Information & Communications Technology Authority

Public Consultation

on

Policy for Unsolicited Electronic Messages

Ref: CD 2006-2

Launch Date: 20th June 2006

Closing date: 18th August 2006

INTRODUCTION

Spam

1. Spam is the term now generally used to refer to unsolicited bulk messages, usually transmitted to a large number of recipients via electronic mediums such as email. They usually have a focus on promoting products, services or fraudulent schemes.

2. Major problems caused by spam are breaches of privacy and a lowering of user confidence, deceptive practices, illegal or offensive content such as pornography and scams, threats to network integrity and security, desired email getting blocked by anti-spam technologies, and the financial costs imposed on ISPs and users.

3. Due to the problems caused by spam and the continuing growth in the volume of spam, a number of governments around the world have enacted or are proposing legislation as one way of curbing spam growth. The ICT Authority considers that legislation against spam may be an appropriate measure for the Cayman Islands also.

Purpose and Scope of Discussion Paper

4. This discussion paper seeks to discuss and obtain feedback on the various policy issues which are raised when considering anti-spam legislation. The objective is to ensure that any anti-spam legislation enacted in Cayman Islands is an effective tool as part of a multi-pronged attack on spam.

5. The paper does not seek to consider content issues such as the sending of pornography over the Internet as these are dealt with under existing legislation. Its focus is rather on addressing the spam problem in general.

Next Steps

6. Subsequent to the receipt of submissions, the ICT Authority will prepare a paper for submission to the Ministry of Communications, Works and Infrastructure on any proposed anti-spam legislation.

7. Views expressed in submissions will be taken into account in the policy development process. It is envisaged that a summary of views will be prepared and published on the Authority's website (www.icta.ky).

BACKGROUND

The forms of spam in the Cayman Islands

8. Unsolicited electronic messages sent over a variety of ICT networks and services are generally described as spam. (Use of the term "spam" was adopted as a result of the Monty Python skit in which a group of Vikings sang a chorus of "spam, spam, spam . . . " in an increasing crescendo, drowning out other conversation. Hence, the analogy applies because such messages are drowning out normal discourse on the Internet.) Spam largely takes the form of unwanted, unsolicited, emails via the Internet which are sent to market or promote some good, service or scam, but can also include SMS text messages, faxes and even telephone calls. How exactly to define “spam” is one of the key issues raised in the paper.

9. Most, but not all, spam received in the Cayman Islands originates from overseas. This highlights the need for International co-operation to address the spam problem. The ICT Authority represents the Cayman Islands at several of the international forums attempting to address this problem.

The detrimental effects and costs of spam

10. Recent studies have determined that between 55 and 75% of all Internet email messages are spam. Email spam imposes costs on all Internet users. It is a nuisance to have to continually deal with unwanted emails. More importantly, however, spam uses scarce resources of users and services providers without compensation or approval. Spam consumes network and computing resources, email administrator and helpdesk personnel time, and reduces worker productivity. The costs are inevitably passed on to the end user as part of their Internet connection charges, while the sender pays virtually nothing.

11. Unlike unsolicited emails, unsolicited telephone calls, faxes and SMS messages are paid for by the sender at least in part and therefore the volumes tend to be less. Nevertheless, many individuals find them most annoying and businesses object to the waste of time and, in the case of faxes, of consumables.

12. The practice of spamming also raises concerns associated with privacy, fraudulent or deceptive messages, the sending of pornographic material, attacks on the security and integrity of computer networks through viruses and the like, identity theft, and reduced consumer confidence in the use of the Internet for the purposes of e-commerce. The indiscriminate sending of offensive or pornographic material through spamming is a particular concern because of the harmful effect it can have on the young and the vulnerable.

Measures aimed at reducing spam

13. There are a number of measures which can be used to address the spam problem. These are:

- Legislative/regulatory measures;
- Self-regulatory measures such as industry codes;
- Education and awareness campaigns for business and Internet users;
- Technical measures such as the use of filtering by Internet Service Providers (ISPs) and users.

14. The trend internationally is to address the spam problem through a multi-dimensional approach combining all of the above measures. The United States, United Kingdom, Australia, New Zealand, Japan, Korea and Hong Kong are among the countries that have enacted legislation against spam. There is also work going on at the international level through organizations such as the OECD and the ITU to consider multilateral approaches to the spam problem by promoting international cooperation.

15. The benefits for the Cayman Islands of legislating against spam are:

- It enables legal action to be taken against spammers based in the Cayman Islands;
- It prevents the Cayman Islands being seen as a safe haven for spammers as legislative measures begin to be implemented in overseas jurisdictions;
- It assists the Cayman Islands in efforts to obtain international co-operation to combat overseas sources of spam if we have our own house in order;
- It allows the Cayman Islands authorities to effectively co-operate with overseas government anti-spam enforcement agencies, to help trace the senders and beneficiaries of spam sent to the Islands.

Questions for discussion and response

1. *Do you consider spam to be an important issue? Has it significantly affected you in any way?*
2. *Do you think legislation has a role to play alongside other complimentary measures?*

EXISTING LEGAL AND POLICY PROVISIONS

Misuse / Abuse of ICT Resources

16. The Computer Misuse Law, 2000 appears to provide adequate coverage concerning the misuse or abuse of computing resources in connection with spam, for example Denial of Service (DoS) attacks, creation of "zombie" computers, "harvesting" of email addresses and virus infections. Provided the computer or information in question is located in the Cayman Islands, these provisions apply to any person outside as well as within the Cayman Islands.

17. Section 82 of the Information and Communications Technology Authority Law, 2004 Revision, states that it is an offence to "remove, alter, damage, disrupt, disable or destroy any ICT network or ICT apparatus except in accordance with this Law or the regulations." Although less comprehensive than the Computer Misuse Law, it does appear to extend similar protection to ICT networks and apparatus that might fall outside the definition of "computer".

Use of an ICT Service to defraud, abuse, annoy, threaten or harass

18. Section 89 of the Information and Communications Technology Authority Law makes it an offence to use an ICT network or service to defraud, abuse, annoy, threaten or harass any other person.

19. Whilst this provision might well be used to prosecute someone using spam to defraud, it might be difficult to bring a case based purely upon the "annoyance" or "harassment" caused by a spammer.

Pornographic Material

20. Although the content of spam is outside the scope of this paper, it is noted in passing that section 155 of the Penal Code deals with obscene publications and that it clearly would cover pornographic content in spam. Some might consider that the maximum penalty of $200 and imprisonment for three months should be reviewed.

Liability of Service Providers and Intermediaries

21. The Electronic Transaction Law, 2003 Revision, states at section 32 that in proceedings against an intermediary or e-commerce service provider for an offence consisting of or arising out of the processing of an electronic record by means of his system, it is a defence for him to show that he did not originate the record and that either:

- He did not know that the processing would give arise to an offence, or
- As soon as he knew, or had reasonable cause to suspect, that the processing would result in an offence, he took what steps he could to prevent the processing and he notified the police of any relevant facts in his possession.

22. These provisions currently have little application with respect to spam as, unless the content is such that it breaches either the ICTA Law or the Penal Code, the sending of spam is not an offence. On the other hand, if anti-spam legislation were to be enacted, an ISP would be required to stop a spammer from using his system, and to advise the police, as soon as he "had reasonable cause to suspect" that an offence were being committed.

Privacy of Personal Information

23. Unlike many other countries, the Cayman Islands has no Data Protection legislation. There is, therefore, no legal protection for personal information such as email addresses that may be held on computers.

Transparency

24. No existing legislation covers the spam issue of transparency – invalid sender addresses (both physical and electronic), no unsubscribe function and misleading/inaccurate headers and subject lines on commercial messages.

KY Domain Policies

25. Policies covering all registrants in the .ky (Cayman Islands) Internet domain include the following statement:

"No sub-domain in the .ky name space may be used for the bulk distribution of unsolicited e-mail (SPAM)."

26. Failure to comply with domain policies could result in suspension or revocation of the domain name. There is no definition of either "bulk" or "spam". Moreover, this policy applies only to names registered in the .ky domain. There are many web sites and email servers located in the Cayman Islands, or located elsewhere but registered to Cayman Islands residents or companies, that are not in the .ky domain (e.g. .com, .org)

3. Do you consider the existing legal and policy provisions in this area are sufficient, or do you believe that additional legislative action (law or regulations) is required?

LEGISLATIVE ISSUES

27. The key legislative issues are:

- Legislative scope – what types of messages should be regulated or prohibited and who should be covered?
- The consent issue – should an "opt-in" or "opt-out" approach be adopted?
- Transparency issues – should there be a requirement for electronic messages to:
  - Include accurate sender information?
  - Contain a functional unsubscribe facility?
  - Provide accurate header/subject information?
  - Provide labels if they are advertising or adult messages?
- Privacy issues - should there be rules against the supply, acquisition or use of address-harvesting software and harvested-address lists?
- Enforcement issues – what sanctions and/or remedies should be specified/available?

Legislative Scope

28. In determining what, if any, types of messages should be regulated or prohibited, a number of questions need to be answered. These are:

- What message mediums should be caught by the legislation (e.g. email, short message services using mobile phones, faxes, telephones, (telemarketing)?
- Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?
- Should the messages caught by the legislation be of a commercial advertising and promotional nature only or should other types of messages be caught? Should there be any exceptions?
- Should the legislation extend to coverage of acts outside of the Cayman Islands?

29. There is also the question of who should be covered by anti-spam legislation. Should it be just the sender of the message, or should the legislation also cover the 'sponsor' of the message (normally the vendor of the product or service being promoted or advertised) and others knowingly a party to the sending of an unlawful message. In the case of telecommunications companies and Internet Service Providers, they are unwitting transmitters of spam and so the general approach in other countries is to exclude them from being covered.

30. The issue of what should constitute consent to the sending of a message will be addressed in the next section.

Message mediums

31. The approach of the EU is to apply its legislation to fax, email and other electronic messaging systems such as SMS and MMS (Multi-media Messaging Service). Australia's legislation applies to "electronic messages", which also covers emails, faxes and other electronic messaging systems. It does not apply to voice calls. The United States spam legislation is limited in its coverage to electronic mail via the Internet (telemarketing is regulated separately).

The issue of "bulk"

32. Spam messages are typically sent in bulk. The issue is whether or not legislation should address the "bulk" characteristic, and if so, how. The EU directive does not specifically address the bulk aspect of spam, but rather refers to electronic mail sent for the purposes of direct marketing. It would seem that the reference to direct marketing indirectly refers to email sent in bulk, although there may be exceptions.

33. In the Australian legislation the issue of bulk has been addressed in the penalty provisions rather than in the definition provisions, with more penalty points applying if a greater number of messages have been sent. In the United States legislation the offence provisions apply to the transmission of "multiple commercial electronic messages", where the term "multiple" means "more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period".

34. The issue of bulk is primarily an issue for people or organisations who are attempting to solve or regulate spam because the concern relates to its collective impact. For the recipients of spam, however, the issue of how many other people may have received a message is generally irrelevant. For them it is the content of the message that is the issue of concern.

35. If individual to individual emails are to be classified as spam (as is the case in the Australian legislation), it would seem that this has the potential to catch emails from an individual who has maybe obtained another individual's email address as a result of an exchange of business cards and has initiated contact over a commercial matter such as an offer to supply goods or services. In this case the email could be described as both "commercial" and "unsolicited" in terms of the Australian legislation, unless consent to the sending of the email could be reasonably inferred.

36. While the above conduct would seem to be no different from sending a letter to the same effect, it is arguable that the sender should send an initial email asking the recipient if they would be interested in receiving this type of information first to expressly cover off the consent issue. While it may be possible to address this sort of situation in the definitions of "commercial" and "unsolicited", requiring that there be a bulk element to spam would be one solution.

What types of messages should be caught?

37. Spam messages are typically commercial or promotional in nature. Their content nature may be defined narrowly (e.g. sent for the purposes of direct marketing – EU; the commercial advertisement or promotion of a commercial product or service - USA) to widely (e.g. to offer to supply goods or services, promote goods or services, advertise or promote a supplier of goods or services, offer to supply land or an interest in land, offer to provide or to advertise or promote a business opportunity or investment opportunity, assist or enable a person to dishonestly or deceptively take advantage of another person – Australia).

38. The Australian legislation expressly provides for exclusions from the types of messages caught by its rules. The specified exclusions are messages from government bodies, political parties, religious organizations and charities relating to goods or services supplied by them, and messages from educational institutions to students, former students or households of students or former students relating to goods or services supplied by them.

39. There would seem to be merit in adopting the wider approach taken by the Australian legislation as most people would consider messages as spam and undesirable if they were trying to entice people to participate in a scam just as much as if they were seeking to promote a product or service. The approach to exclusions appears to be based on the idea that there is a public interest in ensuring that certain types of messages with a social value should not be caught as spam.

Extra-territoriality

40. Given that much of the spam received in the Cayman Islands is sent from overseas, should anti-spam legislation extend to coverage of acts outside of the Cayman Islands? While issues of enforcement and jurisdiction arise there would seem to be merit in adopting this approach, as has been done in Australia. In the Australian legislation it provides that it extends to acts, omissions, matters and things outside Australia and that it applies to commercial electronic messages that have an "Australian link". Messages having an "Australian link" include messages sent from overseas to Australian email account holders.

41. There can be situations where the Cayman Islands vendor of a product or service arranges for spam promoting or advertising that product or service to be sent from overseas. By providing that the legislation covers acts outside of the Cayman Islands, the Cayman Islands vendor can then be prosecuted notwithstanding the overseas source of the spam (and assuming that they are covered – see below).

42. In relation to enforcement against persons overseas, this would require co-operation with the authorities from the country concerned. This has occurred with other Cayman Islands legislation however.

Who should be covered?

43. The sender of spam is not the only person who can be a party to the act of spamming. Often a vendor of goods or services will sponsor someone else to do the spamming for them. Australia has applied its legislation to not only the sender of the message but also those who cause the message to be sent, those who aid, abet, counsel or procure a contravention of the requirements and those who are in any way a party to such a contravention.

4. *What message mediums should be caught by the legislation (e.g. email, short message services using mobile phones, Internet instant messaging, faxes, telephones (telemarketing))?*
5. *Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?*
6. *Should the messages caught by the legislation be of a commercial advertising and promotional nature only or should other types of messages be caught? Should there be exceptions and if so what should be exempted?*
7. *Should the legislation extend to coverage of acts done overseas? If so, what acts should be covered?*
8. *Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation? Should there be express exceptions such as for telecommunications companies and ISPs?*

The Consent Issue – Opt-in or Opt-out

44. One of the main characteristics of spam is that it is unsolicited and/or unwanted. To address this issue legislators have either provided that electronic commercial messages can only be transmitted if the recipient has expressly or implicitly consented to such transmission (opt-in), or that such messages cannot be transmitted if the recipient has already taken action to indicate to the sender that such messages are unwanted (opt-out).

Opt-in

45. The opt-in approach has been the approach favoured by those opposing spam and by the majority of legislators (e.g. EU, Australia). Some anti-spam groups favour a double opt-in approach whereby the recipient must respond in 2 different ways to indicate consent. The merit of the opt-in approach is that it places the onus on those wishing to send messages and is thereby more effective in addressing the spam problem. In addition many recipients of spam are reticent to respond with a message to not send any more messages as this can represent a confirmation of an address that leads to more spam.

46. Issues that arise with the opt-in approach are:

- What conduct/relationships should amount to or be deemed to constitute implicit consent?
- What is the scope of any opt-in assent?

47. The Australian legislation defines "consent" as meaning "express consent or consent that can reasonably be inferred from the conduct and the business and other relationships of the individual or organisation concerned". This definition does seem to create an area of uncertainty as to what conduct and relationships would result in there being a reasonable inference of consent.

48. The fact that 2 individuals know one another and have exchanged business cards including their email addresses may, of itself, not be enough to constitute inferred consent to the sending of an email about a "commercial" matter. The question is, is this too restrictive an approach or should the issue be dealt with by defining spam as being the sending of bulk messages, or the sending of messages by someone where the email address of the recipient was not given personally to the sender by the recipient or published?

49. The Australian legislation provides that consent can be inferred from the fact that an email address has been published. Many would consider this to be unreasonable. There are circumstances where procedures require the publication of an email address (e.g. registration of a domain name subsequently published by WHOIS) or where such publication is essential to enable accessibility by the general public (e.g Government officials and departments, customer service departments). It is difficult to see why such individuals should be exempted from the protection of anti-spam legislation.

50. A further issue arises concerning the scope of any opt-in assent. If someone does respond to an email by opting in, the question arises of what this should authorise the sender to do. Should this mean that the sender can only send promotional material relating to the subject matter of the email responded to or should the sender be able to send messages relating to different subjects? Should the sender be entitled to pass your email on to other organisations? The approach of the Australian legislation seems to relate the issue of the scope of any 'consent' to whether a particular message was expressly consented to or consent could reasonably be inferred.

Opt-out

51. The opt-out approach has been supported by some direct marketing organisations on the basis that the Internet is a legitimate and efficient way of advertising and promoting goods and services to customers or prospective customers and that its members will respect any response by an individual indicating that they no longer wish to receive such email. The opt-out approach has been adopted by the United States in its CAN-SPAM Act of 2003.

52. The problems with the opt-out approach are:

- It legitimises anyone sending emails to an individual's mailbox without any assent at all;
- There is a very valid concern that if an individual responds to a message with an opt out response that they will confirm their address and end up receiving more spam;
- It is seen as legitimising the sharing of email address lists by businesses with one another.

53. The above problems with the opt-out approach are seen by anti-spam groups as helping to make the spam problem worse rather than minimising it.

54. Based on the issues and arguments described above, the Authority's current preference is towards an opt-in approach. However the Authority is requesting feedback from interested groups on their views on this matter.

9. Should the Cayman Islands adopt an opt-in, double opt-in or opt-out approach in legislating against spam? Why?

10. If an opt-in or double opt-in approach were to be adopted, what should amount to express consent and what actions and/or relationships should amount to inferred consent to the sending of a "commercial" electronic message?

11. How should the scope of any opt-in or double opt-in assent be framed?

Transparency Issues

55. Some of the transparency concerns that arise around spam are that the sender is not able to be identified by the recipient from the message, the message does not contain a functional unsubscribe facility, the header /subject information is misleading or inaccurate and there is no clear labelling that the message is of an advertising or adult nature. The lack of transparency associated with spam appears to be designed to avoid identification and detection and avoid anti-spam filter mechanisms.

56. The Australian legislation has specifically addressed the first two of these concerns by providing that a person must not send a commercial electronic message unless the message:

- clearly and accurately identifies the individual or organisation who authorised the sending of the message; and
- includes a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual or organisation who authorised the sending of the message, and such electronic address is functional.

57. The United States legislation also addresses the concern over misleading or inaccurate header and subject information by providing that it is unlawful for a person to transmit commercial electronic mail messages with materially false header information and with a subject heading that is misleading as to the content of the message.

58. Another way of requiring transparency and to assist in the filtering of spam is to require messages of an advertising or adult nature to include a label such as ADVT (for advertising) and ADLT (for adult).

59. Requiring transparency for commercial electronic messages would seem to have merit as such transparency would assist in minimising the spam problem.

12. Should there be a requirement for commercial electronic messages to accurately identify the sender of the message? If so, what constitutes accurate identification (e.g. name and physical address, name and email address)?

13. Should there be a requirement for commercial electronic messages to include a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the sender, to ensure that such electronic address is functional, and that the sender acts on the unsubscribe instruction?

14. Should there be a requirement that commercial electronic messages provide accurate header and subject information?

15. Should there be a requirement for the labelling of advertising or adult messages?

Privacy Issues - Address Harvesting

60. Address harvesting is the use of computer software to search the Internet for email addresses and then collect and compile those addresses. Spammers use address harvesting to obtain a list of addresses to send messages to. It does raise issues relating to privacy as in many cases the addresses obtained are from sources on the Internet where there was no intention that the addresses be available for any form of public use, such as chat rooms.

61. The Australian legislation sets out rules against the supply, acquisition and use of address-harvesting software and harvested-address lists in connection with the unlawful sending of electronic messages. The Australian legislation adopts this approach in order to ensure a comprehensive code against all aspects of a spammer's activities.

62. The advantage of specific rules against address harvesting connected with spam activities is that it gives greater tools for enforcement against the actions of spammers and therefore assists to minimise the spam problem.

63. There are some problems involved in seeking to legislate against address harvesting. Address harvesting can be used for legitimate purposes and it can be difficult to determine whether the purpose of address harvesting software is legitimate or not. In addition, if the addresses being harvested are publicly made available on the Internet there is an argument that the sending of unsolicited email messages to those addresses is legitimate as any privacy rights have been forgone.

64. There is also the argument that the key problem with spam is the actual sending of spam messages rather than the collection of email addresses which, by itself, does not cause any harm.

> *16. Should anti-spam legislation include rules against the supply, acquisition and use of address-harvesting software and harvested address lists in connection with the unlawful sending of electronic messages?*

Enforcement Issues

65. The enforcement issues that arise around any anti-spam legislation concern who may bring an action, whether there should be criminal or civil penalties imposed, what should be the nature of those penalties and what types of remedies should be available.

Who may bring an action?

66. The general approach to enforcement of anti-spam legislation has been to give a particular government agency primary responsibility for carrying out investigations and taking enforcement action. In Australia that agency is the Australian Communications Authority (ACA) and in the United States it is the Federal Trade Commission (FTC).

67. The approach of the Australian legislation is to give the ACA the right to bring actions for breach of civil penalty provisions and seek injunctions and undertakings while giving victims the right to join any action by the ACA to seek compensation. The approach of the United States legislation is to give the FTC the right to bring both criminal and civil actions while also giving rights to bring particular types of actions to State authorities and to the providers of Internet access services.

68. For individuals or firms that are the recipients and victims of spam, the resources necessary to carry out an investigation and bring court action are generally beyond them, hence the approach of other jurisdictions to assign primary

responsibility for this to a government agency. In the Cayman Islands, the agency best placed to take on this role is probably the ICT Authority. Other possibilities are the Police and the Ministry of Communications, Works and Infrastructure.

69. The approach of the United States in giving rights of action to Internet Service Providers would seem to have merit as they can be affected by spam activities in a major way and are more likely to have the resources to take an action. In the United States, for example, four Internet Service Providers have recently taken action under the CAN-SPAM Act against six Internet marketers. There would also seem to be merit in giving victims the right to join actions for the purpose of seeking compensation.

Penalties and other remedies

70. Given the costs that spam can impose and the difficulties involved in carrying out a successful court action, the penalties able to be imposed under anti-spam legislation should be sufficient to be able to serve as a deterrent.

71. The penalty options include the imposition of a civil pecuniary penalty (e.g. Australia) and the imposition of a fine or a term of imprisonment (United States).

72. In terms of the amount of any penalty or fine, the Information and Communications Technology Authority Law is one possible guide. Under that Law, operating an ICT network or service without a licence can result in a maximum fine of $50,000 (and imprisonment for 5 years), and if the offence is a continuing one to a further fine of $10,000 for every day or part of a day that the offence is continued. The maximum penalties under the Australian Spam Act are quite substantial, being AU$220,000 (CI$144,500) for a single day's contraventions and AU$1.1m (CI$722,250) for further breaches.

73. A further issue is whether the penalty should be in the form of a civil pecuniary penalty or in the form of a fine and/or imprisonment as part of an offence provision. One of the differences between taking the civil penalty approach and the criminal offence approach is that concerning the required standard of proof. For civil proceedings the standard is on the balance of probabilities while for criminal proceedings it is beyond reasonable doubt, which is a stricter standard.

74. Other possible remedies include the ability to seek injunctions against the actions of spammers as well as the ability of victims to seek compensation or damages and the ability to seek exemplary damages.

Powers of investigation

75. Another issue is what powers should be given to the investigating authority. Under the Information and Communications Technology Authority Law, for example, the ICT Authority is given the ability to obtain search warrants to investigate possible contraventions of that Law. These search warrants confer powers of entry, search, and seizure of evidence in the form of documents and

goods. If enforcement is to be effective it would seem that there is merit in the investigating authority having the ability to obtain search warrants.

17. *Who should be able to bring an action against an alleged spammer?*
18. *What agency should have the enforcement role under the legislation?*
19. *What should be the available penalties and remedies for breaches of anti-spam legislation and what should be the maximum fine or pecuniary penalty?*
20. *Should contraventions give rise to criminal or civil penalties?*
21. *Should the responsible enforcement agency be given the ability to obtain search warrants conferring powers of entry, search and seizure?*

PROCEDURE

76. In order to be considered, comments must be in writing and must be submitted to the Authority by 18 August 2006.

77. The Authority may address interrogatories to persons that file comments. A further round of comments from participating persons concerning interrogatory responses may be invited, should circumstances so require.

78. All submissions should be filed with the Authority at **one** of the addresses provided below.

By post:

Information and Communications Technology Authority
P.O. Box 2502 GT
Grand Cayman
Cayman Islands

Or by courier:

Information and Communications Technology Authority
3rd Floor, Alissta Towers
North Sound Way
Grand Cayman
Cayman Islands

Or by e-mail:

consultations@icta.ky

Or by fax:

(345) 945-8284