Bills Committee on Unsolicited Electronic Messages Bill

Administration's Response to the Outstanding Issues Raised at the Bills Committee Meetings

Meeting on 31 October 2006

Definition of "commercial electronic message" (clause 2)

Stevenson, Wong & Co. proposed to expand the definition of "commercial electronic message" to cover "to obtain, to assist to obtain, to attempt to obtain any gain, benefit or advantage in the course of or in the furtherance of any business". The submission cited an example that a spammer sending an e-mail advising the recipient that he has won a lucky draw and asked the recipient to call a telephone number for redemption of the prize, during which the spammer would attempt to sell a product or service.

2. After consideration, we do not propose to expand the definition of "commercial electronic message" as suggested by Stevenson, Wong & Co. First, the proposed expansion of the definition would cast the net too wide and may catch some messages unintentionally. Second, for the example cited by Stevenson, Wong & Co., we consider that, considering the concerned e-mail in context, the spammer's intention in sending that e-mail amounts to "promoting a business", even though the message was silent on that point. Our legal opinion is that the current draft of the definition of "commercial electronic message" should be sufficiently broad to cover such situation.

Meeting on 14 November 2006

Web traffic and other modes of information provision in response to a request

3. To make clear that web-browsing and information sent in response to a request (e.g. faxback service) would not be classified as unsolicited electronic messages as defined in the Bill, we propose to amend

Schedule 1 and to add a new Table 2 exempting any commercial electronic message sent to a person in response to information communicated by or the conduct of that person (e.g. entering a website address in a web browser or clicking on a hyperlink on a web page or an e-mail) from the application of Part 2 of the Bill To prevent potential abuse of this exemption, we propose that the commercial electronic message being exempted should be sent to the person within a reasonable period of time after the request has been made. Otherwise, a sender may claim exemption through this item for supplementary information sent in response to a request made by the recipient many years ago. Consequential amendments to clauses 5 and 6 are also proposed.

Meeting on 21 November 2006

Meaning of "send" (clause 4)

4. A Member raised the question whether an attempt to send unsolicited commercial electronic messages, which were not sent in the end but the content of which was not in compliance with certain requirements stipulated in the Bill, would constitute a contravention under the Bill. We wish to clarify that the purpose of this clause, insofar as "attempt" is concerned, is to make clear that commercial electronic messages will be treated as "sent" regardless of whether it is successfully received by the recipient (e.g. there could be technical problems in the transmission process).

5. According to section 159G(1) of the Crimes Ordinance (Cap. 200), an attempt to commit a triable offence must go beyond a preparatory step. Our interpretation for offences prescribed in Parts 3 and 4 of the Bill (which are triable) is that a spammer who has, for example, programmed the sending of a message at some future juncture from a computer should be considered as having gone beyond preparatory steps and hence has attempted to send the message. However, if a person has merely asked an agent to send a message on his behalf but the message is not sent by the agent in the end, we consider that the person would not be considered as contravening the provisions under Parts 3 and 4 of the Bill.

6. Section 159G(1) of the Crimes Ordinance does not apply to the rules prescribed in Part 2 of the Bill as non-compliance with those rules are not triable offence *per se*. Nevertheless, in its ordinary meaning, "attempt" means "make an effort to achieve or complete". For this Part of the Bill, we are thus of the view that if a person has not made an effort to send the message, it should not constitute an "attempt" to send. From a practical law enforcement point of view, if the message is not sent in the end, the Telecommunications Authority (TA) would not be able to obtain information or evidence to reasonably justify the issue of an enforcement notice under clause 35 of the Bill, which specifically requires him to form an opinion that a person "is contravening" or "has contravened" any provision of Part 2 of the Bill.

Unsubscribe Facility (clause 8)

7. As mentioned at the Bills Committee meeting, we propose to add clauses 8(1)(ba) and (bb) to provide that the unsubscribe statement and unsubscribe facility must comply with the requirements specified in the regulations to be made by the the Secretary for Commerce, Industry and Technology (SCIT).

Concept of "recklessly" (clauses 14 to 18)

8. We have no objection to the suggestion of a Member to remove the concept of "recklessly" from the offences in Parts 3 and 4 of the Bill.

Relay or retransmission of multiple commercial electronic messages (clause 19)

9. A Member questioned the need for setting thresholds of number of messages sent in order to consider the sender as having committed an offence. We wish to clarify that the definition of "multiple commercial electronic messages" adopted in the Bill is modelled from the US CAN-SPAM Act. Upon our enquiry, the US Federal Trade Commission and the US Department of Justice advised that for the US CAN-SPAM Act, the thresholds set therein could limit the actions that could be taken by the States or Internet Service Providers. The objective is

to protect businesses from being inundated with legal actions on the basis of a mere handful of technical violations. The US Department of Justice further advised that, in practice, the thresholds in the US CAN-SPAM Act are well below the standard e-mail practices adopted by spammers and have not hampered their enforcement objective of targeting professional spamming activities. We understand that Singapore's Spam Control Bill has adopted the same thresholds for "multiple commercial electronic messages" as in the US CAN-SPAM Act.

10. In addition, the thresholds for "multiple commercial electronic messages" are only applicable to certain offences in Parts 3 and 4 of the Bill. Those are illicit activities generally associated with professional spammers. We consider it desirable to adopt similar thresholds to harmonise with those jurisdictions on similar offences, thereby facilitating information and intelligence exchange as well as law enforcement. In any case, the rules in Part 2 of the Bill that set out the opt-out regime, with which businesses need to comply when sending commercial electronic messages, are not subject to the thresholds for "multiple commercial electronic messages". The structure of the Bill is such that every single commercial electronic message sent by telemarkters needs to comply with the requirements under the opt-out regime in Part 2 of the Bill, while offences in Parts 3 and 4 are geared towards tackling professional spammers.

Meeting on 28 November 2006

Enforcement

11. As set out in our previous response to the Bills Committee dated 21 November 2006, the enforcement agencies in Australia and US have adopted a targeted and progressive approach to handle complaints from the public to make the best use of their resources and to maximize the effectiveness of the law. Drawing reference to overseas experience, OFTA intends to formulate similar enforcement strategies.

12. Under the Australian model, the regulator accepts "reporting" and "complaints" from the public ("reporting" means passing UEMs to the regulator as intelligence in a one-way communications and

possibly with insufficient details/evidence whereas "complaint" means the complainant is willing to make a formal statement, supply primary evidence and to testify in the court of law). To obtain primary evidence and press charges against the offender, OFTA would need to seek formal statements from complainants, collect evidence from the relevant computers and secure their willingness to testify in court if necessary. Due to the higher commitment required of complainants, it would be useful to accept "reports" from those members of the public who do not wish to be directly involved in the investigation. Reporting, in this case, helps to indicate the scale of a particular email "campaign" and hence allows OFTA to effectively channel its resources in prioritising investigations.

13. OFTA has set up an anti-spam team which comprises four staff headed by a Division head. It is estimated that after the enactment of the Bill, more manpower resources will be required. The additional staff would likely be in the region of three to five to handle reports and complaints and carry out simple investigation.

14. At present, OFTA has set up the Telecommunications Users and Consumers Advisory Committee, members of which include representatives from the commercial sector, the industry, the general public and the Consumer Council, to listen to their opinion on various issues. It is considered that the Committee is an appropriate platform to gauge the industry and public opinion on issues in relation to unsolicited electronic messages, including the enforcement of the Bill.

<u>Initiating transmission of multiple commercial electronic messages from telecommunications device, etc., accessed without authorisation (clause 21)</u>

15. A Member enquired about the circumstances to which clause 21 of the Bill would be applicable but section 161 of the Crimes Ordinance would not. We wish to explain that clause 21 makes it an offence for any person to initiate the transmission of multiple commercial electronic messages that have a Hong Kong link from a telecommunications device, service or network that the person has accessed without authorization. The major difference between clause 21 of the Bill and section 161 of the Crimes Ordinance lies with the fact that the latter requires proof of a

"dishonest" intent, whereas clause 21 of the Bill does not. In other words, a spammer who has an "honest" intent to make a gain by sending multiple commercial electronic messages will be caught by clause 21 of the Bill but not section 161 of the Crimes Ordinance. In addition, section 161 of the Crimes Ordinance applies if a person who accesses a computer with an intent to commit a crime. Clause 21 of the Bill will be the underlying provision which creates the "crime". If clause 21 does not make such an activity an offence, section 161 of the Crimes Ordinance will not be applicable as the spammer would not have committed any crime.

16. On the experience in the US in the application of the statutory provision comparable to clause 21, we believe that the provision comparable to clause 21 of the UEM is in the CAN-SPAM Act section 4 (otherwise known as title 18, USC, 1037 (a) (1): Accessing a Protected Computer without Authorization to Send Multiple Commercial Email Messages). In the report dated December 2005 by the US Federal Trade Commission entitled "Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress", it described that there had been three successful prosecutions in 2004 and 2005 under this provision.

<u>False representation</u>

17. On the potential offences that a person who used the e-mail address of the President of the Legislative Council had committed, we have consulted the Security Bureau. While not commenting on individual cases, it was pointed out that in general, subject to the facts and evidence of an individual case, if a person knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer (i.e. hacking), he may have committed an offence under section 27A of the Telecommunications Ordinance (Cap. 106) and could be liable on conviction to a fine of $20,000. If a person obtains access to a computer with the intent to commit an offence or with a dishonest intent to deceive, or for dishonest gain or causing loss to another, he may have committed an offence under s.161 of the Crimes Ordinance and could be liable on conviction upon indictment to imprisonment for 5 years.

Meeting on 5 December 2006

Enforcement

18. We remain of the view that since the Police has general powers over all criminal offences under the Police Force Ordinance (Cap. 232), it would not be necessary to specifically spell out in the Bill that the Police would be responsible for enforcing Part 4 of the Bill. Nevertheless, we will highlight the division of enforcement responsibility between the TA and the Police in the speech by SCIT for the resumption of the second reading debate.

Authorized officers (clause 27)

19. Clause 27 is an enabling provision to cater for the administrative arrangement that the TA may appoint authorized officers to perform functions as specified in the authorization. Such authorization is confined to those functions that are conferred or imposed on authorized officers under other provisions of the Bill, such as the power to certify extracts from the "do-not-call" register, to arrest offenders and to search premises under the authority of a warrant. Since only Part 5 of the Bill contains provisions conferring or imposing functions on authorized officers, we agree to Members' suggestion to amend this clause to clarify that officers authorized by the TA would perform functions conferred or imposed on them under "Part 5 of the Ordinance", instead of "this Ordinance".

Codes of practice (clause 28)

20. We propose to amend clause 28(10) to clarify that a notice published in the Gazette for notification of approval of / revision of / withdrawal of approval from a code of practice under clause 28(3) or 28(7) is not subsidiary legislation.

21. As explained at a previous Bills Committee meeting, we consider it inappropriate to provide for statutory consultation on code of practice in the Bill. However, it is our intention to consult the ITB Panel, as well as the industry and the public, on the preparation of codes of

practice and on their subsequent major amendments. We will highlight our policy intention in the speech by SCIT for the resumption of second reading debate.

Do-not-call registers (clause 30)

22. Since the necessary telecommunications and computer systems for running the do-not-call registers have not yet been developed, it would not be possible to give an accurate estimate of the charging level for telemarketers to access the do-not-call register. OFTA's intention is to adhere to the cost-recovery principle as applicable to trading funds as far as possible. Drawing reference to overseas experience, OFTA is considering a simple charging scheme based on an annual fee for registered telemarketers. OFTA estimates that the charge should be in the region of a few thousands dollars for one year's unlimited access to the do-not-call registers. To cater for other telemarketers who may run their marketing campaigns on an *ad hoc* basis, OFTA will propose other arrangements, such as one-month access with lower fees, to cater for their needs. Given the relatively low level of fees involved and that the cost-recovery principle would be adhered to as far as possible, we do not consider it necessary to regulate the level of fee/charges under the Bill. This is similar to section 32E(f) of Telecommunications Ordinance on the cost recovery of testing work done by OFTA.

23. The charging schemes of US and UK for access to do-not-call registers are set out at **Annex A**.

24. We also propose to add new clauses 30A to explicitly prescribe the powers of the TA in relation to do-not-call registers. In addition, two new sub-clauses 31(3) and 31(4) are proposed respectively to empower the TA to impose a charge for accessing a do-not-call register, and to specify the right of a registered user of an electronic address to verify, free of charge, whether his electronic address is on a do-not-call register.

25. We agree with the suggestion made by a Member that the do-not-call registers should be kept up-to-date by periodic cleansing. We therefore propose to add a new enabling provision in clause 33(1A) to

empower the TA to issue directions to telecommunications service providers, who are allocated telephone numbers by OFTA, to, inter alia, provide information on surrendered telephone numbers so that OFTA can remove these numbers from the do-not-call registers.

Chinese term of "do-not-call register"

26. We agree to the proposal to replace "拒收登記冊" with "拒收訊息登記冊".

Meeting on 12 December 2006

Authority may issue directions to telecommunications service providers (clause 33)

27. We propose to add a new clause 36A to provide for financial penalty for telecommunications service providers who do not comply with directions issued by the TA under this clause. The proposed penalty level is modeled on those prescribed in section 36C of the Telecommunications Ordinance (i.e. up to $200,000 for the first occasion, up to $500,000 for the second occasion, and $1 million for any subsequent occasion).

Authority may obtain information or documents relevant to investigation (clause 34)

28. The Magistrates Ordinances (Cap. 227) and the rules made under that Ordinance do not contain any provision in relation to the procedures involved in the proceedings. However, in practice, the TA needs to submit an application to the Magistrates Court to commence the proceedings. According to clause 34(3), such an application so made by the TA has to be supported by information on oath. The Magistrate, on receiving that application and the supporting affidavit evidence from the TA, will then consider all relevant information and evidence, including any representations received by the TA under clause 34(2), before issuing an order. In any event, the magistrate always has the discretion to call on the affected person to hear his representations, if he considers necessary, before making an order. Nevertheless, we have no objection to Members'

suggestion to make clear in the Bill, by adding clause 34(3A), that the affected person has the right to be heard and make representations.

Power of entry, search, arrest, etc. (clause 37)

29. On whether the wording of clauses 37(1) and 37(2) should provide that while no warrant would be required for TA or an authorized officer to arrest at public places any person whom TA reasonably suspected of having committed a specified offence, a warrant would be required if the arrest was to take place inside any private place or premises, we consider that it is not the normal practice to qualify the power of arrest in such a manner as it could lead to unnecessary legal complications. We consider it unnecessary to make any changes to those clauses.

30. On whether clause 37(2)(a) should explicitly provide that only "reasonable force" would be used, we are of the view that the wording of clause 37(2)(a) is not unusual as many laws of Hong Kong authorize the use of force but do not expressly spell out the words “reasonable force”. The notion of “reasonableness” is already built in the administrative law regime. Therefore we are of the view that it is not necessary to explicitly provide that only “reasonable force” should be used. This is consistent with the power of arrest of the Police as provided under section 50 of the Police Force Ordinance (Cap. 232) and the power of investigating officers under section 122 of the Copyright Ordinance (Cap. 528).

31. On whether clause 37(3)(b) should specify that the information that TA might require to be produced included "passwords" to ensure that TA could obtain relevant information contained in a computer or any other telecommunications device in carrying out a search under clause 37, we agree to the Member’s suggestion and a new clause 37(3)(ab) is proposed accordingly to empower TA to seek information (such as passwords), documents or other things.

Meeting on 19 December 2006

Service of Notice (clause 34)

32. We agree to a Member's suggestion to prescribe the manner in which a notice issued by the TA under various provisions of the Bill should be served on the person concerned. We propose to add a new clause 40A which is modeled on relevant provisions in the Broadcasting Ordinance (Cap.562).

Powers of entry, search and arrest (clause 37)

33. A comparison between the provisions on the powers of entry, search and arrest in the Bill and similar provisions in the Telecommunications Ordinance, the Broadcasting Ordinance and the Interception of Communications and Surveillance Ordinance (Cap.589) is at **Annex B**.

34. On whether the affected person would be provided with a copy of the search warrant under the existing procedures, the Security Bureau advised that the law enforcement agencies will act according to the various legislative provisions prescribing the circumstances under which the powers of entry, search and arrest may be exercised, and will keep the relevant persons affected appropriately informed. As far as the current arrangements for search warrants are concerned, generally, the search warrant will be shown to the affected person. A copy of the warrant will be provided to the affected persons if he so requests. OFTA, when exercising such powers in accordance with the various legislative provisions under the Telecommunications Ordinance, takes a similar approach. We are of the view that the existing procedures are sufficient to safeguard the rights of the person affected.

Obstruction of Authority and authorized officers (clause 39)

35. We wish to clarify that it is our intention to apply the penalties provided for in clause 39 to cases of non-compliance under clause 37 only. To make clear our policy intention, we propose to suitably amend clause 39. For non-compliance with directions issued by the TA under clause

33(1), as above-mentioned, a new clause is proposed to prescribe the penalty.

Recovery of costs and expenses (clause 40)

36. A Member enquired about the policy to allow trading fund agencies to recover the costs and expenses of investigation. We wish to clarify that it is not a common arrangement for trading fund departments to undertake law enforcement responsibility. Under section 36A(6) of the Telecommunications Ordinance, OFTA is empowered to recover any costs or expenses incurred in respect of a determination or determination process under subsection 36A(1) of Telecommunications Ordinance. Since the OFTA Trading Fund is not funded by the Government but by licence fees, we are of the view that it is reasonable for OFTA to recover the costs and expenses incurred in the course of investigations from parties convicted of offences under the Bill.

37. Drawing reference to section 36A(6) of the Telecommunications Ordinance, we propose to state in a new clause 40(4) of the Bill that the recoverable costs and expenses include, but are not limited to, staff costs and expenses, and the financing of liabilities, paid out of the OFTA Trading Fund. As such, the costs of police officers undertaking investigations for potential offences under Part 4 of the Bill, as well as assisting TA in the course of investigation or enforcement work, which would not charged to the OFTA Trading Fund, would not be recovered from the convicted offenders.

Establishment of the Appeal Board (clause 43)

38. A Member suggested that the basic criteria for the appointments of the Chairman, Deputy Chairman and panel members of the Appeal Board (e.g. there must not be any conflict of interest) and the maximum tenure of the appointments of panel members should be stated explicitly in the Bill. We are of the view that it is unnecessary to specify in the Bill the basic criteria for appointment (other than the necessary qualifications), as only persons with suitable capability and background would be appointed and any potential conflicts of interest must be declared before they are involved in any hearings. The current provision is

consistent with the provisions in relation to the establishment of other Appeal Boards, such as the Telecommunications (Competition Provisions) Appeal Board and Administrative Appeals Board.

39. As to the tenure of appointment of panel members, we remain of the view that it is unnecessary to specify the maximum tenure in the Bill in order to maintain flexibility to appoint panel members who may wish to serve a longer or shorter tenure. In any event, for such appointments, we will stick to the "six boards, six years" rule as far as practicable.

Meeting on 16 January 2007

Liability of directors, partners, etc (clause 54)

40. To make clear that an evidential burden, rather than a legal burden, will be imposed on the persons who are responsible for the internal management of companies, partnerships or unincorporated body, we propose to amend clause 54 drawing reference to the proposed CSAs of similar provisions of the Copyright Rights (Amendment) Bill 2006 which had been agreed by the Bills Committee for that Bill.

Matters excluded from application of Ordinance (Schedule 1)

41. It is our intention that those television programme services which are not licensed under the Broadcasting Ordinance, such as broadband TV, should similarly be excluded from application of the Bill. We, therefore, propose amendments to Schedule 1 of the Bill accordingly.

Other Proposed CSAs

42. In addition to a number of minor technical and drafting amendments aiming at improving the provisions of the Bill, we propose the following amendments to strengthen the Bill.

Commencement Date (clause 1)

43. It is our intention to bring the Bill, except Part 2 and certain provisions related to the opt-out regime, into force as soon as possible after

enactment. We hence propose to amend clause 1(2) and add a new clause 1(1A) to the effect that the enacted Bill, except Part 2 and certain provisions related to the opt-out regime, can commence operation immediately upon gazettal without the need to make a separate commencement notice. For Part 2 and those related provisions, they will come into operation on a day to be appointed by SCIT through a commencement notice, which is subject to negative vetting by the Legislative Council (LegCo).

44. In this connection, we wish to advise the Committee that because of tendering procedures and system development, the do-not-call registers could only be ready for operation by November 2007 at the earliest. The TA intends to set up three such registers, one for pre-recorded electronic messages, one for fax messages and one for SMS/MMS messages. Depending on the interest of the registered users of telephone numbers, taking into account the capacity of the computer systems of the do-not-call registers and that there are over 10 million telephone and fax numbers in use, we estimate that it could take some three months for all registered users of telephone and fax numbers to place their telephone or fax numbers on the registers. If it is considered desirable that all registered users of telephone and fax numbers should be given an opportunity to place their telephone or fax numbers on the registers before the relevant statutory provisions related to do-not-call registers and the opt out regime commence operation, then the commencement date of those provisions would need to be deferred to early 2008. On the other hand, if it is considered acceptable for the opt-out regime to be brought into operation as soon as the do-not-call registers are operational, without any time allowed for "pre-registration" of telephone and fax numbers on the registers, then the commencement date of the provisions related to do-not-call registers and the opt out regime could be advanced to November 2007. We wish to seek the Members' views on which timeframe is more desirable.

Claims for loss or damage (clause 52)

45. After further consideration, we agree to the suggestion of the Assistant Legal Advisor of LegCo to clarify that clause 52(1) applies to any contravention, whether or not the contravention is itself an offence

under the Bill, or whether the person has been convicted of an offence in relation to the contravention.

Exemption (Schedule 1)

46. In their submissions and presentations to the Bills Committee, some members of the industry and some chambers of commerce were concerned that transactional or service-related messages, such as bills or invoices with company logos or short promotion messages, introductory messages for services, warranty information, etc, may fall within the definition of "commercial electronic message" and could cause substantial disruption to their normal correspondence with their customers. After further consideration and drawing reference to the arrangements in the CAN-SPAM Act of the US, we propose to exempt commercial electronic messages the primary purpose of which is transactional, service-related or employment related from the application of Part 2 of the Bill. The proposed exemptions are prescribed in the proposed items 2 to 4 of the Table 2 of Schedule 1.

Communications and Technology Branch
Commerce, Industry and Technology Bureau
22 February 2007

Annex A

Charging Scheme of Do-not-Call Registers in the United States and the United Kingdom

United States

Annual charge for accessing the national registry	US$ 17,050 (HK$ 133,000)
Annual charge for accessing one area code[1]	US$ 62 per area (HK$484)

United Kingdom

	Residential TPS[2]	Corporate TPS
Annual charge[3] for accessing the full TPS	£ 3,184 (HK$47,760)	£ 6,368 (HK$95,520)
Annual charge for accessing up to 50% of the TPS	£ 2,385 (HK$35,775)	£ 5,546 (HK$83,190)
Annual charge for accessing up to 25% of the TPS	£ 1,274 (HK$19,110)	£ 2,543 (HK$38,145)
Annual charge for accessing up to 5% of the TPS	£ 475 (HK$7,125)	£ 951 (HK$14,265)
Annual charge for accessing up to 1% of the TPS	£ 317 (HK$4,755)	£ 640 (HK$9,600)

---

1 There are 383 area codes in the United States each of which contains about 0.5 million numbers.

2 The do-not-call register in the United Kingdom is called Telephone Preference Service (TPS), comprises two parts, namely the resident TPS holding residential telephone numbers and corporate TPS containing the number of business users.

3 A 28-day charge is also offered that allow telemarketers access to the system up to 28 days at about 15% of the costs listed.

Annex B

Administration's Response to Issue Raised at the Bills Committee meeting on 19 December 2006 relating to powers of entry, search and arrest

PURPOSE

At its meeting on 19 December 2006, the Bills Committee requested the Administration to explain how the provisions in clause 37 and 38 of the Bill which confer powers of entry, search and arrest compared with similar provisions in the Telecommunications Ordinance (Cap. 106), the Broadcasting Ordinance (Cap. 562) and the Interception of Communications and Surveillance Ordinance (Cap. 589). This paper briefs members on the differences and similarities of the relevant provisions.

POWERS OF ENTRY AND SEARCH

The Bill

2. Clause 37(1)(b) of the Bill empowers the Telecommunications Authority (TA) or any authorized officer to enter and search any premises or place where a warrant has been issued under clause 38 in respect of the premises or place. Under clauses 37(2)(a) and (b), the TA or an authorized officer may break into and forcibly enter any premises or place that he is empowered to enter and search and may remove by force any person or thing obstructing him in the performance of such functions.

3. Under clause 38, a magistrate may issue a warrant to empower the TA or an authorized officer to enter and search any premises or place if the magistrate is satisfied by information on oath that there are reasonable grounds for suspecting that there is, or is likely to be, in or on the premises or place any telecommunications device or other thing that is or that contains, or that is likely to be or to contain, evidence of the commission of a specified offence. The term "specified offence" is

defined by clause 26 to mean an offence under Part 3 or Part 5 of the Bill. It does not cover offences under Part 4 or Part 6 of the Bill.[1]

Telecommunications Ordinance (Cap. 106)

4. The Telecommunications Ordinance (Cap. 106) contains two provisions relating to the entry and search of premises for the purposes of the enforcement of that Ordinance. The first provision is section 32J (Appendix A). Under section 32J(7), a magistrate may issue a warrant to empower the TA or any authorized officer to enter and search any premises, vehicle, aircraft or vessel specified in the warrant and to examine, test and confiscate any apparatus found on or in the premises, vehicle, aircraft or vessel. A warrant may only be issued if the magistrate is satisfied by information on oath that access to the premises, vessel, aircraft or vehicle, or permission to examine or test the apparatus, has been requested and has been unreasonably refused.

5. The second provision is section 35 (Appendix A). Under section 35(1)(b), the TA or any public officer authorized by the TA is authorized to enter and search any place, or board and search any vessel or aircraft (except ships of war and military aircraft), or search any vehicle, in which he reasonably suspects that there is anything liable to seizure under section 35(1)(c). The things liable to seizure under section 35(1)(c) are things in respect of which the TA or authorized public officer reasonably suspects an offence has been committed or that appear to him to be or to be likely to be, or to contain, evidence of an offence. Under section 35(1)(d), the TA or authorized public officer may also enter and inspect any premises at or from which any person manufactures, sells or otherwise deals in apparatus that may be used for telecommunications. Section 35(2) provides that no premises used for dwelling purposes shall be entered or searched except pursuant to the warrant of a magistrate issued under that section.

6. Under section 35(3)(a), (b) and (c), the TA or an authorized public officer may break open any outer or inner door of any place that he is empowered or authorized by or under Cap. 106 to enter and search, may forcibly board any vessel, aircraft or vehicle that he is empowered by Cap. 106 to board and search, and may remove by force any person or

[1] Parts 1, 2 and 7 of the Bill do not contain any offences.

thing obstructing any arrest, detention, search, inspection, seizure or removal that he is empowered to make.

7. Regulation 14 of the Telecommunications Regulations (Cap. 106 sub. leg. A) (Appendix B) and regulation 6 of the Telecommunications (Control of Interference) Regulations (Cap. 106 sub. leg. B) (Appendix C) also authorize a magistrate, in the circumstances specified in those regulations, to issue a warrant to empower the TA or any public officer authorized by the TA to enter and search any premises, vehicle, aircraft or vessel specified in the warrant.

8. The powers of entry and search conferred by clause 37 of the Bill are narrower in scope than those conferred by sections 32J and 35 of Cap. 106. Under clause 37(1)(b), the TA or an authorized officer must obtain a warrant issued by a magistrate under clause 38 before they may enter and search any premises or place. The same requirement for a warrant applies in relation to entry and search under section 32J of Cap. 106 but under section 35 of Cap. 106 a warrant is only required for the entry and search of premises used for dwelling purposes. In effect, no warrant is required under section 35 of Cap. 106 in connection with the entry and search of premises that are not used for dwelling purposes, such as business premises.

9. With regard to the use of force in effecting entry onto the premises, the powers given to the TA and authorized officers under clauses 37(2)(a) and (b) of the Bill are similar in scope to those given to the TA and authorized public officers under section 35(3)(a), (b) and (c) of Cap. 106 although the form of wording used in Cap. 106 is different.

Broadcasting Ordinance (Cap. 562)

10. Section 7A of the Broadcasting Ordinance (Cap. 562) is the only provision of that Ordinance that confers powers of entry and search (Appendix D). Under section 7A(1)(c), the TA or any public officer authorized by the TA is authorized to enter and search any premises on which he reasonably believes that the person has committed or has attempted to commit an offence under section 6(1) or (1A) or 7(1) of Cap 562. Section 7A(3) provides that domestic premises shall not be entered or searched except pursuant to the warrant of a magistrate issued under section 7A(4).

11. Under section 7A(5)(a) and (b), the TA or an authorized public officer may break open any outer or inner door of any place that he is authorized to enter and search and may remove by force any person or thing obstructing him or resisting any arrest, detention, search, inspection, seizure or removal that he is empowered to make or carry out.

12. The powers of entry and search conferred by clause 37 of the Bill are narrower in scope than those conferred by section 7A of Cap. 562. Under clause 37(1)(b), the TA or an authorized officer must obtain a warrant issued by a magistrate under clause 38 before they may enter and search any premises or place. Under section 7A of Cap. 562, a warrant is only required for the entry and search of domestic premises. In effect, no warrant is required in connection with the entry and search of premises used for non-domestic purposes, such as business premises.

13. With regard to the use of force, the powers given to the TA and authorized officers under clauses 37(2)(a) and (b) of the Bill are similar in scope to those given to the TA and authorized public officers under section 7A(5)(a) and (b) of Cap. 562 although the form of wording used in Cap. 562 is different.

Interception of Communications and Surveillance Ordinance (Cap. 589)

14. The Interception of Communications and Surveillance Ordinance (Cap. 589) contains two provisions relating to the entry onto premises for the purposes of that Ordinance, i.e. sections 29 and 37(1)(b) (Appendix E).

15. It is inappropriate to draw comparisons between the provisions of Cap. 589 which confer ancillary powers of entry only and the provisions of the Bill which confer powers of entry and search. The powers of entry and search conferred by clauses 37 and 38 relate to the general enforcement of specified offences under the Bill. The powers of entry found in Cap. 589, on the other hand, serve a substantially different purpose i.e. to facilitate the carrying out of covert operations authorized under that Ordinance.

16. With regard to the use of force, the relevant provisions of Cap. 589 provide that “reasonable” force may be used “if necessary”. Clause 37(2)(a) of the Bill also authorizes the use of force but it does not

specifically state that the force used must be "reasonable". However, the wording of clause 37(2)(a) is not unusual insofar as the use of force is concerned. Many Ordinances authorize the use of force to effect the entry onto premises but do not expressly limit it to "reasonable" force.[2] The notion of "reasonableness" will be implied by the common law.[3]

POWERS OF ARREST

The Bill

17. Clause 37(1)(a) of the Bill empowers the TA or any authorized officer to arrest, without warrant, any person whom he reasonably suspects of having committed a specified offence. Under clause 37(4), the TA or any authorized officer must, without delay, take an arrested person to a police station to be dealt with there in accordance with the Police Force Ordinance (Cap. 232) or deliver him into the custody of a police officer for that purpose.

[2] See , for example, s. 14(2)(b) of the Dutiable Commodities Ordinance (Cap. 109), s. 10(1) of the Coroners Ordinance (Cap. 504), s. 122(2)(a) of the Copyright Ordinance (Cap. 528), s. 18(4)(a) of the Prevention of Copyright Piracy Ordinance (Cap. 544), s. 191(1) of the Securities and Futures Ordinance (Cap. 571), s. 17(1)(a) of the Construction Workers Registration Ordinance (Cap. 583) and s. 33(1) of the Protection of Endangered Species of Animals and Plants Ordinance (Cap. 586).

[3] It is a doctrine of administrative law that statutory powers must be exercised reasonably. See generally, Wade and Forsyth, *Administrative Law*, 9th ed., 2004, Oxford University Press, at pp. 351-361. In relation to searches, this principle is illustrated by the case of *Simpson v Attorney General (Baigent's Case)* 1994 3 NZLR 667 (New Zealand Court of Appeal) where Hardie Boys J stated at p. 694 that "a search that is carried out unreasonably exceeds the authority conferred by the warrant".

Telecommunications Ordinance (Cap. 106)

18. Section 35(1)(a) of Cap. 106 empowers the TA or any public officer authorized by the TA to arrest any person whom he reasonably suspects of being guilty of an offence under that Ordinance (Appendix A). Section 35(1)(a) is similar to clause 37(1)(a) of the Bill except that the latter provision, in conformity with more common precedents[4], makes clear that the arrest may be made without a warrant.

29. Cap. 106 does not contain any provisions equivalent to clause 37(4) of the Bill (i.e., provisions requiring the arrested person to be brought to a police station). However, in practice, the TA follows the same procedure.

Broadcasting Ordinance (Cap. 562)

20. Section 7A(1)(b) of the Broadcasting Ordinance (Cap. 562) authorizes the TA and any public officer authorized by the TA to arrest any person whom he reasonably suspects of being guilty of an offence under section 6(1) or (1A) or 7(1) of that Ordinance (Appendix D). Section 7A(1)(b) of Cap. 562 is similar to clause 37(1)(a) of the Bill except that that the latter provision, in conformity with more common precedents[5], makes clear that the arrest may be made without a warrant.

21. Section 7A(2) of Cap. 562 is similar to clause 37(4) of the Bill, which requires the arrested person to be brought to a police station.

---

[4] See, for example, s. 11(1) of the Oil (Conservation and Control) Ordinance (Cap. 264), s. 11(1) of the Agricultural Products (Marketing) Ordinance (Cap. 277), s. 11(1) of the Reserved Commodities Ordinance (Cap. 296), s. 11(1) of the Protection of Non-Government Certificates of Origin Ordinance (Cap. 324), ss. 11(2) and 14(5) of the Prisoners (Release under Supervision) Ordinance (Cap. 325), ss. 12(2) and 13B(1) of the Immigration Service Ordinance (Cap. 331), s. 17A(1) of the Customs and Excise Service Ordinance (Cap. 342), s. 19(3) of the Marine Fish Culture Ordinance (Cap. 353), s. 16B(1) of the Trade Descriptions Ordinance (Cap. 362), s. 38(1) of the Kowloon-Canton Railway Corporation Ordinance (Cap. 372), s. 20(1)(b) of the Amusement Rides (Safety) Ordinance (Cap. 449), s. 25(2) of the Marine Parks Ordinance (Cap. 476) s. 13(1)(b) of the Aviation Security Ordinance (Cap. 494), ss. 26(1) and 40(1) of the Long-term Prison Sentences Review Ordinance (Cap. 524), s. 22(1) of the Mutual Legal Assistance in Criminal Matters Ordinance (Cap. 525), s. 8(1) of the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526), s. 9(1) of the Rehabilitation Centres Ordinance (Cap. 567), s. 18(1) of the Chemical Weapons (Convention) Ordinance (Cap. 578) and s. 37 of the Protection of Endangered Species of Animals and Plants Ordinance (Cap. 586).

[5] See footnote 7.

Interception of Communications and Surveillance Ordinance (Cap. 589)

22. The Interception of Communications and Surveillance Ordinance (Cap. 589) does not contain any offences or provisions conferring powers of arrest.

Communications and Technology Branch
Commerce, Industry and Technology Bureau
February 2007

Sections 32J and 35 of the Telecommunications Ordinance (Cap. 106)

32J. Interference

(1) A person shall not knowingly, and without lawful excuse, use an apparatus, whether or not it is an apparatus for telecommunications, in a manner that causes direct or indirect harmful interference with any telecommunications service lawfully carried on, or other apparatus for telecommunications lawfully operated, in or outside Hong Kong.

(2) The Authority may, by notice in writing, direct a person possessing an apparatus, whether or not it is an apparatus for telecommunications, to take such measures as the Authority specifies and within the time directed to prevent the interference specified in the notice.

(3) A person who contravenes subsection (1) or fails to comply with the direction in subsection (2) commits an offence and shall be liable on summary conviction to a fine at level 5 and to imprisonment for 6 months.

(4) The Authority may, by order, specify the limits of conducted or radiated interference from any apparatus which is not subject to the licensing requirement under section 8, to prevent harmful interference with telecommunications networks, systems, installations or services.

(5) The powers of the Authority under Part VA extend to the apparatus mentioned in subsection (4).

(6) The Authority may require an apparatus mentioned in subsection (4) to be submitted to the Authority for testing to verify whether the apparatus complies with the limits specified by the Authority under that subsection.

(7) A magistrate may, if he is satisfied by information on oath that—

(a) access to premises, vessel, aircraft or vehicle has been requested; or

(b) permission to examine or test any apparatus has been requested,

and in either case has been unreasonably refused, issue a warrant empowering the Authority, or an authorized officer, to enter and search the premises, vehicle, aircraft or vessel specified in the warrant and to examine, test and confiscate any apparatus found on or in the premises, vehicle, aircraft or vessel.

35. Power of Authority

(1) The Authority, or any public officer authorized in writing in that behalf by the Authority, may—

(a) arrest any person whom he reasonably suspects of being guilty of an offence under this Ordinance;

(b) subject to subsection (2), enter and search any place, or board and search any vessel (other than a ship of war) or any aircraft (other than a military aircraft) or search any vehicle, in which he reasonably suspects that there is anything liable to seizure under paragraph (c);

(c) seize, remove and detain—

(i) anything in respect of which he reasonably suspects that an offence under this Ordinance has been committed;

(ii) anything that appears to him to be or to be likely to be, or to contain, evidence of an offence under this Ordinance;

(d) enter and inspect the premises at or from which any person manufactures, sells or otherwise deals in apparatus that may be used for telecommunications and require the production to him of any books or documents relating to such apparatus.

(2) Where he is satisfied by information on oath that there is reasonable ground for suspecting that there is in any premises used for dwelling purposes anything that is liable to seizure under subsection (1)(c), a magistrate may issue his warrant authorizing such premises to be entered and searched by the Authority or any other public officer, and no premises used for dwelling purposes shall be entered or searched under this Ordinance except pursuant to the warrant of a magistrate issued under this subsection.

(3) The Authority or any public officer may—

(a) break open any outer or inner door of any place that he is empowered or authorized by or under this Ordinance to enter and search;

(b) forcibly board any vessel, aircraft or vehicle that he is empowered by this Ordinance to board and search;

(c) remove by force any person or thing obstructing any arrest, detention, search, inspection, seizure or removal that he is empowered by this Ordinance to make;

(d) detain any person found in any place that he is empowered or authorized by or under this Ordinance to search until such place has been searched;

(e) detain any vessel or aircraft that he is empowered by this Ordinance to board and search, and prevent any person from approaching or boarding such vessel or aircraft, until it has been searched;

(f) detain any vehicle that he is empowered by the Ordinance to search until it has been searched.

Appendix B

Regulation 14 of the Telecommunications Regulations (Cap. 106 sub. leg. A)

14. Entry and search of premises etc.

(1) Where a magistrate is satisfied by information on oath that—

(a) there are reasonable grounds for believing that there is, upon any specified premises or in any specified vessel, aircraft or vehicle, apparatus for telecommunications and—

(i) the apparatus is possessed or used without lawful authority or contrary to the terms of the licence or other authority authorizing such possession or use, and additionally or alternatively;

(ii) the Authority has reasonable grounds for examining and testing any apparatus found in or on such premises, vessel, aircraft or vehicle;

(b) access to such premises, vessel, aircraft or vehicle has been demanded, or permission to examine or test any such apparatus has been requested, but in either case has been unreasonably refused,

the magistrate may issue his warrant empowering the Authority, or any public officer authorized in writing in that behalf by the Authority to enter and search such premises, vessel, aircraft or vehicle and to examine and test any apparatus found thereon or therein.

(2) Any person who obstructs or hinders the Authority or any public officer acting under the authority of a warrant issued under subregulation (1) shall be guilty of an offence and liable on conviction to a fine of $20000 and to imprisonment for 6 months.

Regulation 6 of the Telecommunications (Control of Interference) Regulations (Cap. 106 sub. leg. B)

6. Entry and search of premises etc.

Where a magistrate is satisfied by information on oath—

(a) that there is reasonable ground for believing that, on any specified premises or in any specified vessel, aircraft or vehicle, apparatus to which these regulations apply is to be found which does not comply with the requirement applicable to it under these regulations; and

(b) that it is necessary to enter those premises, or that vessel, aircraft or vehicle, and to examine or test any apparatus to which these regulations apply which may be found therein or thereon for the purpose of determining whether any such apparatus does or does not comply with the requirement applicable to it under these regulations; and

(c) that, within fourteen days before the date of the application to such magistrate, access to the premises, vessel, aircraft or vehicle for the purpose aforesaid has been demanded by, or permission to examine any such apparatus as aforesaid which has been found therein or thereon has been requested by, the Authority or any public officer authorized in writing in that behalf by the Authority and producing sufficient documentary evidence of his identity and, in the case of a public officer authorized as aforesaid, of his authority, but in either case has been unreasonably refused,

the magistrate may issue his warrant empowering the Authority or any public officer or officers authorized in writing in that behalf by the Authority and named in such authorization to enter the premises or, as the case may be, the vessel, aircraft or vehicle and any premises on which it may be and to search the premises, vessel, aircraft or vehicle with a view to discovering whether any apparatus to which these regulations apply is situate thereon or therein, and, if he finds or they find any such apparatus thereon or therein, to examine and test it with a view to determine whether it does or does not comply with the requirement applicable to it under these regulations.

Section 7A of the Broadcasting Ordinance (Cap. 562)

7A. Provisions supplementary to sections 6 and 7

(1) Where the Telecommunications Authority or any public officer authorized in writing in that behalf by the Telecommunications Authority has reasonable grounds for believing that a person has committed or has attempted to commit an offence under section 6(1) or (1A) or 7(1), then he may—

(a) require the person to produce for his inspection, at any place specified by him, any unauthorized decoder or decoder—

(i) imported, exported, manufactured, sold, offered for sale or let for hire by the person in the course of trade or business; or

(ii) possessed or used, or authorized to be possessed or used, for the purpose of, or in connection with, any trade or business;

(b) arrest any person whom he reasonably suspects of being guilty of an offence under section 6(1) or (1A) or 7(1);

(c) subject to subsection (3), enter and search any premises on which he reasonably believes that the person has committed or has attempted to commit an offence under section 6(1) or (1A) or 7(1), and require the production to him of any books or documents relating to any unauthorized decoder or decoder referred to in paragraph (a);

(d) seize, remove and detain—

(i) any unauthorized decoder or decoder referred to in paragraph (a);

(ii) anything that appears to him to be or to be likely to be, or to contain, evidence of an offence under section 6(1) or (1A) or 7(1).

(2) Where a public officer referred to in subsection (1) arrests a person under paragraph (b) of that subsection, the public officer shall, without delay, take him to a police station to be dealt with there in accordance with the Police Force Ordinance (Cap 232) or deliver him into the custody of a police officer for that purpose.

(3) Domestic premises shall not be entered or searched under subsection (1)(c) except pursuant to a warrant issued under subsection (4).

(4) Where a magistrate is satisfied by information on oath that there are reasonable grounds for suspecting that there is anything liable to seizure under subsection (1)(d) in any domestic premises possessed or used by a person whom he has reasonable grounds for believing has committed or has attempted to commit an offence under section 6(1) or (1A) or 7(1), then he may issue a warrant authorizing the Telecommunications Authority or any other public officer to enter and search the premises.

(5) The Telecommunications Authority or any public officer authorized in writing in that behalf, in the exercise of the powers under subsection (1) or pursuant to a warrant issued under subsection (4), may—

(a) break open any outer or inner door of any place that he is empowered or authorized to enter and search;

(b) remove by force any person or thing obstructing him or resisting any arrest, detention, search, inspection, seizure or removal that he is empowered to make or carry out;

(c) detain any person found in any place that he is empowered or authorized to search until such place has been searched.

(6) A magistrate or court may, upon application by or on behalf of the Telecommunications Authority or by any public officer authorized in writing in that behalf by the Telecommunications Authority, order that any unauthorized decoder or decoder in respect of which there has been a contravention or attempted contravention of section 6(1) or (1A) or 7(1) shall be forfeited to the Government, whether or not proceedings have been taken against any person in respect of the contravention or attempted contravention.

(7) Any person who wilfully obstructs the Telecommunications Authority or any public officer authorized in writing in that behalf by the Telecommunications Authority in the exercise of any power conferred upon him under this section shall be guilty of an offence and shall be liable on summary conviction to a fine at level 4 and to imprisonment for 6 months.

Sections 29 and 37 of Interception of Communications and Surveillance Ordinance (Cap. 589)

29. What a prescribed authorization may authorize or require under or by virtue of its terms, etc.

(1) A prescribed authorization for interception may—

(a) in the case of a postal interception, contain terms that authorize one or both of the following—

(i) the interception of communications made to or from any premises or address specified in the prescribed authorization;

(ii) the interception of communications made to or by any person specified in the prescribed authorization (whether by name or by description); or

(b) in the case of a telecommunications interception, contain terms that authorize one or both of the following—

(i) the interception of communications made to or from any telecommunications service specified in the prescribed authorization;

(ii) the interception of communications made to or from any telecommunications service that any person specified in the prescribed authorization (whether by name or by description) is using, or is reasonably expected to use.

(2) A prescribed authorization for covert surveillance may contain terms that authorize one or more of the following—

(a) the use of any surveillance devices in or on any premises specified in the prescribed authorization;

(b) the use of any surveillance devices in or on any object or class of objects specified in the prescribed authorization;

(c) the use of any surveillance devices in respect of the conversations, activities or location of any person specified in the prescribed authorization (whether by name or by description).

(3) A prescribed authorization, other than an executive authorization, may contain terms that authorize the doing of anything reasonably necessary to conceal any conduct authorized or required to be carried out under the prescribed authorization.

(4) A prescribed authorization, other than an executive authorization, may, if it is reasonably necessary for the execution of the prescribed authorization, contain terms that authorize the interference with any property (whether or not of any person who is the subject of the interception or covert surveillance concerned).

(5) A prescribed authorization, other than an executive authorization, may contain terms that require any person specified in the prescribed authorization

(whether by name or by description), on being shown a copy of the prescribed authorization, to provide to any of the officers of the department concerned such reasonable assistance for the execution of the prescribed authorization as is specified in the prescribed authorization.

(6) A prescribed authorization for interception also authorizes—

(a) the installation, use and maintenance of any devices required to be used in order to intercept any of the communications authorized to be intercepted under the prescribed authorization;

(b) the entry, by the use of reasonable force if necessary, onto any premises in order to carry out any conduct authorized or required to be carried out under the prescribed authorization;

(c) the incidental interception of any communication which necessarily arises from the interception of communications authorized to be carried out under the prescribed authorization; and

(d) where subsection (1)(a)(ii) or (b)(ii) is applicable, the provision to any person, for the execution of the prescribed authorization, of particulars of the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying—

(i) in the case of subsection (1)(a)(ii), the communications made to or by the person specified in the prescribed authorization; or

(ii) in the case of subsection (1)(b)(ii), the communications made to or from any telecommunications service that the person specified in the prescribed authorization is using, or is reasonably expected to use.

(7) A prescribed authorization for covert surveillance also authorizes—

(a) where subsection (2)(a) is applicable—

(i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on the premises specified in the prescribed authorization; and

(ii) in the case of Type 1 surveillance, the entry, by the use of reasonable force if necessary, onto the premises, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization;

(b) where subsection (2)(b) is applicable—

(i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on the object, or an object of the class, specified in the prescribed authorization; and

(ii) in the case of Type 1 surveillance, the entry, by the use of reasonable force if necessary, onto any premises

where the object, or an object of the class, is reasonably believed to be or likely to be, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization; and

(c) where subsection (2)(c) is applicable—

(i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on any premises where the person specified in the prescribed authorization is reasonably believed to be or likely to be; and

(ii) in the case of Type 1 surveillance, the entry, by the use of reasonable force if necessary, onto the premises, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization.

37. What a device retrieval warrant also authorizes

(1) A device retrieval warrant also authorizes the undertaking of conduct, including the following conduct, that is necessary for and incidental to the carrying out of what is authorized to be carried out under the warrant—

(a) the retrieval of any enhancement equipment for the devices authorized to be retrieved under the warrant;

(b) the entry, by the use of reasonable force if necessary, onto any premises where the devices or enhancement equipment is reasonably believed to be or likely to be, and onto any other premises adjoining or providing access to the premises, in order to retrieve the devices or enhancement equipment;

(c) the temporary removal of any conveyance or object from any premises for the retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises;

(d) the breaking open of anything for the retrieval of the devices or enhancement equipment; and

(e) the provision of assistance for the execution of the warrant.

(2) A device retrieval warrant which authorizes the retrieval of any tracking devices also authorizes the use of the tracking devices and any enhancement equipment for the tracking devices solely for the purposes of the location and retrieval of the tracking devices or enhancement equipment.