CB(1)2253/05-06(04)

Discussion on the Unsolicited Electronic Messages Bill

Prepared by the Hong Kong Computer Society

1 Introduction

Hong Kong Computer Society (HKCS) has been taking an active interest in the growing problem of UEMs, and this document is the latest in a series of papers and events by HKCS on the topic[1,2,3,4,5,6,7,8,9,10,11]. The issues and points raised in the

[1] "Response to the UEM Proposals", http://www.hkcs.org.hk/en_hk/misc/ISSD_ResponseUEM200602_final.pdf

[2] "Anti-Spam Recommendations", http://www.hkcs.org.hk/en_hk/doc_general/as-recommend-final.pdf

[3] "Anti-Spam Conference", 10 March 2006, http://www.hkcs.org.hk/whatsnew/20060304/20060304w.htm

[4] "Anti-spam Forum 2006 - How to Regulate?", 24 March 2006, http://www.hkcs.org.hk/whatsnew/20060311/20060311w.htm, http://www.hkcs.org.hk/whatsnew/20060429/Rundown.pdf

[5] "Key Challenges in Combating Spam. How Government and Industry Experts Can Help Lower Email Security Risk", 21 October 2005, http://www.hkcs.org.hk/whatsnew/Symantec_211005.doc

[6] "Spam is a Human Prolem", http://www.hkcs.org.hk/en_hk/doc_newsletter/doc_general/HKCS1st05(5)(OP2)EM.pdf

[7] "Telecoms InfoTechnology Forum: e-Security in the Broadband Age" http://www.hkcs.org.hk/whatsnew/20060304/TIF_March2006_010306.doc

[8] "Anti-Spam Forum – to REGULATE or NOT", 13 January 2004, http://www.hkcs.org.hk/en_hk/misc/events.asp?year=2004

[9] "Response to the OFTA Consultation Paper, "Proposals to Contain the Problem of Unsolicited Electronic Messages"", http://www.hkcs.org.hk/doc_journal/antispamresp.pdf

[10] "Gone Phishing – ISSG Seminar", http://www.hkcs.org.hk/en_hk/doc_newsletter/doc_general/HKCS5_6em2.pdf

[11] "Anti-Spam Seminar in Hong Kong Productivity Council", 14 June 2006, http://www.hkcs.org.hk/whatsnew/20060603/Anti_SpamSeminar.pdf

previous documents are still valid and this document specifically discusses the Unsolicited Electronic Messages Bill (the Bill), recently brought before the Legislative Council (LegCo).

Hong Kong urgently needs Good Legislation to control UEMs, we hope that the Bill can be improved sufficiently to become Good Legislation.

Some of the discussion provided throughout this paper relates to good general principles. A large amount of the discussion contained within this paper pertains to the actual detailed wording of the draft Bill and its potential technical implications.

HKCS is a society of Information Technology Professionals, not lawyers, and this may have led to some misunderstandings of the legal terms currently contained within the draft Bill.

The Bill, as currently drafted, appears to have been assembled by lawyers who have not fully appreciated and taken into consideration the various technical implications that could negatively arise should this bill be adopted into legislation. To be successful, the Bill must unite both the legal and technical spheres.

The HKCS would like to encourage the detailed discussion included within this response to be considered in light of bridging the gap between the legal and technical spheres, which would ultimately lead to a positive improvement in the adopted legislation.

2 General Comments

2.1 Experience of Criminal Investigations

The Bill places investigation and enforcement under the Telecommunications Authority, but the offences defined are a mixture of civil and criminal. Also, the nature of the problem is directly related to the number of incidents. This raises some important questions:

(1) Will the Authority have sufficient resources to be capable of handling an excessively large number of incidents and cases which are currently occurring on a daily basis?

(2) Does the Authority have sufficient investigative and technical level experience to investigate cases in the context that may readily change from being civil to criminal, particularly with regard to the requirement to acquire a large amount high technology related forensic evidence?

2.2 International Cooperation

UEMs are a global problem, and effective control will require an International approach. A good definition of the "Hong Kong link" is one aspect of this. Another aspect is obtained through the close collaboration achieved between different governments. Unfortunately the draft Bill only appears to have considered this critical element in one short sub–subsection: Section 34.(5)(b)(iii). To the best of the knowledge of the HKCS, Australia is currently the only country to have laws providing for this sort of cooperation.

The HKCS feels that reliance on Section 34.(5)(b)(iii) only may be insufficient to allow full reciprocal cooperation with, in this case, the Australian authorities, and any other countries that elect to introduce similar legislation.

3 Technical Issues

3.1 Section 2, Interpretation

3.1.1 "electronic address"

The definition of "electronic address" includes Internet protocol (IP) address. The implication of this is far-reaching: all traffic on the Internet is therefore an "electronic message", within the terms of the Bill.

Many types of electronic traffic could not be classified as "commercial". For example, "ping" traffic merely tests and reports whether a host is active. One very significant type of electronic traffic that often is deemed to be commercial is Web traffic. The inclusion of "IP address" within the definition of "electronic address" could potentially encapsulate websites under the control of the Bill, which the HKCS believes is not the intent and may not be desirable.

It is currently unclear what effects the inclusion of "IP address" would ultimately have. Individuals do not subscribe and unsubscribe from web pages as they do mailing lists, but perhaps the end of a web page transfer meets the definition of an unsubscribe request, in which case the website administrator would have to, by law, keep a record of all session ends for seven years (Section 8.(3)). This sort of requirement should not be imposed as an unintended consequence of a "too-broad" definition.

3.1.1.1 Internet Use Banned

Another consequence arises from Section 13.(1)(a): here DNS resolvers may be classified as "address-harvesting software", and are therefore banned. When you use the Internet, for example to visit the website of Company X, you type the website address into your browser: http://www.companyx.com, the DNS resolver is the software on your computer that takes that address and finds out the IP address of the website by contacting one or more DNS servers on the Internet: it searches for the IP address of the site on the Internet. This appears to match the definition of "address-harvesting software" in Section 13.(1)(a). Without DNS resolvers, the Internet becomes inaccessible; including "Internet Protocol address" in the definition of "electronic address" will prevent Hong Kong from using or participating in the Internet.

3.1.2 "registered user"

The definition of "registered user" for an electronic mail address is, "the individual or organization who is responsible for the relevant electronic mail address account". Is clarification needed to specify when the registered user is the individual, and when it is the organization? For example, a company might allocate an address to a member of staff, primarily for business purposes, but also allows the staff member to use this address for personal correspondence. Some of the provisions of the Bill are quite different, depending on whether the registered user is an individual or an organisation, as noted below.

This should be very clearly addressed within the Bill to ensure clarity as to when, and in what circumstances, the application of different provisions within the Bill should be applied.

3.2 Section 3: Meaning of "Hong Kong link"

3.2.1 Transit through Hong Kong

The "Hong Kong link" does not appear to address messages that pass through Hong Kong (i.e. in transit). The Bill only appears to address messages that either originate or terminate in Hong Kong.

An example scenario that may arise as a result of allowing “all” messages to transit Hong Kong occurs where email could be sent through an open relay located in Hong Kong. Hong Kong could, as a result, become a haven for open relays. The legislation as currently written may not apply because of the narrow definition of Hong Kong link. As a result it may not be possible to shut down open relays through any legal action. This oversight could be detrimental for Hong Kong. Overseas system administrators could observe that most messages arriving from Hong Kong are spam, and therefore decide to block all messages from Hong Kong. In fact there are already some anti-spam organisations that do exactly this, block “all” messages being sent from Hong Kong.

3.2.2 Registered User

As identified above, the uncertainty over whether a registered user is an individual or organisation is significant. As an example, suppose a HK company allocated an email address to a member of staff who takes a trip out of HK (for business or holiday) and then accesses their email. If the organisation is considered to be the registered user, then there is a HK link, but if the individual is considered to be the registered user, there is no HK link.

3.2.3 .hk Top Level Domain

Section 3.(1)(e) provides that there is a HK link if the recipient’s electronic address was assigned or allocated by “the Authority”. We recommend adding the registrar for the .hk domain, currently, HKDNR: i.e. all .hk domains are regarded has having a HK link. Also, this should be extended to the sender or the receiver.

3.3 Section 5: Meaning of “consent” and related matters

Sections 5.(3) and (4) specifies that anyone can give or withdraw consent on behalf of the registered user. This seems to be an open invitation for abuse, for example, company A has a mailing list of customers, and competing company B sends company A withdraw of consent instructions on behalf of those customers. Company A must, by law, remove those customers from the list, even though they suspect company B was not authorized to send the instructions.

In those circumstances, the obvious response of Company A would be to get someone (e.g. a member of their staff) to give consent for those addresses. However, Section 9.(3)

states that subsequent consent can only be given by the registered user. Does Section 5.(b), “that person shall be treated as having been authorized to send that message on behalf of the registered user” override Section 9.(3)?

This ambiguity should be cleared up. There should be no blanket assumption that a subscribe or unsubscribe message is authorised by the Registered User. There is still the issue of how a sender can determine who the Registered User is, or who has been authorised by the registered user. Suitable methods will depend on the type of message, so perhaps they should be listed in a Schedule or a Guideline issued by the Authority. For example:

- SMS: A message containing the word “unsubscribe” or the Chinese equivalent sent from the recipient’s number to the sender’s number.
- SMTP Email:

    1. A message sent from the recipient’s address to the Reply-to address containing the word “unsubscribe” in the Subject, then the sender may send one message stating that the unsubscribe request has been received, and that the recipient will be unsubscribed if they take no further action; or
    2. A message sent from the postmaster address of the domain of the recipient’s address to the Reply-to address or the postmaster of the sender’s domain requesting unsubscription of the recipient’s address, then the sender may send one message stating that the unsubscribe request has been received, and that the recipient will be unsubscribed if they take no further action;

Explanation: The sender number for an SMS cannot be easily forged (unless the sender is a Telecommunications Service Provider – if a service provider is shown to have misused their power in this way, they should loose their license), so additional confirmation is not needed. Conversely, forging the sender of SMTP email is very easy, so the unsubscribe confirmation message alerts the recipient of the unsubscribe request. The second option allows the administrator of a domain (the “postmaster”) to issue unsubscribe requests for mailboxes that have been deleted (e.g., the member of staff has left the organisation).

Following the procedures laid out in the Schedule or Guideline would be a defence in a court, the validity of any other procedure would be left for the court to decide whether it was reasonable.

3.4 Knowing there is a HK link

Section 7.(2)(b) specifies that the requirement does not apply if the sender did not know there was a Hong Kong link. This appears to be a dangerous and overly broad exemption, consider:

Section 3.(1)(c): There is no way for a sender to determine where the telecommunications device used to access the message is located, so the sender can always claim ignorance, even when a reasonable person would assume the location is in HK.

Section 3.(1)(d)(i): Similarly, a sender cannot determine the location of an individual, in fact, doing so might be in breach of the Personal Data Protection Ordinance (the location of a person is data about a living person). Again, the sender can claim ignorance ("I know all these addresses are registered at a HK ISP, but I thought the individuals might be on holiday outside HK").

The same wording is also used in Sections 8.(2)(b), 9.(4)(b) and 10.(4)(b). Section 10.(4)(b) is particularly interesting: the fact that an address is in a Hong Kong do-not-call list is not taken as an indication of a HK link.

So, with the current wording, it appears that you could have an email address in a .hk domain, and be physically present in Hong Kong, using telecommunications equipment located in Hong Kong, and registered on a Hong Kong do-not-call list, but a sender would still be allowed to send you messages without accurate sender information, and ignore your unsubscribe requests because the sender didn't **know** there was a HK link!

3.5 Part 3: Address Harvesting

The problem of the definition of electronic address and the definition of address–harvesting software in Section 13.(1)(a) has already been mentioned above (3.1.1.1 Internet Use Banned). However, the definition is not very clear in many other ways.

3.5.1 Section 13.(1)(a) No Definition of the Internet

This section says, "searching the Internet or a public telecommunications network", but "the Internet" is not defined. Companies have their own computers connected to, and accessible from, the Internet – are they included in “the Internet” for the purposes of this Bill? If they are, then a company is not free to search the information it has collected on its own machines for its own use. If they are not, then everyone who can access those machines can search them as they like – Part 3 is ineffective.

3.5.2 Section 13.(1)(b) Addresses and Logging

This is another example of the effects of the definition of electronic address including an IP Address. Many servers on the Internet, including web servers and email servers, routinely collect the IP addresses of the machines that contact them, or they contact. They may be useful in diagnosing technical problems, some sites analyse the logs for statistics, and many simply delete them regularly. As they are collected lists of IP addresses, the software that produced them, i.e. mail servers and web servers, may be classified as “address–harvesting software” and therefore fall under the control of Part 3.

3.5.3 Status of Search Engines

There are many search engines available on the Internet that can be used to search for anything, including electronic addresses. For example, searching for “smith@yahoo.com” on the Google search engine returned 32,300 hits, many including addresses like <*name*>.smith@yahoo.com. So, using common surnames can reveal many full email addresses. Are these search engines “address–harvesting software”?

Section 13.(1) includes the phrase, “specifically designed or marketed for”, so perhaps the search engines are not “address harvesting software” because they are not **specifically** designed for this purpose. But, in that case, the definition can be undermined by using a different design objective, for example, “this software searches the Internet for strings of non-space characters with one ‘@’ character”.

Section 14.(4) does allow a defence of not knowing and having no reason to suspect that the customer intended to use the results for spamming, but the major search engines have every reason to suspect that some of their users are misusing their services.

The search engines are an important component in what makes the Internet so useful: they enable ordinary people to easily find the information they need. This service can be misused, but do we ban highways because they make it easy for bank robbers to make a fast getaway?

3.5.4 Specialist Software Users

Other activities may be caught in the rather vague definition of “address–harvesting software”, leading to confusion and uncertainty among technical staff. This would have a detrimental effect if the law is not clearly–worded enough for technical staff to understand what is, and is not, allowed – they may be reluctant, or refuse to perform tasks that were not intended to be covered, because the definitions are imprecise. Examples may include:

- Administration: mail system administrators routinely collect and process addresses by various automated means.
- Security testing: Penetration test methodologies (professionals simulating what attackers may do with the purpose of identifying and highlighting security vulnerabilities) often involve the gathering of data, including addresses, as a preparatory stage to the simulated attack(s). Address–harvesting software and “automated means” (in the sense defined in Section 17.(6)) are often used in this context. If the intent (or part of the intent) of the test is to determine how vulnerable an organisation is to having their addresses harvested for spamming, then it could be argued the use is “in connection with … the sending of commercial electronic messages…” as specified in Section 15.(1).

3.5.5 Section 16: Harvesting and Consent

Section 16.(1) has in exception, “without the consent of the registered users”. Giving consent on behalf of a registered user has already been discussed above (3.3 Section 5: Meaning of “consent” and related matters).

Also consider that a common way of processing subscriptions to mailing lists is a web-based form: people visit the form and subscribe to the mailing list by entering their address and clicking “submit”. The software that processes the form input is “address–harvesting software” as defined in Section 13.(1)(b).

Conversely, Section 16.(1) is limited to “commercial electronic messages”, but a message that merely asks, “Can I add you to our mailing list?” has no commercial content. Therefore, potentially a spammer could harvest an unlimited number of addresses, and send them endless subscription invitations without committing a crime. The subscription invitation could also be misleading (“our book–readers mailing list” when the list is used to send any type of spam), and there would still be no offence. If a recipient subscribes and then unsubscribes, the spammer can resume sending the non–commercial subscription invitations.

3.5.6 Proof of Harvesting or “Automated Means”

A major difficulty with limiting the legislation to lists collected or compiled by address–harvesting or automated means is that, once the list has been created, there is nothing to show how it was created. If a list is sold, what reasonable means can the purchaser use to test whether the list was originally created in an allowed manner?

This is a problem that does not affect an “opt-in” regime – a buyer can contact a random sample of addresses and enquire whether they provided their informed consent.

3.6 Carte Blanche for Telecommunications Service Providers

Section 18.(4)(b) appears to allow telecommunications service providers unlimited opportunity to send unsolicited commercial messages about their services.

3.7 Section 19: Retransmission and Deception

Section 19 appears intended to prevent spammers obfuscating the source by relaying or retransmitting the message. However, there are potential problems:

3.7.1 Hong Kong Link

As mentioned above (3.2.1 Transit through Hong Kong), the limited definition of Hong Kong link may make Hong Kong a safe transit haven for spammers elsewhere.

This has a potential severe detrimental effect on Hong Kong: recipient organisations may be inclined to block all messages arriving from or via Hong Kong, and legitimate business communications may be disrupted as a result.

3.7.2 Section 19.(1): Deception

Section 19.(1) specifies there must be, “intent to deceive or mislead recipients”, this may leave a large loophole:

1. A relay can be used to multiply the sender’s effort: the message is transmitted to the relay once, with a long list of addresses. The relay then does the work of transmitting the message to each address. Thus, the sender takes advantage of the

relay’s bandwidth. A spammer could argue that there was no intent to deceive, only intent to use bandwidth.

2. Many recipients use automated filters to remove spam. A spammer could argue that their intent was not to deceive the recipient (they might even have clear and accurate sender information in the message body), but to bypass the filters. This would not be forbidden by Section 19.(1) because, firstly, an automated filter does not have a mind and thus cannot be deceived, and secondly, the automated filter is not the recipient.

This also applies to Section 22.

3.8 Section 28: Convoluted Subsection

The meaning and intent of Section 28.(5) is unclear.

3.9 Sections 30, 31: Do–not–call Registers

The management and maintenance of do–not–call lists is potentially a difficult and complex task. The biggest risk is that the lists may be used for spamming because they are known–good addresses. The administration involved with making sure that requests for addition and deletion are properly authenticated and processed in a timely manner is considerable. However, do–not–call lists are essential for the success of an opt–out regime: they are the only mechanism that lightens the burden imposed on the recipient for unsubscribing from an endless number of lists they never subscribed to. The alternative approach, opt–in, makes all the problems of these registers disappear: essentially, every address is automatically on a do–not–call register, so there is no administration, no authentication issues, and no threat of disclosure.

However, the Bill establishes an opt–out regime, so the issue of whether the provisions for do–not–call lists are suitable must be addressed. The issues mainly concern whether the Authority will have the flexibility to define procedures that will make do–not–call registers effective.

3.9.1 Section 30.(6) Consent for Listing

Section 30.(6) specifies that there must be consent from the registered user before an electronic address is listed in a do–not–call register. This could be interpreted to prevent the Authority allowing the addition of domains or “canaries” to a register:

3.9.1.1 Domains

If an organisation, which has registered its own domain name, determines that it does not want any of its email users to receive UEMs, it could be allowed to add its domain to the do–not–call list. This could be very useful for Companies that want to use email for their own business purposes, and it would relieve the staff or system administrators from the burden of adding new addresses to the register when staff change. However, the narrow definition of Section 30.(6) might not allow this – is the organisation the registered user of the domain, or are the individual staff registered users of their individual addresses?

3.9.1.2 “Canaries”

“Canaries” are fake data values inserted into the register for the purpose of revealing misuse – if a message arrives at the fake address it is clear evidence that the sender has misused the register. This could be implemented in conjunction with domain registrations – the Authority could add invented addresses in the listed domains, or in collaboration with HKDNR, by establishing “fake” domains with “fake” addresses in them. However, Section 30.(6) prevents such canaries being added, because there is no registered user to give consent.

3.9.2 Section 31: Access to Registers

Section 31.(1) specifies that the register, “or the information contained in it” be made available, the following subsection says that may be in a form and manner, “as the Authority considers appropriate”. This might be unnecessarily broad: the register contains addresses, the information contained in it is the addresses, but the information that a sender of UEMs requires is not the addresses themselves, just whether the addresses on the sender’s list are in the register. It is unclear whether this would allow these methods of preventing misuse of the register:

3.9.2.1 Hashing the Register

Instead of publishing the list of addresses, a list of cryptographic hashes of the addresses is published. The UEM sender can check whether an address is in the register by calculating the cryptographic hash and checking against the list of hashes.

3.9.2.2 Lookup–Only Access

The Authority could make the list only available for lookup: essentially, the UEM sender asks the Authority whether an address is listed, and the Authority replies. This can be done in an efficient and scalable way by using DNS, in the same way that DNS black– and whitelists are published today.

However, a lookup-only register can still be misused. Spammers would prefer to get their messages to real, active addresses – there is no chance of a profitable response if the message is not received because the recipient no longer or never existed. An access do–not–call register is therefore an opportunity for spammers to improve the quality of addresses on their lists: they can take an automatically generated list of address, or an old list with many obsolete addresses, and use the lookup-only register to select the ones that are in use.

This could be countered by using a lookup-only register in combination with the canary and domain registrations described above: the Authority would reply “listed” for every address queried when a domain is registered, and “listed” for only a few addresses in their “fake” domains. The spammer trying to clean-up their address list will then not know whether a “listed” response is for an address that is real and active, or it is a non-existent address in a real domain, or a fake address in a fake domain.

3.9.3 Section 32.(2) Misuse of a Register

The registered user of an address is not permitted to check the do–not–call register to verify whether or not their address is registered!

There may be other circumstances when the narrow definition of Section 30.(2)(b) prevents a harmless and possibly useful reason for checking the register – for example, technical staff investigating why a message was not received.

3.10 Section 32.(1): Misuse of Information

Under Section 32.(1), the information in an unsubscribe message must only be used for the purpose of complying with Section 9. Under the scenario described above (3.3 Section 5: Meaning of “consent” and related matters), if Company B has sent an unsubscribe message without the registered user’s consent to Company A, and Company A investigates the message and discovers that it was not sent from the registered user, they have broken Section 32.(1).

Potentially, not only can your competitor unsubscribe all your customers from your lists without their knowledge or consent, if you try to check whether they have done it, you get sent to jail!

3.11 Section 34: Obtaining Information

3.11.1 Section 34.(1) Revealing Passwords

As information security professionals, we emphasise to users that they must never, ever tell anyone their passwords.

3.11.2 Section 34.(4) No Obligation of Retention of Information

A person may avoid their responsibility to provide information under Section 34.(1) by simply scheduling frequent automatic deletion of the information (e.g., deletion of log files).

3.12 Section 52: Civil Claims

The loss or damage caused by one UEM is quite small, perhaps of the order of a few dollars or less, trivial even for the Small Claims Tribunal. It is the overall number of such messages that make them a serious nuisance. Will there be provision for the aggregation of claims across:

1. Multiple messages from one sender to one address
2. Multiple messages from one sender to multiple addresses of one registered user
3. Multiple messages from one sender to multiple addresses of one organisation
4. Multiple messages from one sender to any group of addresses

4 Comments on CTB(CR) 7/5/18(06)

LEGISLATIVE COUNCIL BRIEF UNSOLICITED ELECTRONIC MESSAGES BILL

4.1 Problems Caused by UEMs

The situation is worse than indicated. In addition to the problems listed in the Brief. UEMs also cause:

4.1.1 Communication Breakdowns

Users, administrators and service providers try to minimise the impact of UEMs by filtering, but automated filtering sometimes mis-classifies genuine messages as UEMs. This can cause loss of business, and/or increased technical support time as the problems are investigated and worked around.

In the worst cases, there might be no indication to the sender that their message has been blocked, so corrective measures are not taken, and opportunities are lost. Some service providers block messages from entire countries on the basis they are a common source for UEMs. The costs of these problems to Hong Kong businesses are unmeasurable.

4.1.2 Automated Systems

We normally think of messages being received by a living person, but this is not necessarily the case. There are examples of systems that receive messages by SMS or by email, and then take predetermined actions, based on the messages. These systems may behave in unexpected ways: failing to work, or taking spurious actions, if they receive unanticipated input.

4.2 Balance Between Allowing e-Marketing and Respecting the Right of Recipients

The brief talks about, “allowing electronic marketing to develop in Hong Kong as a legitimate promotion channel”, but does not clarify the scope of electronic marketing.

Restricting the usage of messaging would not affect other electronic marketing channels, such as websites. A company website is their “electronic shop window”, and banner adverts on other sites can increase a company’s exposure.

Messaging, conversely, is about sending a message to an address. The recipient has paid to establish the address, and has paid for the communications service. Shouldn’t the recipient have the right to decide how the address is used?

The Brief asserts, “In sum, business interests, including small and medium enterprises (SMEs), preferred more room and flexibility for e-commerce and e-marketing development.” This summary neglects the preferences of business interests, including SMEs, many of them long-time users of the Internet, that have seen UEMs grow to the extent of destroying the utility of electronic messaging. While UEMs may still be effective at finding the one potential sales contact in a million, or ten million, addresses, the cost is that important messages about ongoing business relationships are being lost or delayed because of the flood of UEMs. The “right balance” presented in the Brief is not the right balance for enabling business communications through electronic messaging.

4.3 Coverage of UEMs

4.3.1 Hong Kong Link

The Bill should cover UEMs sent through Hong Kong, in addition to sent from and sent to described in the Brief.

4.3.2 Commercial Nature

The Brief advises a targeted approach, “the content of the message is about offering or promoting goods or services for furtherance of business.”, but this is unnecessary, and sometimes dangerous. The correct criterion is whether the message is **solicited.**

4.3.2.1 Government

When the Government needs to send a message to the whole population, it already has adequate means for broadcasting: TV, radio, posters in public buildings etc. Government departments also have numerous *ad hoc* address lists, but these are not unsolicited: the recipients have requested to be added to the lists, to receive library book request notifications, or notifications about Strategic Commodities Control System changes, or whatever.

Furthermore, the Bill also has provisions about list management: the recipient has the right to stop receiving messages. The Government should not be absolved of responsibility for managing its lists properly.

4.3.2.2 Charitable Organisations

In general, charities are not sending unsolicited requests for donations. What has happened is fraudsters sending fake donation requests: for Asian Tsunami victims and Hurricane Katrina victims. We can help to reduce the success rate of this type of fraud by not exempting charities from the Bill: there will be a gap between the expected behaviour of a real charity, and the fraudulent messages that the recipient can recognise, "a real charity would not send this, so it must be fake".

Again, there should be no exemption from the requirement to manage address lists properly.

4.3.2.3 Bills and Invoices

Normally, bills and invoices are not unsolicited, so there would be no problem if the Bill used "solicited" as the criterion. Exempting bills and invoices does leave a potential loophole: the sender could copy a real invoice for one of their customers to an unlimited number of other recipients. Of course, the invoice would itemise some of the sender's interesting products or services, with pricing. The fact that the invoice has been sent to unrelated addresses does not change its nature as an invoice. If there were no exemption, then the invoice would be solicited for the correct recipient, and unsolicited for all the others.

4.4 Opt–out Regime

As noted elsewhere, we consider the opt–out regime to be ineffective, and an opt–in regime should be adopted. Furthermore, the creation, management, maintenance and protection of do–not–call registers are expenses that are unnecessary if an opt–in regime is adopted.

4.5 Enforcement and Penalties

The Brief indicates that the Telecommunications Authority (TA) would enforce some of the rules, it does not specify who would enforce the address harvesting and related rules, fraud related activities would be enforced by the Police, and victims could make civil claims.

The major problem caused by UEMs is wasting time, but the mixture of different authorities and procedures could exacerbate the problem. Serious consideration should be given to streamlined, efficient processing of reports. The objectives should be:

- Recipient convenience. The recipient is the victim, they should not be required to correctly identify which one among many departments to contact before making a report.
- Collection of evidence. A simple UEM report may lead to a fraud investigation, the reporting should preserve the necessary forensic evidence.
- Automation. If the Bill is successful, there will be a massive number of reports to be processed. Correlating separate reports into one case will allow efficient use of investigative resources, and maximise the chance of successful prosecution.
- Feedback. When appropriate, the recipient could be provided with information necessary for a civil claims case. In other cases, the option to receive a notification, “thank you, your report was used as evidence in this prosecution” would encourage involvement in the continuing effort against UEMs.

OFTA and the Police will need to cooperate closely to enforce the Bill, how will this be achieved?

4.6 Implications of the Proposal

The Brief asserts, “most responsible electronic marketers should be able to comply with them at acceptable extra costs”. It would be more accurate to say that responsible electronic marketers **are already** in compliance; therefore there are no extra costs for responsible electronic marketers.