Bills Committee on Unsolicited Electronic Messages Bill

Summary of views submitted to the Bills Committee and the Administration's response
(Position as at 27 October 2006)

(I)	**General**		
(1)	***Opt-out regime***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
1.1.1	Hong Kong Direct Marketing Association (HKDMA) Asia Digital Marketing Association (ADMA)	Support the proposed opt-out regime.	"Opt-in" and "opt-out" regimes have their pros and cons, as recognised globally. We consider the "opt-out" regime to be more suitable to Hong Kong's circumstances, where 98% of business establishments are SMEs employing 60% of the working population. SMEs would need room to take advantage of the low cost e-communications channel to market their products or services. Furthermore, the US Federal Trade Commission (FTC), on examining the data from an international e-mail filtering company on the volume of spam e-mails received in UK, which imposes an opt-in regime, believed that an opt-in regime in the UK has not decreased the amount of spam e-mail UK citizens receive. Thus, it is probably inconclusive from overseas experience as to whether an opt-in or opt-out regime is more effective at protecting its community from spam. The key issue is that recipients of commercial electronic messages can exercise their right to refuse further messages and the "opt-out" regime can deliver such an arrangement.
1.1.2	Consumer Council (CC) Hong Kong Computer Society (HKCS) Paul Gardiner	Support an opt-in regime.	

(2)	***Party to be charged***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
1.2.1	Tseung Kwan O District Environment Concern Group (TKODECG)	All costs must be borne by the senders of commercial electronic messages.	It is a common arrangement among mobile operators throughout the world that roaming fees are charged to the called party because the caller is unable to know in advance where the called party is. From a practical point of view, if the roaming charges are to be paid by the calling party, the operator would need to inform him and seek his consent before making the connection. This may have implications on the called party's privacy. To provide a remedy for the called party who may suffer losses due to contravention of the Bill, he may take civil action under the Bill against the caller and seek just and equitable remedies.
1.2.2	張國衡、趙祥貴	The telemarketers should pay the mobile service charge for the recipient so as to increase their cost of sending unsolicited electronic messages.	
1.2.3	CC	Suggest instigating a caller-party charging scheme to encourage telemarketers to be more selective when sending out messages.	
(3)	***Harmonisation with overseas anti-spam laws***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
1.3.1	The American Chamber of Commerce in Hong Kong (ACCHK) (verbal) Business Software Alliance (BSA)	The UEM Bill should harmonise with overseas anti-spam laws where possible. Inconsistencies present major difficulties for the development by multinationals of global compliance procedures.	In drafting of the UEM Bill, we have reviewed many overseas anti-spam laws, and exchanged experience with enforcement agencies of different countries. It is observed that these anti-spam laws vary widely in terms of regime and scope, for example, opt-out vs opt-in, criminal offence vs civil claim, etc. While we have made references to other overseas anti-spam laws, the proposals in the Bill are made having regard to the views received during the public consultations and the particular situation in Hong Kong.

(4)	***Enforceability***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
1.4.1	CC	Suggests expediting international co-operation to tackle the problem of extra-territorial enforcement.	Identifying and bringing to justice spammers sending unsolicited e-mails to Hong Kong could be difficult under the Bill. We need co-operation with overseas enforcement agencies. The Government has been actively developing such co-operation with overseas anti-spam bodies. Clause 34(5)(b)(iii) of the Bill seeks to empower the enforcement agency to exchange information with overseas counterparts to fulfil obligations under relevant international agreements. If any future international agreements require other reciprocal arrangements that need to be empowered in the Bill, we will seek amendments to Bill.
1.4.2	HKCS	Clause 34(5)(b)(iii) may be insufficient to allow full reciprocal cooperation with any other countries that elect to introduce similar legislation.	
1.4.3	Paul Gardiner 張國衡、趙祥貴	Concerned about how the Bill can be enforced against overseas organisations.	
(5)	***Coverage of the Bill***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
1.5.1	Wharf T&T Limited (WTT)	The Bill should adopt a targeted approach by regulating the sending of electronic messages of general commercial nature, i.e. the content of the message is about offering or promoting goods or services for furtherance of business.	Noted.
1.5.2	HKCS	The Bill advises a targeted approach, "the content of the message is about offering or promoting goods or services for furtherance of business", but this is not necessary and sometimes dangerous. The correct criterion is whether the message is solicited.	We consider that the messages of a commercial nature form the bulk of the problem of UEMs and therefore the legislation should first and foremost target them. This is in line with anti-spam laws in major overseas economies and ensures that freedom of speech and expression will not be unnecessarily impaired.

1.5.3	The British Computer Society (Hong Kong Section) (BCS(HK)) (verbal)	No need to differentiate "commercial" and "non-commercial" messages as they are usually very difficult to distinguish.	For reasons explained in item 1.5.2, we consider that the legislation should first and foremost target messages of a commercial nature. As a result, it becomes necessary to distinguish between "commercial" and "non-commercial messages. The definition of "commercial electronic messages in Clause 2 is intended to serve this purpose by defining the types of commercial messages which are intended to be covered by the Bill. Whether or not an electronic message will fall within the definition will depend on the facts of the particular case.
1.5.4	HK CAS/COM Joint Chapter of IEEE (verbal)	The scope of the UEM Bill should cover non-commercial illicit spams by extending Part 3 of the Bill to both commercial and non-commercial messages. Alternatively, the Bill should be re-named as "Unsolicited Commercial Electronic Messages Bill" so that the general public will not be misled in a way that the Bill is targeted to solve all the problem of spams.	
1.5.5	徐小姐	The Bill should not regulate e-mail and fax because they are low cost advertising channels for the small and medium size enterprises.	The Bill only requires that a sender of commercial electronic messages respect the wish of the recipient. E-mail and fax advertisements can still be sent until the recipient decides not to receive further messages.
1.5.6	Civic Party	Most organizations in Hong Kong, including political parties, non-governmental organisations and charitable organizations are registered under Companies Ordinance and regarded as carrying on a business. It would be possible that organisations might be caught offending the law whilst promoting their organisations. Suggest making it clear by defining "commercial" or "business" as not including the aforesaid organisations.	The Bill does not propose to provide exemption to any organisation. Instead, the application of the Bill intends to focus on the contents of the message, i.e. whether there is a commercial element in the sense described in the definition of "commercial electronic message", rather than the nature of the organisation which sends the message.

1.5.7	Civic Party	Concerned that the business of polling agents would be regulated by the Bill. Suggests making it clear that polling is not regulated under the Bill.	A pure polling message (e.g. to solicit people's opinion about a policy) without any promotional / advertising elements, or any inducement for further business, will not amount to a "commercial electronic message" under the Bill.
1.5.8	HKDMA ADMA	Recipients should be provided the right to opt out of receiving political, religious or charitable communications.	For the reasons explained in item 1.5.2, we consider that the legislation should first and foremost target messages of a commercial nature. The Bill is not intended to apply to political, religious or charitable communications which do not have a commercial element in the sense described in the definition of "commercial electronic message".
1.5.9	HKCS	There should be no exemption for charitable organisations or the Government from the requirement to manage address lists properly.	The Bill does not provide exemption for individual organisations.
(6)	***Drafting Style***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
1.6.1	CSL/New World Mobility (CSL/NWM)	Suggests including all interpretation provision under Part One of the Bill.	The interpretation provisions that apply to only a single Part of the Bill have been inserted into the relevant Part. This is not an unusual drafting practice and is intended to make the Bill easier to read and understand as a whole. We will further consider if Members have a preference to insert all the interpretation provisions in Part 1 of the Bill.
1.6.2	CSL/NWM	The Bill should not use gender specific drafting.	It is not a requirement that gender specific language should not be used in our legislation. We can rely on section 7(1) of the Interpretation and General Clauses Ordinance (Cap. 1) which states that "words and expressions importing the masculine gender include the feminine and neuter genders."

(7)	***Resources and Expertise for Enforcement***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
1.7.1	HKCS WTT	Raises questions on whether the TA has sufficient resources, investigative and technical level expertise to enforce the Bill.	We consider that OFTA is an appropriate organisation to be the enforcement agency for Part 2 and Part 3 of the UEM Bill. Part of OFTA's duty is to investigate into telecom-related offences which are of a criminal nature. OFTA therefore possesses the necessary criminal investigation experience and expertise in telecom-related areas. OFTA will be working closely with the HK Police Force which has substantial expertise in IT forensic skills.
(8)	***Other general views/concerns***		
1.8.1	WTT	There is a need to strike a balance between respecting the right of a recipient to refuse further UEMs and allowing electronic marketing to develop in Hong Kong as a legitimate promotion channel as advocated by various business entities including the small and medium enterprises.	Noted.
(II)	**Part 1 - Interpretation and meaning of terms, exclusions**		
(1)	***Definition of "Electronic Address"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.1.1	HKCS	The inclusion of Internet Protocol address in the definition of "electronic address" will have far-reaching implications. One very significant type of electronic traffic which is deemed to be commercial is Web traffic. The proposed definition could encapsulate websites under the control of the Bill.	As web pages are displayed in response to requests made by viewers (e.g. by entering an Internet Protocol address or a domain name, or by clicking a hyperlink on a webpage), we do not intend to cover website traffic under the Bill. We will consider if further clarification is necessary to exclude such type of web traffic from the scope of the Bill.

(2)	***Definition of "Electronic Message"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.2.1	Doctor First Centre Limited (DFC) (verbal)	The current definition of "electronic message" may be too wide that potentially covers TV commercials and electronic billboards.	Advertisements on TV are part of the television programme services regulated under the Broadcasting Ordinance and hence would be excluded from the application of the Bill by virtue of Item 3 of Schedule 1. Similarly, advertisements on radio are part of the sound broadcasting services under the Telecommunications Ordinance and hence would be excluded from the application of the Bill by virtue of Item 4 of Schedule 1.
(3)	***Definition of "Commercial Electronic Message"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.3.1	HKDMA ADMA BSA HKASC ACCHK (verbal) CSL/NWM	The current definition of "commercial electronic messages" is too broad and may cover newsletters whose primary purpose is to inform but may at the same time carry small advertisements, or electronic invoices accompanied by discount coupon for future purposes. Suggests that "commercial electronic messages" should be defined as those messages whose "primary purpose" is to promote and sell goods or services etc.	We consider that the "primary purpose" test could result in ambiguity and argument on whether the requirements of the proposed Bill should be applicable to specific messages. Unscrupulous senders may exploit this ambiguity to send advertisements in messages accompanied by other messages of irrelevant primary purpose. In such case, recipients would have no way to refuse receiving these partially commercial messages.

2.3.2	HKCS	Bills and invoices would be excluded if the Bill used "solicited" instead of "commercial" as the criterion. However, exempting bills and invoices could leave a potential loophole – sender could copy a real invoice for one of their customers to an unlimited number of other recipients with a view to promoting its products or services with pricing.	A pure transactional or service-related message (e.g. an invoice or bill or welcome message) without any elements to promote or advertise products or services, or any inducement for furthering business, will not amount to a "commercial electronic message" under the Bill.
2.3.3	WTT	Certain flexibility should be allowed in order to exempt certain commercial electronic messages from compliance, i.e. bills or invoices from a business entity should fall outside the scope of the Bill.	
2.3.4	Stevenson, Wong & Co (SWC)	There are situations where spammers sent emails informing that a person has won a lucky draw and ask the person to contact the spammers for redemption of the lucky draw price. It is recommended that the definition of commercial electronic message should be widened by adding a new category as "to obtain, assist to obtain, or attempt to obtain any gain, benefit or advantage in the course of or in the furtherance of any business".	We will consider whether an expansion of the definition of "commercial electronic messages" is necessary.
(4)	***Meaning of "Hong Kong link"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.4.1	HKDMA ADMA	Support the proposed coverage of "Hong Kong link", although it is not clear how any-territorial application will be handled and how effective they will be.	Noted. OFTA will develop cooperation channels with overseas anti-spam agencies with a view to identifying overseas spammers and prosecuting them as far as possible.

2.4.2	HKCS SWC	The definition of Hong Kong link should cover messages that pass through Hong Kong. The current definition could result in Hong Kong becoming a haven for open relays.	Coverage extended to “transmitted via HK” may result in casting the net too wide. Current technology allows a network to use the most efficient route, without the knowledge of the sender. It is possible that a message could be in compliance with the laws of both the sending and receiving jurisdictions, but in violation of the Bill due to the "transmit through" element. It is not appropriate to criminalise open relays/proxies (sometimes may be a result of misconfiguration) and they can be prevented or addressed by other measures such as regulatory measures.
2.4.3	HKCS	Recommends adding under section 3(1)(e) the registrar for the “.hk” domain, currently, Hong Kong Domain Name Registration Company Limited, in order to regard all “.hk” domains as having a Hong Kong link.	Since the “.hk” domain names are currently assignable to applicants who do not necessarily have a Hong Kong presence, i.e. for individuals, they may not need to be Hong Kong residents, or for organisations, they may not need to carry out any business or activities in Hong Kong, the Hong Kong connection is not certain. In view of this, we consider that it is not appropriate to include “.hk” domain in the definition of Hong Kong link.
2.4.4	PCCW-HKT	Concerned about the extension of the scope of the Bill to include commercial electronic messages (without a Hong Kong connection) sent by overseas senders to overseas electronic addresses accessed by any telecommunications device in Hong Kong.	We consider this element to be necessary in order for the Bill to cover electronic addresses with no clear geographic identifier but used by, e.g., people physically in Hong Kong and using their PCs to access those electronic addresses such as e-mail accounts. The same approach is adopted in the Australian Spam Act 2003.

(5)	***Meaning of "Send"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.5.1	HKDMA ADMA	Concerned that, other than telecommunications service providers, the Bill does not differentiate between the "originators" of e-mail messages and service providers who hosted messaging delivery platforms to legitimate marketers. Suggest that only the "originator" of the message should be responsible for any breach of the proposed Bill, not other organisations that provide the infrastructure and technology to deliver such messages.	The respective liability of the principal and the agent is the same as in common law. In principle, the product/service supplier as the principal will be liable for acts done by the e-marketing company which acts as its agent. However, it shall be a defence for the product/service supplier to prove that it has taken practicable steps to prevent the agent from doing acts or engaging in practices which contravene the anti-spam legislation.
2.5.2	Yip Ming, Edward	Suggests adding a provision to the effect that a person who employs an intermediary for sending out electronic messages of commercial promotion of whatever expressed means should be held responsible for the act of the intermediary in respect of the sending out of electronic messages.	

(6)	***ISP's Responsibility***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.6.1	Paul Gardiner	The Bill should not provide immunity to ISPs as it is their duty to protect their subscribers from nuisance messages. Any ISP which hosts the sender of mass-marketing messages should also be required to prove that the sender has fully complied with the Bill.	The Bill only provides that when a telecommunications service provider is merely providing a service and exercise no control over the content or use of such service, it would not be treated as sending or causing the sending of the message. If the telecommunications service provider knowingly assist spammers in contravention of the UEM Bill, it may be liable for 'aiding, abetting, counselling or procuring' the contravention under section 89 Criminal Procedure Ordinance (Cap. 221).
2.6.2	WTT	Agreed that under Clause 4(4), for the purposes of any legal proceedings, a telecommunications services provider who merely provides a service that enables a commercial electronic message to be sent, shall unless the contrary is proved, be presumed not to have the message and not to have authorised the message to be sent.	
(7)	***Meaning of "Consent"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.7.1	HKDMA ADMA	Definition of consent implies an opt-in approach, a change from the initial discussions and may hinder the growth of SMEs in Hong Kong.	While the Do-Not-Call register enables a recipient to refuse receiving commercial electronic messages from all senders at that electronic address, consent enables the recipient to select to receive some commercial electronic messages from specific senders. Consents are not mandatory for the sending of commercial electronic messages, unless the recipient has unsubscribed from a sender or has added his electronic address in a Do-Not-Call register, and would not constitute a departure from the opt-out regime.

2.7.2	HKCS	The provision in clauses 5(3) and 5(4) that anyone can give or withdraw consent on behalf of the registered user seems to be an open invitation for abuse. There should not be blanket assumption that a subscribe or unsubscribe message is authorised by the registered user. Suggestions on how a sender of a message can determine who the registered user is, or who has been authorized by the registered user to send subscribe or unsubscribe SMS and e-mail messages were given.	Clause 5(3) provides that if a person other than the registered user of an electronic address uses the relevant account to consent or withdraw previous consent, that person shall be treated as doing it on behalf of the registered user. The clause is intended to facilitate compliance by senders of commercial electronic messages who receive unsubscribe requests from registered users of electronic addresses. It allows the senders to rely on the unsubscribe request as having been authorised by the registered user of an electronic address and thereby avoid the need to take further steps, at additional cost, to verify that the registered user has personally consented to the sending of the unsubscribe request. On receipt of an unsubscribe request, the sender can immediately act upon the request by removing the relevant electronic address from its sending list in compliance with Clause 9. This is in line with current business practices by organisations that provide unsubscribe facilities in their commercial e-mail messages. We therefore do not consider it appropriate to make changes to Clause 5(3). Clause 5(4) serves a different purpose and has been included for greater certainty. It is intended to make clear that consent may be given on behalf of a registered user by means other than those specified in Clause 5(3), i.e. by means other than by using the "relevant account". An example would include a letter sent by post.

(8)	***Meaning of "Registered User"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.8.1	HKCS	Clarification is needed on when the registered user is an individual or an organisation. In the case of a HK company allocating an e-mail address to a member of staff who takes a trip out of HK and then accesses their e-mail, if the organisation is considered to be the registered user, then there is a HK link, but if the individual is considered to be the registered user, then there is no HK link.	In the case of an organisation, the organisation is the registered user of the domain and all its email addresses, while individuals may deem to be acting on behalf of the registered user if he/she uses the relevant account to make the unsubscribe request or consent.
(9)	***Person-to-person Telemarketing Calls***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
2.9.1	Civic Party CC 張國衡、趙祥貴	Suggest that the Bill also regulate human to human, instant/real time communication.	We recognise that casting too wide a net for the regulatory regime could have an adverse impact on normal business activities. For instance, it is a generally accepted practice in HK for sales persons to make personal telephone calls to promote certain products or services to existing or potential clients. To leave room for such normal and legitimate marketing activities, we are of the view that we should be light-handed in regulating this mode of e-marketing and thus some exclusions are included in the UEM Bill. Nevertheless, we propose that the exclusions may be amended by the Secretary for Commerce, Industry and Technology (SCIT) through regulations. Thus, if there is a need to amend the exclusion list to cater for the latest development, such amendments could be introduced within a short period of time.
2.9.2	PCCW-HKT	Supports that normal commercial telemarketing activities not be covered by the legislation, and objecting the call for including "cold-calling" in the Bill.	
2.9.3	Yip Ming, Edward	Suggests repealing paragraph 2 of Schedule 1.	
2.9.4	HKDMA Doctor First Centre Ltd (verbal)	Person-to-person telemarketing calls should be excluded from the scope of the Bill.	
2.9.5	WTT	The Bill should not be applicable to person-to-person messages given that they are far less intrusive than machine generated messages.	

(III)	**Part 2 - Rules about sending commercial electronic messages**		
(1)	***Accurate sender information***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
3.1.1	HKDMA ADMA	Unnecessary to provide a defence to the sender that he did not know and could not have ascertained that a message has a Hong Kong link. Spammers may exploit this loophole.	Some senders may be outside Hong Kong and might not be able to ascertain with reasonable efforts that a message could have a "Hong Kong link". The proposed Bill strikes a balance and puts the onus on the sender to show that he has exercised reasonable diligence before he can claim the defence. Similar defence is also provided in the Australian Spam Act 2003.
3.1.2	HKCS	Clause 7(2)(b) which exempts a sender from the obligations in clause 7(1) to provide accurate sender information if the sender did not know that there was a Hong Kong link appears to be a dangerous and overly broad exemption, especially since there is no way a sender can determine where the recipient or telecommunications device used to access the message is located.	
3.1.3	TKODECG	The sender of commercial electronic messages must let the recipient know the identity of the sender.	The Bill will mandate a sender of UEM to provide accurate sender information and functional unsubscribe facilities, which are required in order for the recipients to learn who sent the messages and to exercise their right to refuse further commercial electronic messages from the sender.
3.1.4	PCCW-HKT	Clause 7(2) should be amended so that the requirements of provision of accurate sender information do not apply where the recipients have given consent.	

(2)	***Unsubscribe facility and unsubscribe requests***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
3.2.1	江燦良先生 Civic Party	Suggest that sender of commercial electronic messages to a mobile phone number must make an announcement at the beginning of the call to the effect that the called party can press the "*" key before and during the playing of the message to stop the message and the called number will be automatically stored in the unsubscribe list. . Civic Party suggests a short introduction should be given before the message begins, so that the recipients would know the nature of the call, and would be able to take appropriate actions in regard to the message.	While the UEM Bill aims to be as technology neutral as possible, we appreciate that some requirements on unsubscribe facility and unsubscribe requests will need to be imposed to ensure that they can be "functional" for the recipients of electronic messages. However, such requirements are technology dependent and new requirements may need to be added when new technology appears. It is our plan that detailed requirements will be prescribed in the regulations to be made by the SCIT.
3.2.2	The Hong Kong CAS/COM Joint Chapter of The Institute of Electrical and Electronics Engineers (HK CAS/COM Joint Chapter of IEEE) (verbal)	Suggests imposing a requirement in Clause 8(1) that the unsubscribe facility provided through "other electronic means" must allow users to unsubscribe with ease, e.g. the unsubscribe request can be sent within 10 minutes.	
3.2.3	HKDMA ADMA WTT	Support the conditions under which unsubscribe facility must be provided and unsubscribe requests must be honoured.	Noted.
3.2.4	TKODECG	Recipients should have the absolute right to refuse receiving commercial electronic messages. It is unreasonable to place the burden on the owner of an e-mail address.	The provisions of the Bill aim to allow the recipients to exercise their right to refuse further commercial electronic messages from the sender. The proposed do-not-call registers will make it more convenient for recipients to exercise such rights.

3.2.5	BSA HKASC ACCHK (verbal)	No other comparable jurisdictions in the Asia-Pacific region and the US have introduced a record retention requirement in their anti-spam legislation. The requirement will place a significant burden on regulated entitles and is unlikely to assist enforcement efforts since illicit spammers are expected to ignore the proposed requirement. The requirement of retaining messages of unsubscribe requests for at least 7 years should be removed. HKASC added that SMEs and also large enterprise will face significant compliance costs in storing and maintaining potentially thousands or millions of unsubscribe messages for a protracted period of time. The proposal will also add to the burden of legitimate foreign businesses seeking to communicate with Hong Kong residents.	The 7-year retention period is proposed on the basis that a victim of a UEM could initiate civil proceedings up to 6 years after a contravention has occurred, as provided for under the Limitation Ordinance (Cap. 347), and that the contravention could have occurred some time after the victim has sent the unsubscribe request. If it is considered that the proposed period will be too onerous to senders of commercial electronic messages, we are prepared to consider shortening this period.
3.2.6	PCCW-HKT CSL/NWM	Concerned that the required duration of 7 years for keeping unsubscribe requests is unnecessarily long. CSL/NWM suggests that the period the retention period should be shortened to 1 year.	

3.2.7	CC	It appears that an overseas spammer would not be held responsible for not responding to an unsubscribe request in view of the difficulties in extra-territorial enforcement. On the contrary, it may enable them to confirm the existence of the electronic address from which the request was sent.	All senders would be obliged to honour unsubscribe requests, subject to the message having a Hong Kong link, and could be subject to prosecution if they contravened clause 32(1) in respect of information obtained by unsubscribe requests. While it would be more difficult to identify and prosecute overseas spammers sending spam e-mails, the law enforcement agencies will continue to develop cooperation channels with their overseas counterparts.
3.2.8	CC	Suggests shortening the grace period of 10 working days to avoid the possibility of abuse.	A balance has to be struck between consumer protection and business efficacy. We consider that a period of 10 working days is reasonable. The same requirement is stipulated in the US CAN-SPAM Act.
3.2.9	CSL/NWM	Suggests that the unsubscribe request should be effective after a period of 20 working days, as the proposed period of 10 working days is too short that business may need to update a number of systems to give effect to the change.	
3.2.10	WTT	Clause 9 stipulates a period of 10 working days for the individual or organisation to process the unsubscribe request is a good start to combat spamming.	

3.2.11	Civic Party	If a person has placed an unsubscribe request under the Bill, will that automatically mean that that person has also placed an opt-out request under section 34 of the Personal Data (Privacy) Ordinance? If so, shouldn't there be consequential amendments to the latter? If not, this is simply creating unnecessary bureaucracy and unnecessary burden on the victim as he or she needs to send 2 different requests to 2 different regulators.	An unsubscribe request placed pursuant to the UEM Bill is placed with the sender of the UEM, NOT the regulatory body (i.e. OFTA). Likewise, under Section 34 of the PDPO, an unsubscribe request is placed with a data user who used the personal data (who, for the purposes of the UEM Bill, shall be the sender of the UEM) for direct marketing purposes. Accordingly, there is no question of a recipient being required to send unsubscribe requests to 2 different regulators. The UEM Bill and the PDPO focus on different aspects. The former concerns the act of sending messages, while the latter concerns the use of personal data for direct marketing. A recipient of a commercial electronic message could request the sender to unsubscribe him under both the Bill and the PDPO, if applicable, at the same time. We will publicise this point in guidelines for consumers.
3.2.12	PCCW-HKT	The Bill does not deal with the overlap between section 34 of the Personal Data (Privacy) Ordinance (direct marketing opt outs) and the requirements in clause 8.	
3.2.13	PCCW-HKT	Clause 8(2) should be amended so that the requirements of provision of unsubscribe facility do not apply where the recipients have given consent.	The unsubscribe facility prescribed in clause 8(1) is also applicable for recipients to withdraw consent. We do not consider it appropriate to exempt senders from complying with clause 8(1) requirement if prior consent has been given
3.2.14	PCCW-HKT	As subscribers often only want to opt out of specific product direct marketing or via a particular electronic address, flexibility for recipient to choose the type of commercial electronic messages or type of products should be provided in the Bill.	The Bill mandates senders to provide option to opt out from all subsequent marketing messages. Telemarketers are at their liberty to offer more options to opt out from specific products, to provide a choice to the recipient of the messages.

3.2.15	SWC	The unsubscribe facility should be provided in both Chinese and English language to avoid any doubts regarding the use of language of the unsubscribe facility.	We concur that unsubscribe statements and facilities must be comprehensible to recipients. However, because of the limitation of certain messaging channels (e.g. SMS messages can only accommodate 70 letters or characters if any Chinese character is included in the message), we intend to prescribe requirements specific to message types through regulations to be made under Clause 56. The language requirement, suitably adapted for different message types, would be reflected in those regulations.
(3)	***Calling line identification (CLI) information***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
3.3.1	江燦良先生 TKODECG DFC (verbal) BCS(HK) (verbal) WTT	Sender of commercial electronic messages to a phone number must include CLI information. Mr Kong suggests that unsolicited telemarketing calling without CLI information should be criminalised.	Clause 12 of the UEM Bill requires that commercial voice and fax calls must not be sent with CLI concealed. TA may issue Enforcement Notice if Clause 12 is contravened. Failing to comply with the Enforcement Notice is a criminal offence under Clause 36.

3.3.2	DFC (verbal)	Callers should register before they can use "133" command to choose not to disclose their CLI information to the recipient. Alternatively, they can be required to pay a much higher airtime charge.	The fundamental question of whether CLI should be provided, and the conditions under which CLI could be given and withheld, were the subject of the public consultation exercise conducted in 1995 and it was found that there are valid privacy concerns for a caller to want to remain anonymous[1]. However, the Administration notes that there is a demand from the general public that telemarketers making calls with pre-recorded commercial messages should provide their CLI so that the recipient has a choice not to pick up any suspicious call without a CLI. Accordingly, we have incorporated into the Bill a provision (clause 12) requiring senders of commercial electronic message from a telephone or fax number to provide valid caller line identification information.

- [1] Please refer to TA Statement "Calling Number Display – The Way Forward": http://www.ofta.gov.hk/en/tas/ftn/ta960705.html

3.3.3	江燦良先生 TKODECG CC 張國衡、趙祥貴	Suggest that telephone numbers with special prefix should be assigned to senders of commercial electronic messages to facilitate identification of callers by the called party.	We noted this suggestion and have discussed with the fixed and mobile network operators over the past few months. Some operators expressed the following concerns of the practicability: (i) It would be difficult for the operators to identify if their customers are telemarketers. (In fact, we would need a clear definition for "telemarketers".) (ii) It would be difficult to implement if telemarketing is only one of their customers' many functions/activities with their telephone systems. In practice, it may be difficult to decide whether the content of a particular telephone call would make a call a telemarketing call if person-to-person calls are to be covered. The difficulty was explained in our letter to Bills Committee on 4 October 2006. We will further consider this proposal.
3.3.4	Paul Gardiner	Suggests that all telephone or fax-based marketing company, whether in Hong Kong or offshore, must register their numbers with OFTA or with each Hong Kong telecommunication company directly and undertake to comply with the UEM Bill. No Hong Kong telecommunication company shall accept mass-marketing services over its network without a caller ID from the marketing organisations.	The telemarketers in Hong Kong will have to comply with the Bill once it becomes effective. Also, it would be impossible for telecommunication service providers to know when a call is commercial and when it is not, since they should not intercept the content of the call.

3.3.5	SWC	There may be a degree of uncertainty or inconsistency because clause 12 is a prohibition; but clause 23(3) is an exclusion but it seems that they cover the same situation. Furthermore, there does appear to be a genuine question how Clause 12 and Clause 23(3) will be reconciled when this question arises in a real life situation.	The two clauses deal with two different kinds of acts. Clause 12 concerns a prohibition on a caller to use a legitimate function of the telecommunications network to instruct (by dialling "133" before a telephone number, or establish a standing arrangement in a handset or with the network) that his calling line identification (CLI) information should not be displayed at the recipient's end. On the other hand, Clause 23 concerns material falsification of header information in electronic messages (e.g. by spammers tampering with the routing information contained in the header of an e-mail so that the spam filters would not block them). Clause 23(3) merely clarifies for the avoidance of doubt that the use of a legitimate function of a telecommunications network to instruct that CLI information should not be displayed at the recipient's end would not be considered as breaching Clause 23(1). The exclusion in clause 23(3) is intended to ensure that a contravention of the rule in clause 12 does not constitute an offence in and of itself. The rule in clause 12 and the offence in clause 23(1) serve different purposes. There should be no need for the court to reconcile the two provisions in the event that a person is prosecuted for an offence under clause 23(1) since each provision should stand on its own.
(4)	***Other views/concerns on rules about sending commercial electronic messages***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
3.4.1	Mail Prove Limited (verbal)	Every message should contain information identifying whether it is sent under the opt-out regime or with the consent of the recipient.	The suggestion may be a burden for some technologies like SMS where length of message is restricted. We will further consider if it should be recommended as a best practice to telemarketers for suitable electronic message types.

3.4.2	TKODECG	Message sending companies can consider using SMS to send commercial electronic messages and discuss with telecommunications operators to use 3G networks to send messages.	Many overseas countries have observed growing trend in SMS spams and some have already taken this into account when they enacted anti-spam laws. By adopting a technology neutral approach in the UEM Bill, SMS and future 3G technologies will also be covered. However, telemarketers are free to choose between different forms of electronic communications for e-marketing.
3.4.3	BSA HKASC ACCHK (verbal)	The UEM Bill should not increase the obligations on persons who send commercial electronic messages in furtherance of pre-existing business relationships. Suggest that the definition of commercial electronic message should exclude transactional or relationship messages. Alternatively, BSA and HKASC support a private arrangements exception to exempt a sender from the requirement to include a functional unsubscribe facility if this exception is qualified by a presumption that all transactional or relationship messages as defined in the US legislation would fall within it. They also support the enactment of a pre-existing business relationship exception to the clause 10 on prohibition of sending commercial electronic messages to persons whose electronic addresses are listed on a do-not-call register.	We consider that the obligations imposed in Part 2 of the Bill such as accurate sender information, provision of unsubscribe facilities etc., are mere good business practices that could well have been implemented by responsible e-marketers. Exclusion of recipients with pre-existing business relationships with the senders could introduce a loophole that may be exploited by unscrupulous e-marketers establishing “business relationships” with individuals primarily for the purpose of bypassing the obligations in the Bill. We do not consider the likely outcome of the proposal from the parties to be desirable from consumers’ point of view.

3.4.4	CSL/NWM	Suggest that the followings be excluded from the definition of commercial electronic messages:- (i) acceptable business communications; (ii) messages sent by a business to persons with whom they have an existing business relationship; (iii) service-related messages, whether or not they also contain additional promotional content; and (iv) messages which are not related to the promotion of a commercial product or service (e.g. invoice) or where the secondary or ancillary purpose of the message is to promote a commercial product or service (e.g. a message in an invoice about a new service).	We consider that the obligations imposed in Part 2 of the Bill such as accurate sender information, provision of unsubscribe facilities etc., are mere good business practices that could well have been implemented by responsible e-marketers. Exclusion of recipients with pre-existing business relationships with the senders could introduce a loophole that may be exploited by unscrupulous e-marketers establishing "business relationships" with individuals primarily for the purpose of bypassing the obligations in the Bill. We do not consider the likely outcome of the proposal from the parties to be desirable from consumers' point of view.
3.4.5	CC (verbal)	There is no need to give exemption to pre-existing business relationship.	
3.4.6	BCS(HK) (verbal)	Concerned about unauthorised dissemination of electronic addresses without the consent of the registered users	In the event that a person collects electronic addresses using address-harvesting software in breach of the relevant provisions of the UEM Bill, he would have committed an offence under Part 3 of the UEM Bill. If the collection of electronic addresses include personal data as well, the dissemination of those electronic addresses may have contravened the PDPO Data Protection Principle (DPP) 1 and the subsequent use of such data could well be in contravention of DPP 3

3.4.7	Civic Party	Suggests imposing strict liability on Part 2 offences.	Because contraventions to Part 2 may be committed inadvertently by legitimate e-marketers, we consider the proposed Enforcement Notice regime to be reasonable. For genuine spammers who ignore enforcement notices, they would be subject to criminal prosecution.
3.4.8	Paul Gardiner	The proposed fine levels are too low to act as a deterrent against habitual breakers of the law. Fines should be set based on the number of illegal messages sent, with a minimum of $5,000 per message.	Diverse views have been received during consultation on the proportionality of the proposed penalty. We consider that if the penalty is set too low, the deterrent effect may be weak. Some reference can be drawn to cold calls which amount to nuisance. This is dealt with under section 20 of the Summary Offences Ordinance (Cap. 228) with penalty of a fine of $1,000 and to imprisonment for 2 months. The proposed fine for contravention of the enforcement notice is at level 6 ($100,000) for the first offence, and at $500,000 for subsequent offences, and should achieve a strong deterrent effect.
3.4.9	WTT	Seriously concerned about the heavy penalties imposed by the Bill in relation to the various offences when compared to the penalty prescribed under the PDPO. In particular, clause 39(2) of the Bill prescribe penalties of a fine at level 5 and imprisonment up to 2 years, while section 14 and 15 of the PDPO impose a penalty of a fine at level 3 and imprisonment up to 6 months only.	
3.4.10	CSL/NWM	Suggests that clause 11 should include a prohibition on “deceptive” conduct as well as conduct that is likely to “mislead”, in keeping in line with the terminology used in the Telecommunications Ordinance.	Part 2 of the UEM Bill (which incorporates Clause 11) are intended to set out some basic rules about the sending of commercial electronic messages. We consider that “misleading” heading is of a relatively minor nature compared to “deception” which, if serious, may amount to fraud. Accordingly, our intention is to deal with “deceptive” conduct under Part 4 of the UEM Bill, in particular Clause 22 which deals with the transmission of multiple commercial electronic messages with the intent to deceive recipients as to the source of the message.
3.4.11	WTT	Agreed to Clause 11 of the Bill, which prohibits misleading subject headings in commercial e-mail messages.	

(IV)	**Part 3 – Rules about address harvesting and related activities**		
(1)	***Definition of "Address-harvesting software"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
4.1.1	HKCS	Domain Name Service (DNS) resolvers may fall within the definition of "address-harvesting software" and will prevent Hong Kong from using or participating in the Internet.	The offences related to address harvesting software (i.e. s.14(1), 15(1) and 16(1)) have some common elements, namely: i) a software specifically designed or marketed to search the Internet/telecom network and collect electronic address; and ii) the software or harvested-address list is for use in connection with, or facilitate the sending of UEM with a HK link without consent of the recipient. We consider that the software described in items 4.1.1, 4.1.2 and 4.1.3 is not considered as specifically designed to search the internet and collect electronic addresses. Also, it is only a breach of the section if the use of these software, or address-harvested list, is in connection with the sending of UEM without the consent of the recipient.
4.1.2	HKCS	If an IP address is included in the definition of "electronic address", then many servers on the Internet, including web servers and e-mail servers, that routinely collect IP addresses of the machines that contact them, or they contact, may be classified as "address-harvesting software" and fall under the control of Part 3 of the Bill.	
4.1.3	HKCS	Many Internet search engines can be used to search for anything, including electronic addresses. Even though clause 13(1) includes the phrase "specifically designed or marketed for" that seems to exclude search engines from "address-harvesting software", the definition can be undermined by using a different design objective.	

4.1.4	HKCS	E-mail system administrators routinely collect and process addresses by various automated means. Security testing often involves the gathering of data, including addresses, as a preparatory stage to the simulated attack. These activities may be caught in the rather vague definition of "address-harvesting software".	The offences related to address harvesting software (i.e. s.14(1), 15(1) and 16(1)) have some common elements, namely: i) a software specifically designed or marketed to search the Internet/telecom network and collect electronic address; and ii) the software or harvested-address list is for use in connection with, or facilitate the sending of UEM with a HK link without consent of the recipient. For items 4.1.4 and 4.1.5, the sender will not fall into the scope of the sections of the Bill because they have the consent of the recipient or registered user and/or the messages are not commercial in nature.
4.1.5	HKCS	A common way of processing subscriptions to mailing lists is web-based form for people to visit the form and subscribe to the mailing list. The software that processes the form input would be "address-harvesting software" as defined in the Bill.	
4.1.6	HKCS	"Internet" is not defined. There is uncertainty whether company computers that are connected to, and accessible from, the Internet are considered to be included in the Internet for the purpose of this Bill.	The ordinary meaning of Internet will apply and company networks are not normally considered as part of the Internet.
4.1.7	WTT	Agreed to the measures for prohibiting the supply, acquisition and use of address-harvesting software and harvested-address lists for sending commercial electronic messages without the consent of the registered users of the electronic addresses and the prescribed heavier fines and penalties (not subject to the enforcement regime) to effectively deter spammers from using harvested-address lists to conduct wide scale spamming.	Noted.

(2)	***Supply, acquisition and use of address harvesting software and harvested-address lists***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
4.2.1	Professional Information Security Association (PISA)	Prohibition of e-mail address harvesting may lead to buying/trading of e-mail or telephone numbers from the Internet. Those databases sometimes consist of e-mail addresses only and without any identifiable personal information and are not within the scope of the Personal Data (Privacy) Ordinance. The Government should consider the potential risk of people selling and buying e-mail address database within Hong Kong.	If the original source of those e-mail addresses or telephone numbers contains personal data as well, selling those e-mail address or telephone lists, even without the personal data in the lists, may have contravened the PDPO if the sale of those information is not one of the purposes of collecting those information.
4.2.2	CSL/NWM	Does not agree with the proposal to allow address-harvesting software and harvested lists in connection with sending a UEM as long as that software or list is used in compliance with the Bill.	Compliance with the UEM Bill (i.e. following the rules in Part 2 of the UEM Bill) does not exempt the sender from offences in Part 3. The offences in the two parts are separately enforceable.
4.2.3	HKCS	Because the prohibition under section 16(1) is limited to the sending of commercial electronic messages, a spammer could harvest addresses and send them subscription invitations without commercial content without committing a crime.	The application of the Bill aims to focus on the content of the message, i.e. whether any products or services etc. are offered. Whether or not subscription invitations would fall within the definition of commercial electronic messages would depend on the facts of individual cases.
4.2.4	HKCS	Once an address list is created, there is nothing to show how it was created. If a list is sold, there would be no reasonable means for a purchaser to test whether the list was originally created in an allowed manner.	The buyer of the list should exercise due diligence and inquire about the source of the list. If there is any doubt or if the seller could not give any assurance that this list is prepared in compliance with the Bill or any other laws, the buyer should exercise caution and should not acquire the list because of the risk of contravening the UEM Bill. We will provide guidance to businesses in this respect.

(3)	***Use of scripts or other automated means to register for 5 or more electronic mail addresses***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
4.3.1	HKCS	Clause 18(4)(b) appears to allow telecommunications service providers unlimited opportunity to send unsolicited commercial messages about their services.	The exemption only applies when the telecommunications service providers are acting in connection with the provision of telecommunications services, because automated creation of their customers' e-mail accounts could be an integral part of its functions. Furthermore, we consider it extremely unlikely that a telecommunications service provider trying to promote its telecommunications services to recipients would resort to automating the registration of e-mail accounts in order to hide the true origin of the messages and evade spam filters.
(4)	***Relay or retransmission of multiple commercial electronic messages***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
4.4.1	HKCS	The limited definition of "Hong Kong link" may make Hong Kong a safe transit haven for spammers elsewhere. The potential detrimental effect is that recipient organisations may be inclined to block all messages arriving from or via Hong Kong, and legitimate business communications may be disrupted as a result. Furthermore, if a spammer is using a relay to transmit messages to multiple addresses, he may argue that there was no intent to deceive the recipient, but only an intent to use bandwidth of the relay or to bypass the spam filters of the recipients.	Coverage extended to "transmitted via HK" may result in casting the net too wide. Current technology allows a network to use the most efficient route, without the knowledge of the sender. It is possible that a message could be in compliance with the laws of both the sending and receiving jurisdictions, but in violation of the Bill due to the "transmit through" element. It is not appropriate to criminalise open relays/proxies (sometimes may be a result of misconfiguration) and they can be prevented / dealt with by other measures such as regulatory measures.

(V)	**Part 4 – Fraud and Other Illicit Activities Related to Transmission of Commercial Electronic Messages**		
(1)	***Definition of "Multiple Commercial Electronic Messages"***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
5.1.1	HK CAS/COM Joint Chapter of IEEE (verbal)	The definition of the "multiple commercial electronic messages" should be tightened so that individuals will not be subjected to too many unsolicited electronic messages as defined in the Bill. It is proposed that individuals shall not receive the same message from same source frequently, say, more than once in every two weeks.	The concept of "multiple" is only applicable to offences in Part 4 of the Bill, which are related to the use of spamming techniques to conduct fraud and illicit facilities. The fraud and illicit activities may itself be another criminal offence (e.g. an offence under the Crimes Ordinance). Part 4 of the Ordinance is intended to deal with offences of a more serious nature and hence the elements of the offence are set to a higher standard to reflect the seriousness of these offences. Accordingly, while a single message will suffice for the offences in Part 2 and Part 3 of the Bill, we consider that it is reasonable to incorporate the concept of "multiple" in Part 4 offences before a sender shall be subject to Part 4 prosecution which, if successful, could result in very substantial fines and/or imprisonment terms. A similar approach is adopted in the US CAN-SPAM Act and the thresholds for the number of messages are also drawn from that law.
5.1.2	SWC	"Fraud / illicit activities" itself is "fraud / illicit activities". Commissioning of the fraudulent / illicit offence should not be subject to an artificial threshold of the number of commercial electronic messages being initiated however superficially convenient that may be to administer. The number of commercial electronic messages being initiated is only relevant to the seriousness of the offence and severity of the penalty imposed by the courts, instead of relating to the actual commission of the offence per se.	

(2)	***Initiating transmission of multiple commercial electronic messages with intent to deceive or mislead recipients as to the source of the messages***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
5.2.1	SWC	Suggested adding the mens rea of "recklessly" i.e. with gross or active negligence relating to actus reus element of "initiates the transmission of multiple commercial electronic messages that have a HK link from a telecommunications device, service or network without authorisation", which may assist the prosecution division to prove the limb of the said actus reus under the clause 22 offence.	The current mens rea requirement is "knowingly initiates ... with the intent to deceive or mislead recipients as to the source of such messages" and it is difficult to see how one could "recklessly" initiate something while at the same time having "the intent" to deceive or mislead recipients. The concepts are incompatible.
(3)	***False representations regarding registrant or successor in interst to registrant of electronic address or domain name***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
5.3.1	SWC	It is noted that there is no mens rea requirement in Clause 25(1)(a) relating to the actus reus element of "falsely represents himself to be the registrant or the legitimate successor in the interest to the registrant of 5 or more electronic addresses or 2 or more domain names".	The nature of the offence under clause 25(1) does not lend itself very readily to the addition of an express mens rea requirement in paragraph (a) of the clause. The absence of an express requirement however does not mean that the prosecution is relieved of the need to prove mens rea. There is a very strong presumption at common law that mens rea is required before a person can be found guilty of a criminal offence. The presumption can be displaced in the case of offences of strict liability but clause 25 is clearly not one of those offences. So, in the case of the offence under clause 25, mens rea must be proven.

(VI)	**Part 5 - Administration and enforcement**		
(1)	***Codes of Practice***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
6.1.1	HKCS	The meaning and intent of clause 28(5) is unclear.	Clause 28(4) stipulates that the TA may from time to time revise or approve Code of Practice and the procedures governing such revision or approval are stipulated in Clause 28(3), i.e. by notice in Gazette. Clause 28(5) simply makes it clear that any revision or approval of a Code of Practice is required to go through the same "gazetting" procedures.
6.1.2	WTT	TA may push through various codes of practices thereby increasing the burden of the telecommunications service providers. Telecommunications service providers should not be singled out given the uncertainty of the extent of the possible measures under the Bill and the consequences for failure to observe the TA's stipulations.	Under Clause 28, the TA may approve and issue codes of practice for the purpose of providing practical guidance in respect of the application or operation of any provision of the Ordinance. Such codes of practice are guidelines for different industries and for different technologies, such as a code of practice for fax marketing and how to use the Do-Not-Call register. So a wide spectrum of audience will be targeted.

(2)	***Do-not-call registers***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
6.2.1	HKDMA ADMA BSA HKASC CC Paul Gardiner ACCHK	Do not support the establishment of do-not-call registers for e-mail addresses.	The feasibility of a Do-Not-Email register was explained in a previous consultation paper and is still considered inappropriate to be established given their potential for abuse. The Federal Trade Commission of the US reached the same conclusion not to set up a Do-Not-Email register in its report to the US Congress in 2004. We will continue to monitor the situation and development in other jurisdictions.
6.2.2	HKCS	Clause 30(6) should allow a company to register its own domain names to a do-not-call register that would have the same effect of adding all e-mail addresses under this domain name to the register, thereby relieving the staff or system administrators from the burden of adding new addresses to the register when there is staff change.	
6.2.3	HKCS	Clause 31(1) might be unnecessarily broad and it is unclear whether this would allow the methods of hashing the register and look-up only access suggested by the HKCS to be used to prevent the misuse of the do-not-call register.	To enable a sender of electronic messages to comply with Clause 10, it is necessary for the sender to learn whether certain electronic addresses are on the registers. This clause prescribes sender's right to access such information. The TA will consider the appropriate mode of operation of the Do-not-call registers having regard to the arrangements for similar registers in other jurisdictions.

6.2.4	HKCS	Clause 30(6) would prevent the TA from inserting “canaries” or fake addresses from fake domains in the do-not-call registers for the purpose of revealing the misuse of information from the registers, since there is no registered user to give consent.	Canaries may work in two ways, namely: (i) poisoning of the Do-Not-Call register by planting fake addresses to lower the call success rate in case of an abuse to the Do-Not-Call register; or (ii) monitoring of the misuse of the DNC by planting working addresses so that messages can be received and checked. OFTA intends to use the second method for more proactive enforcement. Since OFTA would be the registered users of those working addresses, OFTA would comply with Clause 30(6) when undertaking this type of monitoring work.
6.2.5	CC WTT	Concerned that the difficulty of extra-territorial enforcement would encourage overseas spammers to harvest from the do-not-call register. WTT does not support the implementation of do-not-call register because it will increase the chances of spammers to abuse the information consolidated under the proposed register and suggests that it would be better to prevent the abuse from the start than relying on Clause 32 to prosecute spammers engaging in offences related to misuse of information prescribed by the do-not-call registers.	Initially, TA will only set up such registers for voice/video messages sent to telephone numbers, fax messages and SMS/MMS messages. Hence, the Do-Not-Call register will only contain the electronic addresses but not any personal data such as the names of the registered users. Since, on average, the chance of successfully dialling a valid telephone number in HK through random dialling is about 50%, the advantage gained by obtaining information from the Do-Not-Call registers is not significant. Several preventive measures will be deployed to protect the Do-Not-Call registers such as requiring telemarketers to register before gaining access to the data. We welcome any other suggestions for the protection of the Do-Not-Call registers.
6.2.6	CC	Suggest shortening the 10 working days grace period as it may be susceptible to be abused by spammers who may send many spams to newly listed addresses before the period expires.	A balance has to be made between consumer protection and business efficacy. We consider that a period of 10 working days reasonable.

6.2.7	Civic Party	Suggests that the do-not-call register should come into effect as soon as possible. Wishes the Government would provide further information to the public on this point.	As an integral part of the opt-out regime, the do-not-call registers will come into effect when Part 2 of the Bill comes into effect.
6.2.8	Paul Gardiner	Rather than "opt-out" via "do-not-call" registers, telephone/fax subscribers should "opt-in" to a public directory if they wish to receive marketing calls/faxes, otherwise, they are presumed not to wish to receive such calls. Option should be provided to registered users of telephone and fax services so that their numbers can remain secret and ex-directory.	Once entered into a do-not-call register, the electronic address will remain in the register indefinitely. Thus, the burden of registration will be very minimal and would strongly support the opt-out regime, which we consider to be more suitable to Hong Kong's situation. A sender of commercial electronic message must be able to learn about the electronic addresses in the registers in order not to send messages to them. It would defeat the very purpose of a do-not-call register if the sender could not find out that an electronic address to which he intends to send a commercial electronic message is in the register.
6.2.9	CSL/NWM	Cannot comment on clause 31 as details of the manner or mechanism via which the TA must set up a do-not-call register are not provided.	The Clause empowers the TA to make available information in the registers in forms and manners as he considers appropriate. He needs such general powers to develop an appropriate system of do-not-call registers having regard to the characteristics of the types of electronic addresses to be included in those registers, including the appropriate safeguards to minimise the possibility of improper access to the registers.
6.2.10	張國衡、趙祥貴	The proposed do-not-call register will be ineffective in the light of the large amount of mobile telephone numbers in Hong Kong.	Various registers similar to the Do-Not-Call register proposed have been implemented around the world and are considered an effective measure for countering telephone spams. For example, there are over 110 million numbers registered in the US Do-Not-Call register. The key is to impose an obligation to senders of electronic messages to remove those electronic addresses in the registers from their sending lists, as required Clause 10.

6.2.11	WTT	The establishment of do-not-call register would not only be costly to maintain and will increase undue financial burden to legitimate marketers.	Given the convenience to recipients, we consider a system of do-not-call registers to be worthwhile, even though it could mean some additional work for e-marketers. Such systems are also implemented in other jurisdictions.
(3)	***Powers of Arrest***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
6.3.1	PCCW-HKT WTT	The TA's powers to arrest should be curtailed and only be exercised with a warrant. The Bill should make it mandatory for OFTA to use the police to exercise these powers. WTT submitted that instead of the TA, the HK Police Force should be prescribed with the investigative powers under clause 37 and 38 (power of entry, search, arrest).	Currently, TA is similarly empowered to make arrests without a warrant under the TO, and so far no complaints on abuse have been received. We consider that such power is necessary to enable the TA to exercise his statutory powers proposed in the Bill. Clause 37(4) also requires the TA to take any person arrested to a police station without delay. Given the division of responsibility between the TA and the Police under the Bill, we consider it inappropriate for the Police to take up all the responsibilities in Clauses 37 and 38.
(4)	***Misuse of information***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
6.4.1	HKCS	The narrow definition in clause 30(2)(b) means that clause 32(2) would not permit the registered user of an address to check the do-not-call register to verify whether or not their address is registered. It may prevent a harmless and possibly useful reason for checking the register – e.g. technical staff investigating why a message was not received.	Clause 32(2) is applicable only to information made available under Clause 31 to senders of commercial electronic messages and is not relevant to a registered user of an electronic address, or anyone on his behalf, verifying the registration of his electronic address.
6.4.2	HKCS	Clause 32(1) would prevent a recipient of an unsubscribe message to investigate whether the unsubscribe message was sent from a registered user or with his consent.	Verification or investigation of whether an unsubscribe request was sent by the registered user or someone on his behalf is to enable the sender of commercial electronic messages to comply with Clauses 8 and 9 of the Bill. Clause 32(1) would not prevent such activities from taking place.

(5)	***TA's power to obtain information or documents relevant to investigation***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
6.5.1	HKCS	Users should not be required under clause 34(1) to reveal their passwords.	Clause 34(1) is required to facilitate investigation and is subject to Clause 34(8) so that a person will not be required to provide self-incriminating evidence.
6.5.2	HKCS	A person may avoid his responsibility to provide information under clause 34(1) by simply scheduling frequent automatic deletion of the information.	It will be an offence under clause 34(9) if a person without reasonable excuse fails to comply with 34(4) as pursuant to the notice given under 34(1).
6.5.3	CSL/NWM	It should be clarified that in the event that the TA seeks an order pursuant to clause 34(3), the person named in the notice must have an opportunity to be present at the proceedings.	Clause 34 is modelled on the existing Section 36D of the TO. Under Clause 34(1), if the TA has reasonable grounds for believing that a person is, or is likely to be in possession of information relevant to an investigation under the UEM Bill, he may issue a notice (Notice A) requiring a person to furnish information. Under Clause 34(1)(b), the person will be given an opportunity to make representations. The next stage is Clause 34(2) - the TA has to consider the representations and then serve another notice (Notice B) stating that he has considered the representations and either (1) he withdraws Notice A, or (2) he states that Notice A remains in force and tells the person that the TA will, on a specified date stated in Notice B, seek an order from the Court under Clause 34(3) to compel the person to comply with Notice A. This being the case, in the case that the TA has to invoke Clause 34(3) to seek an order from the Magistrates to compel the person to comply with Notice A (to furnish information), the person is in fact fully "on notice" about the TA's proposed application to the Court. In any event, Clause 34(3)(a) clearly states that the Court will only

			make an order if: (1) the Court is satisfied with the information "on oath" by the TA (Clause 34(3)(a)); and (2) after considering the representations made by the person (Clause 34(3)(b)). A further protection is since the person would have been notified of the TA's proposed application to the Court for an order (the date of the application will have to be stated in Notice B), it is up to the person to appear before the Court hearing to make further representations to the Court. And of course, the Court always has the residual discretionary power to invite the person to come in to make representations.
6.5.4	WTT	Instead of the TA, the HK Police Force should be prescribed with the investigative powers under clause 34 to obtain information.	The Police has the necessary investigative powers under the Police Force Ordinance (Cap. 232). Because of the division of responsibility for enforcing the Bill, the TA needs the investigative powers under Clause 34 to carry out his duties.
(6)	***Other views/concerns on administration and enforcement***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
6.6.1	TKODECG	Deposits should be paid when obtaining business registrations. Such deposits should be forfeited if the company is found to have breached the rules under the Bill.	Empowering victims to seek compensation for loss or damage, or the Court to impose fines, could provide similar deterrent effect on offenders without creating a burden on the majority of businesses which are law-abiding.
6.6.2	PCCW-HKT	An adequate mechanism is needed to allow operators (or others) to recover their costs of assisting the Government in its investigations.	Costs incurred by operators (or others) in assisting the investigations can be considered losses or damages suffered as a result of a contravention of the Bill. The operators or others may seek compensation under Clause 52 from the party who contravened the Bill.

6.6.3	WTT	Clause 33 stipulates the power of the TA to issue directions to telecommunications service providers requiring them to take such actions to facilitate the telecommunications service provider's compliance of the legislation or to enable the TA or an authorised officer to perform any function under the proposed legislation. It is submitted that telecommunications service providers should not be singled out given the uncertainty of the extent of the possible measures under the Bill and the consequences for failure to observe the TA's stipulations.	The regulatory burden in the Bill falls mostly on the senders of UEMs. Nevertheless, telecommunications service providers and Internet service providers are particularly well placed to assist the TA in the investigations because UEMs are sent through their networks or facilities. Since a reduction of UEMs would benefit telecommunications service providers and Internet service providers as well, we consider it not unreasonable to require them to render assistance to the TA.
6.6.4	HKCS	The Legislative Council Brief does not specify who would enforce the address harvesting and related rules. Also, OFTA and the Police will need to cooperate closely to enforce the Bill. It is not clear how this will be achieved.	It is not uncommon that a piece of legislation does not specify the enforcement agency. In the context of the UEM Bill, our intention is that the Police will be responsible for enforcing Part 4 of the Bill while OFTA will be responsible for enforcing the rest of the Bill. In practice, OFTA and the Police will work closely together in these cases especially if fraud or deception elements are suspected to be involved.
6.6.5	WTT	For fraud and related activities in connection with spamming, WTT supports that the Hong Kong Police Force should be responsible for enforcing these fraud and related offences.	

6.6.6	WTT	Instead of the TA, the HK Police Force or alternatively the Privacy Commissioner should be the designated Authority to administer and enforce the provisions under the Bill because: 1) the telecommunications service providers would effectively be funding the various activities to be undertaken by the TA to administer and enforce the provisions under the Bill; and 2) in view of the Government's proposal to merge the BA and the TA, the future of TA is uncertain.	OFTA is the appropriate party because of its expertise in telecommunications systems through which commercial electronic messages are sent. A reduction in spam will not only benefit recipients, but also the telecommunications service providers since the amount of illicit traffic carried by their networks will be reduced. The proposed merger of the TA and the BA is in response to convergence of telecommunications and broadcasting services and would not affect the future discharge of responsibilities under the Bill by the Communications Authority (CA), if such responsibilities are transferred from the TA to the CA.
6.6.7	WTT	Recouping of the costs of investigation from a party convicted by the court of an offence under Clause 40 of the Bill should follow the existing criminal procedures as stipulated by the courts.	As stipulated under Clause 40, ultimately it is the Court which has the discretion to grant an order that the person convicted is to pay to the TA the whole or a part of the costs and expenses of that investigation. Whether the Court would like to follow existing criminal procedures in making such an order is a matter of discretion by the Court.

(VII)	**Part 6 – UEM (Enforcement Notices) Appeal Board**		
(1)	***Appeals to Appeal Board***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
7.1.1	BSA HKASC ACCHK (verbal)	Oppose clause 44(3) because a person could contravene an enforcement notice while awaiting the outcome of an appeal as to the correctness of the issuing the enforcement notice in the first place. Recommends that clause 44 be amended to provide that the relevant authority can only commence criminal proceedings alleging failure to comply with an enforcement notice upon the expiry of the 14-day period allowed for lodging a notice of appeal, or the completion of a merits-based review establishing the correctness of the TA's decision.	If the Appeal Board orders that an Enforcement Notice should be suspended, there would be no question of non-compliance with the Notice itself or any part therein (which is the criminal offence). If the Appeal Board does not order that an Enforcement Notice should be suspended, the sender of commercial electronic message should comply with the Notice in the meantime while lodging an appeal. Again, there should be no question of non-compliance with the Notice. Clause 35(3) provides that, subject to special circumstances under Clause 35(4), the period specified in an enforcement notice for taking the steps specified shall not expire before the end of the 14-day period (which is the period specified for lodging an appeal). Thus, in practice, it is not possible (save under special circumstances specified in Clause 35(4)) for the TA to commence criminal proceedings against a sender of unsolicited electronic messages for non-compliance with an Enforcement Notice before the 14-day appeal period expires.
7.1.2	PCCW-HKT	Clause 46(1)(i) provides for the Appeal Board the discretion to suspend the operation of an Enforcement Notice. However, there are no procedural provisions to make it practical for the Appeal Board to be in a position to suspend the Enforcement Notice prior to when compliance is required. Procedures are required to provide certainty for operators as to how these clauses will work.	If a recipient of an enforcement notice applies to the Appeal Board to suspend an Enforcement Notice, it is the responsibility of the Appeal Board to consider such applications before the end of the period specified in the Enforcement Notice.

7.1.3	WTT	Supported the establishment of the UEM Appeal Board and agreed that for the purposes of an appeal under Clauses 46 and 50, all the parties concerned shall have the same privileges in respect of the disclosure of any material as if the proceedings before the Appeal Board were proceedings before a court and the witnesses before the Appeal Board shall be entitled to the same privileges and immunities as if he were a witness in civil proceedings in the Court of First Instance.	Noted.

(VIII)	**Part 7 – Miscellaneous provisions**		
(1)	***Claims for loss or damage***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
8.1.1	BSA HKASC ACCHK (verbal)	Concerned about the breadth of the private right of action. Affording standing to individual spam recipients may encourage unproductive litigation. In many cases, the losses suffered by individual spam recipients do not justify the cost of court proceedings. Suggest limiting the proposed right of action to ISPs, email service providers and other intermediaries that have a clear interest and are capable of representing the interests of spam recipients in the legitimacy of online marketing channel. Alternatively, only those who have suffered losses above a prescribed monetary threshold should be given the private right of action.	The proposed civil claim is based on tort principle. We consider that the just and equitable remedies, which may include injunctive remedies, should be available to any victimised party. We do not consider it appropriate to arbitrarily limit such right on the basis of the status of the victimised party or the quantum of losses suffered.
8.1.2	Civic Party	It is difficult for the victim to show the quantum of the claim. Moreover, it may not be economical for the victim to bring the claim if his loss or damage is insignificant. It might also bring along a flood of cases for which Small Claims Tribunal would have to tackle. Suggests that there should perhaps be fixed amounts recoverable under this head.	

8.1.3	HKCS	Since loss or damage caused by one UEM is quite small, it is suggested that there should be provision for the aggregation of claims across multiple messages from one sender to one address, to multiple addresses of one registered user, to multiple addresses of one organisation, and to any group of addresses.	The proposed civil claim is based on tort principle. We consider that the just and equitable remedies, which may include injunctive remedies, should be available to any victimised party. We do not consider it appropriate to arbitrarily limit such right on the basis of the status of the victimised party or the quantum of losses suffered.
8.1.4	CC (verbal)	There is no need to limit the rights for compensation to ISPs and operators only.	
(2)	***Directors' Liability***		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
8.2.1	CSL/NWM WTT	WTT expressed concerns as to the statutory presumption under Clause 53, in particular that the employer or principal is required to bear a heavy burden to rebut the presumption. WTT believes the presumption of innocence should prevail and the burden of proof should remain on the prosecution to prove beyond reasonable doubt that the employer or principal has engaged in blameworthy conduct. WTT submitted that the Basic Law and the Bill of Rights protect the presumption of innocence and the derogation of the presumption would only be justified if it is justified by the rationality test and the proportionality test. As a result, WTT does not support the derogation of such principle, as the crime in question is not so serious as to warrant such derogation. CSL submitted that liability under civil actions	Clauses 53 and 54 are intended to make clear the responsibilities of employers and principals in relation to the acts of their employees or agents and the responsibilities of managing directors and partners in relation to the acts of their companies or partnerships. Various provisions of clauses 53 and 54 may become relevant in the event a civil action is initiated under clause 52 or a criminal proceeding is initiated in relation to an offence under the Bill. Insofar as civil actions under clause 52 are concerned, the only applicable provisions are clauses 53(1) and (2) which deal with the acts of employees and agents. Clause 53(1) creates a presumption that an act done by an employee in the course of his employment has been done by the employer. It is similar to the presumption in section 65(1) of the Personal Data (Privacy) Ordinance. It is important to note that the presumption is dependent on whether the employee is acting "in the course of his employment", which is a matter that will need to be proven by the plaintiff in accordance with the normal standard and burden of proof applicable in civil proceedings. If this matter is not proven accordingly, then the presumption will not apply.

		should follow the common law standard, i.e. the liability attaches to an individual or corporation (or other entity such as partnership) where it can be reasonably shown that they are the party responsible. The presumption in clause 54 should be reversed so that a director is not to be held liable unless he or she has acted in a manner that suggests otherwise.	Clause 53(2) operates in a similar manner but applies in the case of principals and agents. It is similar to the presumption in section 65(2) of the Personal Data (Privacy) Ordinance. It reflects in broad terms the common law applicable in civil proceedings. We do not consider these presumptions to impose an unreasonable burden on employers or principals. Clauses 53(3) to (5) provide defences to principals, employers and employees who are charged with an offence under the Bill. They do not apply in relation to civil actions under clause 52. Clause 54 applies only to criminal proceedings under the Bill. It does not relieve the prosecution of proving an offence beyond reasonable doubt in accordance with normal common law principles. Clause 54(3) makes it clear that a managing director, managing partner or other manager who is charged with an offence under the Bill bears only an "evidential" burden to displace the presumptions created by clauses 54(1) and 54(2). The person charged is not required to disprove a critical element of the offence. We do not consider these presumptions to be unreasonable or to be inconsistent with the Basic Law.
(IX)	**Other views not directly related to the Bill**		
	Organisations / Individuals	**Views / Concerns**	**Administration's Response**
9.1	PISA	The Government should take the lead in implementing Sender Policy Framework or Domain Keys in major government mail gateways, in order to speed up the acquiring of knowledge and standard.	We have referred to view to the Office of the Government Chief Information Officer for consideration.

9.2	PISA	After the UEM Bill is enacted, the Government should start to review the adequacy of current education and legal framework on spyware and phishing attacks.	We have referred the view to the relevant bureau and departments for their consideration.
9.3	BCS(HK) (verbal)	The Government should do more to control spam emails from overseas, e.g. ISP to block.	The government has adopted a multi-pronged approach to tackle spam which is not limited to legislative measures but also technical solutions, partnership and other measures.
9.4	HKCS	The process of reporting UEMs should be efficient and streamlined. Recipients should not be required to correctly identify which department to contact before making a report. UEM reports filed by recipients should preserve the necessary forensic evidence. Correlating separate reports into one case will allow efficient use of investigative resources and maximize the chance of successful prosecution. Where appropriate, the recipients should be provided with information necessary for a civil claims case or a notification that the report was used as evidence in a prosecution.	Noted and we will consider this suggestion in the design of reporting systems. It has always been envisaged that automation would be needed in handling complaints or reporting due to the potential volume and sizes of complaints.
9.5	周文	A complaint on receiving unsolicited fax commercial messages.	The complaint was handled by OFTA on 29.9.2006.
9.6	Edward Brook	Suggests dealing with physical “junk mail” by amending the Post Office Ordinance or expanding the coverage of the Bill	By nature, physical junk mails are not “electronic” messages per se. We do not consider it appropriate that the sending of physical “junk mail” be covered by the UEM Bill.

- End -