEAN Economic Community by 2015. A part of this is the commitment to develop a harmonised legal infrastructure for e-commerce according to its Roadmap for Integration of the e-ASEAN Sector.

(d) Payment flows / banking secrecy

To our knowledge there is no international framework on payment flows or banking secrecy expressly relevant to Thailand. The question of whether banking secrecy rules constitute an obstacle to the Coalition should be determined with reference to Thai national law. We would note however that an international framework aimed at combating the use of banking secrecy for the purposes of tax evasion has been established by the OECD and Thailand, unlike, for instance, Malaysia and Philippines, was not listed on the 2 April 2009 OECD blacklist of countries not having agreed to international tax standards.[230] The standards agreed upon by OECD and non-OECD countries and approved by the UN, create an obligation for banks and companies to keep reliable books and records and provide access to information about beneficial ownership and banking transactions.[231]

(e) Information flow from or between law enforcement to private parties

To our knowledge there is no international framework on information flow from or between law enforcement to private parties applicable to Thailand. Thailand's Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992)[232] addresses the transfer of information between Thailand and *foreign states* through diplomatic channels.

1.4 Subjects of Indirect Relevance

(a) Fundamental rights

(i) UN Convention on the Rights of the Child

Ratified by Thailand in 1992, the Convention details the fundamental rights that countries must guarantee for their children.

(ii) Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

Thailand acceded to the Optional Protocol in 2006 but has not ratified it.

(iii) Thailand is a signatory of the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights.

(iv) Thailand is a signatory of the Convention on the Elimination of all Forms of Discrimination Against Women and the Convention on the Elimination of All Forms of Racial Discrimination.

230 http://www.oecd.org/dataoecd/38/14/42497950.pdf

231 http://www.oecd.org/document/14/0,3343,en_2649_37427_42630286_1_1_1_1,00.html

232 http://www.amlo.go.th/richtext_file/File/MLAT_ENG.pdf

(v) Thailand is a signatory of the Hague Convention on the Civil Aspects of International Child Abduction and of the Hague Convention on the Protection of Children and Cooperation in Respect of Inter-country Adoption International.

(vi) The Working Group for an ASEAN Human Rights Mechanism

Thailand is a member of the ten-strong ASEAN organisation. At present there is no binding ASEAN agreement or treaty on universal human rights, though Article 14 of the ASEAN Charter calls for the creation of an ASEAN human rights body (the **AHRB**) which will protect and promote human rights and fundamental freedoms. Thailand may be in a position to oversee the launch of the AHRB during 2009, while ASEAN is under the chairmanship of Thailand. It is not anticipated that the AHRB would have the power to investigate or punish violators of human rights.[233]

(vii) The Asia Pacific Forum of National Human Rights Institutions

Thailand was admitted in 2002 to the Asia Pacific Forum of National Human Rights Institutions (**APF**), which supports the establishment and strengthening of national human rights institutions in the region. The APF aims to provide a framework for such institutions to cooperate on a regional basis on a range of issues (including combating child pornography).

(b) Money laundering

(i) The Egmont Group

The Anti-Money Laundering Office is a member of the Egmont Group of Financial Intelligence Units (FIUs) and has exchanged intelligence as well as signed bilateral memoranda of understanding on cooperation with FIU counterparts based in at least 23 countries.

(ii) Asia/Pacific Group on Money Laundering (**APG)**

Thailand is a member of APG, an associate member of the Financial Action Task Force on Money Laundering (**FATF**), and as such is committed to the effective implementation and enforcement of internationally accepted standards against money laundering, in particular the Forty Recommendations and Nine Special Recommendations on Terrorist Financing of the FATF.

There is no international framework on money laundering which is binding upon Thailand.

(c) Human trafficking

Bilateral

(i) MOU between Cambodia and Thailand (Thailand and Cambodia) on Bilateral Cooperation in Eliminating Trafficking in Children and Women and Assisting Victims of Trafficking 31 May 2003 (the Thai-Cambodia MOU)[234]

233 http://www.aseansec.org/HLP-OtherDoc-1.pdf

234 http://www.no-trafficking.org/content/PDF/thaicambodian_mou_on_ht.doc

(ii) MOU between Lao PDR and Thailand (Thailand and Lao PDR) on Cooperation to Combat Trafficking in Persons, Especially Women and Children 13 July 2005 (the Thailand-Lao PDR MOU)[235]

(iii) Treaty on Extradition between the Kingdom of Thailand and the Lao People's Democratic Republic (the Thai-Lao Extradition Treaty)[236]

Multilateral

(i) Coordinated Mekong Ministerial Initiative against Trafficking (COMMIT) Memorandum of Understanding on Cooperation Against Trafficking in Persons in the Greater Mekong Sub-region dated 29 October 2004 (the COMMIT MOU)

(ii) The COMMIT Sub-Regional Plan of Action Achievements in Combating Human Trafficking in the Greater Mekong Sub-Region, 2005-2007 dated December 2007 (COMMIT SPA I)

(iii) The COMMIT Sub-Regional Plan of Action Achievements in Combating Human Trafficking in the Greater Mekong Sub-Region, 2005-2007 dated December 2007 (COMMIT SPA II)

(iv) Asian Regional Initiative Against Trafficking (ARIAT) Plan of Action (ARIAT Action Plan) March 2000

(v) Regional Commitment and Action Plan of the East Asia and the Pacific Region (RCAPEAP) against Commercial Sexual Exploitation of Children (CSEC) (East Asia and the Pacific Regional Consultation for the Second World Congress against Commercial Sexual Exploitation of Children) October 2001[237]

(vi) ASEAN Declaration Against Trafficking in Persons Particularly Women and Children 29 November 2004 (ASEAN Declaration)[238]

(vii) Resolution No. Res 29GA/2008/Soc/06 On Establishment of AIPA Expert Working Group On Legal Cooperation to Combat Trafficking in Persons[239]

(viii) Medan Declaration to Combat Trafficking of Children For Sexual Purposes in Southeast Asia (South-East Asia Conference on Trafficking of Children for Sexual Purposes) 30 March 2004[240]

(ix) Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime, Senior Officials Meeting: Report to Ministers 7-8 June 2004[241]

(x) Bali Ministerial Process on People Smuggling, Trafficking in Persons and Related Transnational Crime: Co-chairs' Statement 29-30 April 2003[242]

---

235 http://www.no-trafficking.org/content/web/Content_20092005/Regional&National/2.2%20Regional/2.2.1.2%20Bilateral%20Agreements%20&%20Initiatives/tha_lao_hou_on_cooperation_to_combat_human_trafficking_eng.pdf

236 http://www.artipproject.org/05_laws/mou/bi/Extradition%20Treaty%20Thai-Lao%201999_English.pdf

237 http://www.no-trafficking.org/content/PDF/regional_commitment_and_action_plan_of_the_eap_region_agains.pdf

238 http://www.no-trafficking.org/content/pdf/asean_declaration_against_trafficking_in_persons_particu_1.doc

239 http://www.aipo.org/AIPA_NB/Twenty%20Ninth%20GA%20Res.htm

240 http://www.no-trafficking.org/content/PDF/medan_declaration.doc

241 http://www.no-trafficking.org/content/PDF/bali_process_som_report_78_june_2005.pdf

242 http://www.no-trafficking.org/content/PDF/bali_ministerial_conference_april_2930_2003.doc

(xi) Bali Ministerial Process on People Smuggling, Trafficking in Persons and Related Transnational Crime 26-28 February 2002[243]

(xii) Bangkok Accord and Plan of Action to Combat Trafficking in Women (Regional Conference on Trafficking in Women) 4 November 1998[244]

International

(i) United Nations Convention Against Transnational Organised Crime (2001)[245] (signed but not ratified)

(ii) UN Protocol to prevent, suppress and punish trafficking in persons, especially women and children, supplementing the United Nations Convention against Transnational Organised Crime (2001)[246] (signed but not ratified)

(iii) UN Recommended Principles and Guidelines on Human Rights and Human Trafficking, (2002)[247]

(iv) UN Protocol against the smuggling of migrants by land, sea and air, supplementing the United Nations Convention against Transnational Organized Crime (2001)[248]

(d) Evidence

Thailand has entered into bilateral extradition treaties with at least fourteen countries, including the United States, the United Kingdom, China, Cambodia and Laos. To our knowledge there is no international framework applicable to Thailand regarding the exchange of evidence. Whilst it is a piece of domestic legislation, Thailand's Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992)[249] addresses the transfer of evidence between Thailand and foreign states through diplomatic channels. Under the act, the Attorney General may order the Thai police commissioner to provide investigative assistance (e.g. taking statements, serving documents, search and seizure, locating persons) in response to a request by a foreign state and/or order the Thai chief public prosecutor to assist in obtaining for a foreign state witness testimonies and other evidence.

1.5 Domestic Legal Framework

(a) Definition of Illegal Child Pornography

There is no definition of "illegal child pornography" under Thai law. In addition, Thai law does not differentiate between material which is "obscene" and material which is "pornographic" and the same word is used for both meanings. Prohibitions against the production, distribution and trade in materials of a pornographic/obscene nature are contained in a number of different pieces of legislation.

Child Protection Act

243 http://www.no-trafficking.org/content/PDF/bali_ministerial_conference_february_2628_2002.doc
244 http://www.no-trafficking.org/content/PDF/bangkok_accord_and_plan_of_action.doc
245 http://www.artipproject.org/05_laws/int/UN_TOC_English.pdf
246 http://www1.umn.edu/humanrts/instree/trafficking.html
247 http://www.artipproject.org/05_laws/int/UN_PG_TIP_English.pdf
248 http://www.artipproject.org/05_laws/int/UN_%20OP%20Against%20the%20Smuggling%20of%20Migrants%202001_English.pdf
249 http://www.amlo.go.th/richtext_file/File/MLAT_ENG.pdf

In 2003, Thailand enacted the Child Protection Act which is the principal piece of legislation in Thailand providing for the protection of children. The Child Protection Act defines a child as a person below 18 years of age, not including those who have attained majority through marriage. Under the Civil and Commercial Code a person may marry at the age of 17 or before such age if in the court's view there is appropriate reason to allow it. Upon marriage such person attains majority. Section 19 of the Civil and Commercial Code states that a child is someone who is below the age of 20. We are of the view, however, that for the purposes of defining illegal child pornography the definition under the Child Protection Act would apply.

The Child Protection Act establishes the framework for intervention by the state for the protection of vulnerable children including orphans, street children, disabled children and children in difficult circumstances or at risk. Article 26 provides minimum standards of treatment of children including a list of forbidden acts against children. Under Article 26(9) it is prohibited to:

"force, threaten, use, induce, instigate, encourage or allow a child to perform or act in a pornographic manner, regardless of whether the intention is to obtain remuneration or anything else, and regardless of a child's consent." Breach of this prohibition carries a penalty of imprisonment of not more than 3 months or of a fine not exceeding Baht 30,000.

In addition, Article 27 provides it is forbidden for anyone to advertise or disseminate by means of the media or any kind of information technology any information on a child or the child's guardian, with the intention of causing damage to the mind, reputation, prestige or any other interests of the child or seeking benefit for oneself or others in an unlawful manner. Breach of this prohibition carries a penalty of imprisonment of not more than six months or a fine not exceeding Baht 60,000.

Although the intention of Article 27 appears to be to protect children against defamation, it could be argued that to sell or otherwise make available to the public pornographic/obscene images of children on the Internet would amount to disseminating for personal gain, information about a child that would be damaging to his or her interests and should therefore also fall within this prohibition. However, as there are no reported cases that deal with these provisions, this argument remains untested.

The Child Protection Act does not provide a definition of what is "pornographic"/"obscene". In addition, other than as described above, the Child Protection Act does not address the offences of producing, distributing, selling or otherwise profiting from child pornography. These offences are covered to some extent in the Criminal Code and in the Computer Act (see below).

The Child Protection Act states that if the same acts are prohibited under any other law of Thailand for which the penalties are greater then the more onerous penalties shall apply.

Criminal Code

Section 287 of the Thai Criminal Code relating to obscene materials provides that:

"*Whoever:*

(i) for the purpose of trade or by trade, for public distribution or exhibition, makes, produces, possesses, brings or causes to be brought into the Kingdom, sends or causes to be sent out of the Kingdom, takes away or causes to be taken away, or circulates by any means whatever, any document, drawing, print, painting, printed matter, picture, poster, symbol, photograph, cinematograph film, noise tape, picture tape or any other thing which is obscene,

(ii) carries on trade, or takes part or participates in the trade concerning the aforesaid obscene material or thing, or distributes or exhibits to the public, or hires out such material or thing,

(iii) in order to assist in the circulation or trading of the aforesaid obscene material or thing, propagates or spreads the news by any means whatever that there is a person committing the act which is an offence according to this Section, or propagates or spreads the news that the aforesaid obscene material or thing may be obtained from any person or by any means,

shall be punished with imprisonment not exceeding three years or a fine not exceeding six thousand baht, or both."

In Judgement No. 978/2492 the Supreme Court of Thailand defined "obscene" as "anything that is sexually shameful to the eyes or offensive which is the direct opposite of artistic expression". A more recent case (Judgement No. 6301/2533 of the Supreme Court) provided a more explicitly descriptive definition of "obscene" for the purposes of the case (which concerned an image of an adult woman) and described the relevant image as "obscene" on the grounds, inter alia, that "it is intended to incite wanton sexual desire".

In terms of content, child pornography would therefore be considered "obscene" under this section of the Criminal Code. In terms of medium it should be noted that Section 287 does not expressly include digital data transmitted over the Internet although the applicability of this Section to such material could be implied under the terms "picture" or "photograph" and in the general prohibition on propagation "by whatever means". Accordingly, the distribution of child pornography over the Internet would be caught by Section 287 of the Criminal Code.

Section 279 punishes anyone who commits an indecent act against a child under the age of 15 by threat or violence or by taking advantage of such person being in the condition of lacking the ability to resist. Any such offence committed against a child over the age of 15 would be caught by Section 278.

In addition Sections 282, 283 and 284 punish anyone who procures, seduces or takes away a child who is under 15, or over 15 but not yet 18, for another person's sexual gratification, whether with the child's consent or whether by any deceitful, threatening, violent or unjust means. These offences extend to the person who obtains the procured child, or to any person who assists the offence as a supporter (see below).

Under Section 84 of the Criminal Code a person who, by employment, compulsion, threat, hire asking as a favour or instigation or by any other means, causes another person to commit any offence is said to be an instigator and shall receive punishment for the offence as the principal offender.

Under Section 86 of the Criminal Code, a person who by whatever means does any act to assist or facilitate the commission of an offence of any other person, even though the offender does not know of such assistance, is said to be a supporter to such offence and shall be held liable to two thirds of the punishment provided for such offence.

The above offences would cover any person who procures children for the purposes of producing pornography and any person who commits an indecent act against the child in the course of producing pornography. Section 86 would cover any person who facilitates as a supporter the procurement of the child or the indecent act against the child in the production of pornography, while Section 84 would cover the producer of child pornography as the instigator of the crimes of procurement and indecent assault against the child. It is questionable whether, for example, a cameraman filming an indecent assault against a child in the production of pornography would be regarded as a supporter or instigator of the offence.

The offence of any person who profits from the distribution of child pornography would be caught by Section 287 as described above.

Computer Act

Thailand's Act on Commission of an Offence relating to Computer enacted in 2007 (the Computer Act), specifically addresses cybercriminal offences:

Section 14 of the Computer Act provides that *'Any person who commits any of the following offences shall be liable to imprisonment for a term not exceeding five years or a fine not exceeding THB100,000, or both. ...(4) entering any computer data of pornographic characteristics into a computer system and that computer data being accessible by the public; (5) publicise or forward computer data despite knowing that it is computer data under (1), (2), (3) or (4) above*.

"Computer data" is defined under the Computer Act as "data, message, command, program or all other things in the computer system that are able to be processed by a computer system, including electronic data under the law on electronic transactions" (i.e. the Electronic Transactions Act of 2001).

The Electronic Transactions Act defines "electronic data" as "a message which is generated, sent, received, stored or processed by electronic means such as electronic data interchange, electronic mail, telegram, telex or facsimile". "Message" means "any narrative or fact regardless of whether it appears in the form of alphabetic letters, numbers, voice, visual image or other form capable of communicating a meaning by itself or through any media".

Accordingly, digital images of a pornographic nature (whether involving children or otherwise) that are entered into a computer system or uploaded onto the Internet will be caught by Section 14 of the Computer Act. Unfortunately, the Computer Act does not provide a definition of "pornographic"/"obscene" and as the law was enacted only in 2007 there has as yet been no case law from the Supreme Court in this regard. However as compared to Section 287 of the Criminal Code and the provisions of the Child Protection Act, it offers more onerous sanctions for offenders under Section 14 as well as being more clearly applicable to Internet-based pornography.

The offences addressed in Section 14 of the Computer Act are limited to the uploading, publicising and distribution of pornographic images on an Internet website and do not include the downloading or simple possession of such images, which accordingly are not offences under Thai law.

Section 15 of the Computer Act provides that any service provider who wilfully supports or consents to the commission of an offence under section 14 through a computer system that is in his/her control shall be liable to the same punishment as an offender under section 14. "Internet Service Provider" is defined as one who provides an Internet access service or any other service that enables communication via computer system irrespective of whether he provides the service on his own behalf or on behalf of or for the benefit of others. It also includes one who provides computer data storage services for the benefit of others. We understand that Internet service providers will form part of the APAC Coalition.

Under Section 17 of the Computer Act an offence taking place outside of Thailand will be prosecuted in Thailand if (i) the offender is a Thai person, and there is a request for punishment by the government of the country where the offence has occurred or by the injured person; or (ii) the offender is an alien, and the Thai Government or a Thai person is the injured person, and there is a request for punishment by the injured person.

The APAC Coalition Case-study

Thai law does not penalise the simple possession of pornographic items by a person with no intention of engaging in commercial or public distribution or exhibition of such items. However for the purposes of the case study we have also considered the following:

(i) whether by purchasing and assisting in the purchase of pornographic material the APAC Coalition can be said to be "taking part" in the trade of obscene materials under Section 287 of the Criminal Code. There is no case law indicating what would constitute "taking part" in the trade of obscene materials and whether purchasing such materials, allowing the materials to be sold on an Internet service provider's service, or supporting the purchase of such materials by way of payment services would be caught by this provision. Generally speaking, Thai criminal law requires there to be unlawful intention for a crime to be committed and the burden of proving such unlawful intention would be on the prosecuting party. In such case, given that there would be no unlawful intention on the part of the APAC Coalition in purchasing the pornographic materials or allowing the sale and purchase of such materials over the Internet, then they cannot be found to have committed a crime under Thai law;

(ii) whether by assisting in the identification of the website and the purchase of pornographic material the Internet service provider can be said to have "wilfully" consented to or supported the crimes under Section 14 of the Computer Act. Again there is no case law on this issue. Given the emphasis on intention in Section 15 of the Computer Act it is unlikely that any Internet service providers forming part of the Coalition and carrying out the actions contemplated by the case-study would fall foul of this provision; and

(iii) whether by passing images from a child pornography website to the law enforcement authorities or to the other APAC Coalition Members, the APAC Coalition would be in breach of Article 27 of the Child Protection Act. This provision specifically requires there to be unlawful intention in the commission of the prohibited act therefore it is unlikely that the APAC Coalition would be in breach of this Article in carrying out the actions contemplated by the case-study.

(b) Data Protection and Privacy

We understand that under the case study, information about the Offender such as account information, personal data (i.e. name and/or address) will be collected and communicated to members of the Coalition and members of law enforcement agencies in Thailand. There is no privacy or data protection law currently in force in Thailand although a data protection bill is under consultative drafting. In addition, personal data may be protected under other laws of Thailand.

The Data Protection Bill

The National IT Committee and the National Electronic and Computer Technology Center (NECTEC) approved plans in early 1998 for a series of information technology and e-commerce laws, including the Data Protection Bill (the Bill).

Currently, Thailand is in the process of drafting the Bill. As the Bill is still in the drafting stages, it is difficult to estimate when the Bill will be enacted. Following our discussions with the relevant officials, the Bill is unlikely to become effective this year. We also understand from the various press releases that the Bill is intended to follow internationally accepted principles on confidentiality such as those enshrined in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The objective of the Bill is to balance privacy rights with the freedom to exploit information technology, so that the right of privacy regarding personal data is sufficiently protected from unauthorized interference, and the commercial development of information technology as a marketing tool is not unreasonably hindered. The Bill provides protection for the personal data of individuals based on the following key principles: consent, notice, purpose specification, use limitation, accuracy, access, security and enforcement.

In the meantime, under Thai law the individual's right to privacy is protected by the Constitution of Thailand and the provisions relating to data protection found in the relevant various pieces of legislation described below.

The Civil and Commercial Code

Section 420 of the Civil and Commercial Code provides that "a person who, willfully or negligently and unlawfully, injures the life, body, health, freedom, property or any right of another person is considered to have committed a tort and therefore bound to compensate that person for such offence."

Any person who infringes upon another person's privacy by disclosing the personal information of its customers to a third party "without having an authority under Thai law or under a contract between the parties" is likely to be considered to have committed a tort under Section 420 of the Civil and Commercial Code. Any person who commits a tort is liable to pay compensation for damages that arise therefrom and the onus is on the claimant to prove that the injury incurred as a result of the unauthorised disclosure of personal information.

In our view, the disclosure by the Coalition of the personal data of the Offender to any law enforcement agency of the Thai State, is unlikely to be considered a tort. This is because such action is lawfully done. However, there is a risk that the disclosure of personal data of the Offender to other Coalition Members would amount to a tort under Section 420.

(c) Defamation

Criminal Code

There are a number of sections in the Criminal Code which provide for offences in connection with disclosure or theft of personal information. However, their applicability is limited to very specific circumstances and would be of limited relevance to the case-study. It is however worth mentioning the crime of defamation which carries relatively heavy penalties under Thai law.

Section 326 provides that "any person who talks to a third party with the intention of defaming another person, causing that person to be degraded or despised has committed a slander and shall be liable to imprisonment for a term of not exceeding one year or a fine of not more than 20,000 Baht, or both."

Intent is an essential part of a criminal offence. In order to constitute slander, a person must disclose customer information with the intent to defame its customer and in such a way as may cause the customer to be defamed. Without the intent and such effect, disclosure of customer information would not constitute a criminal offence.

Constitution of the Kingdom of Thailand 2007

Of less relevance is the Constitution of Thailand which provides a general right to privacy and to be protected against defamation. The Constitution of Thailand does not however in itself give individuals a right of action against another.

Computer Act

The Computer Act gives the competent official (being the relevant official appointed by the Minister of Information and Communication Technology) the power to order the submission by an Internet service provider of personal information, computer data and computer traffic data relating to an alleged Offender for the purposes of investigation and evidence. The competent official has an obligation not to disclose such personal information, computer data or computer traffic data to any person. However this prohibition does not apply in carrying out any legal action against an offender under the Computer Act, or in accordance with the order or permission of the court.

The competent official may order the service provider to maintain computer traffic data for more than ninety days but not more than one year. The service provider is also obliged to maintain client data which is necessary for identifying a client from the first use of the services and must maintain such data for not less than ninety days as from the end date of the services.

The provisions of the Computer Act with regard to collecting personal data of an alleged Offender and the powers of the competent official in this regard would be useful to the Coalition in carrying out the undercover operation detailed in the case study.

(d) Banking Secrecy Rules

It is one of the central tenets underpinning Thai banking laws that banks and other financial institutions ("**Financial Institution**") must keep customer data confidential regardless of whether the client is an individual or a legal entity. There are a number of pieces of legislation that include banking secrecy rules aimed at protecting the personal and credit data of customers.

The Financial Institutions Business Act

The Financial Institutions Business Act applies to Financial Institutions which are defined under the Act as banks, finance companies and credit financiers.

Sections 154-155 of the Financial Institutions Business Act B.E. 2544 (2001) prohibit a person who knows information relating to any business of a Financial Institution from revealing such information to third parties, except for:

(i) disclosure required by law or for the purposes of a criminal investigation or court hearing;

(ii) disclosure of any crime committed under this Act;

(iii) disclosure to the auditor of such Financial Institution or to a domestic agency or foreign agency having the power to regulate such Financial Institution;

(iv) disclosure for the purposes of compliance with a domestic agency or foreign agency having the power to regulate Financial Institutions according to an agreement between such agencies;

(v) disclosure for the purposes of improving the Financial Institution's finance;

(vi) disclosure for the purposes of obtaining an approval of loan of Financial Institution;

(vii) disclosure of customers' data that was already in the public domain;

(viii) disclosure of customers' data for which consent was already given by the customers;

(ix) disclosure to a company being in the same financial business sector; and

(x) disclosure for the purposes of compliance under the law.

We note that the exceptions to the banking secrecy rule as provided under the Financial Institutions Business Act are widely drafted and would allow the Coalition to pass on customer data both to law enforcement agencies (under (i) above) and to other members of the Coalition that are also Financial Institutions (under (ix) above). However, under regulations applying specifically to electronic transactions, described below, the exceptions to the banking secrecy rule are much narrower.

Electronic Transaction Committee Regulation

The Electronic Transaction Committee Regulation applies to Service Providers under the regulation, which are defined as persons or entities providing any business service as stipulated in the Royal Decree re: Control of Electronic Payment Business B.E. 2551. A Service Provider may therefore include the providers of electronic data capture networks, credit card networks or any type of electronic money.

The Electronic Transactions Commission appointed under the Electronic Transactions Act B.E. 2544 (2001) issued the Electronic Transaction Committee Regulation on 30 January 2009 (the Electronic Transactions Regulation), Article 10 of which provides that data on customers shall be kept strictly confidential, except for:

(i) disclosure with the written consent or any form of electronic consent indicated by Financial Institutions from the customer;

(ii) disclosure for the purposes of an investigation or court hearing;

(iii) disclosure to the auditor of such Financial Institution;

(iv) disclosure for the purposes of legal compliance; and

(v) disclosure for the purposes of a regulation of the Bank of Thailand

Under the Electronic Transactions Regulation, the Coalition Member having personal data of the alleged Offender would only be permitted to disclose such data to the law enforcement agencies or other relevant authorities. It would not be permitted to disclose the data to other Coalition Members.

Credit Card Company Act

The Credit Card Company Act applies to Credit Information Companies. A Credit Information Company is a company that has obtained a licence to do Credit Information Business. Credit Information Business includes any business activities which involve collecting information identifying a customer or the qualifications of a customer, requesting applications for finance or details of finance history, approving finance applications or requesting details of credit card usage and repayment.

The Credit Card Company Act B.E. 2545 ("CCC") imposes an obligation on a credit company, its employees and agents to keep banking secrets. However, the CCC specifies the circumstances in which a credit card company may disclose customers' data acquired while carrying out its professional activity which are as follows:

(i) disclosure for the purposes of legal compliance;

(ii) disclosure for the purposes of an investigation or court hearing;

(iii) disclosure for the purpose of performing under the CCC;

(iv) disclosure to a government or to a domestic agency having the power to regulate Financial Institutions or any other person having jurisdiction;

(v) disclosure with the written consent of the customer; and

(vi) disclosure of customers' data relating to any claim filed in a court that was already revealed to the public.

Sanctions

Under the Financial Institutions Business Act, a violator of the banking secrecy rules may be subject to imprisonment for a term not exceeding 1 year and/or a fine not exceeding Baht 100,000. Moreover, under the Electronic Transactions Act B.E. 2544 (2001) together with the Electronic Transactions Decree B.E. 2551 (2008), a violator of the banking secrecy rules may be subject to an administrative fine. Where there is seen to be a continuing breach of the banking secrecy rules, the administrative authority may issue an order to the Financial Institution to cease its businesses and/or may terminate its license to operate as a business in the financial services sector. A violator of the banking secrecy rules under the CCC may be subject to imprisonment for a term of 5 to 10 years and/or a fine not exceeding Baht 500,000.

Summary

The basic principal of Thai law is to protect the privacy of account holders and the disclosure of details of an alleged Offender to third parties is generally prohibited under Thai law. However, such protection is limited and indeed explicit provisions have been established requiring Financial Institutions to set aside the secrecy rights of the individual (personal or corporate) in certain circumstances. Based on the exceptions set out above, customer data on the Offender may be disclosed to a law enforcement agency for the purposes of an investigation or court hearing. Data on the Offender may also be disclosed to a competent official as appointed under the Computer Act for the purposes of legal compliance with the Computer Act if applicable. However, disclosure to other Coalition Members would not be permissible.

Breach of the banking secrecy rules by the Coalition Members may result in administrative sanctions and such sanctions would presumably dissuade any disclosing of relevant information other than as permitted under the regulations.

(e) Termination of Contract and other Contract Law Issues

General Principles

Thai law does not provide the grounds for rescission of a contract other than for non-performance by one party of its obligations within the time stipulated under the contract, and for impossibility. Generally speaking, the rights of termination of the parties to a contract will be set out in the contract itself. The extent to which APAC Coalition Members could terminate their services to the Offender would therefore depend on the terms of each service contract.

Illegality

Section 150 of the Civil and Commercial Code of Thailand (the CCC), provides that a legal transaction having an objective which is prohibited by law or is contrary to public policy or good morals is void. In general, the motive of one party in entering into a legal transaction will not be regarded as an

objective of the legal transaction unless the motive is discovered by the other party (the Supreme Court's decision no. 1124/2512). In the Supreme Court's decision no. 707/2487 and 358/2511, the court held that a loan given to finance illegal drugs trading is void and a loan advanced to pay for an assault service is void since the objectives of the loans are prohibited by law. Under this illegality provision therefore any contract between the Offender and the APAC Members which is used for the purposes of trading in illegal child pornography will only become void for illegality once the APAC Member has discovered the Offender and the Offender's activities. Moreover, whilst the illegality provision would render the relevant sale and purchase transactions void the underlying service contract with the APAC Member would not be affected.

Current Account

Where the underlying service contract is for the setting up and use of a current account, Section 859 of the Civil and Commercial Code provides that in the absence of anything appearing to the contrary in the contract either party may at any time terminate a contract of current account and have the balance struck.