Electronic Frontiers Australia Inc

PO Box 382 North Adelaide
SA 5006 AUSTRALIA
www.efa.org.au
email@efa.org.au
Tel: 07 3424 0201
Fax: 07 3424 0241

20 October 2003

The Secretary
Senate Environment, Communications, Information
Technology and the Arts Legislation Committee
Parliament House
CANBERRA ACT 2600

Email: ecita.sen@aph.gov.au

Dear Sir

Inquiry on the Spam Bill 2003 and Spam (Consequential Amendments) Bill 2003

Please find attached submission from Electronic Frontiers Australia Inc. to the Committee's inquiry.

EFA appreciates the opportunity to make a submission and would be pleased to present oral testimony and respond to any questions Committee members may have.

Yours faithfully

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)

Submission to Senate Environment, Communications, Information Technology and the Arts Legislation Committee

Inquiry on the Spam Bill 2003 and Spam (Consequential Amendments) Bill 2003

20 October 2003

Contents:

Executive Summary

- EFA supports the general intent of the *Spam Bill 2003* insofar as it is intended to reduce the quantity of unsolicited bulk commercial electronic messages.
- However, we are concerned that although the proposed legislation does prohibit the sending of some types of spam, it also:
    - ♦ prohibits the sending of single messages that are not generally regarded as spam; and
    - ♦ establishes special classes of senders who are authorised to send spam "relating to goods and services" and exempts those senders from the requirement to provide a functional unsubscribe facility; and
    - ♦ specifically legitimises and authorises the sending of other spam that has a commercial aspect.
- The legislation should be applicable to the sending of all unsolicited commercial electronic messages in bulk. It should not create categories of approved "designated" spam.
- The legislation should not treat a single message sent to one specific individual as spam merely because the message has a commercial aspect.
- The entry, search and seizure powers enable ACA appointed inspectors (government employees) and police to enter homes and search and seize an individual's computer/email and other possessions without a search warrant and without the consent of the relevant individual. A judicial warrant must be required.

- The entry, search and seizure powers enable entry and search/seizures (with and without a warrant) in relation to the premises and possessions of a *recipient* of spam. Searches of *recipients'* premises or possessions must not be permitted (unless they are suspected on reasonable grounds of having breached the *Spam Act 2003)*.
- The assistance order provision enabling a suspect or other person to be imprisoned for forgetting or losing a password, encryption key, or other information is completely absurd in legislation that does not involve imprisonment even if a person is found guilty. The assistance order provisions must be deleted.
- The exemptions for Australian (and overseas) government bodies, political parties, religious organisations, charities and charitable institutions and educational institutions must be deleted. The sole purpose of these exemptions is to authorise such bodies to send *unsolicited commercial* messages "relating to goods and services". If such bodies wish to promote or advertise their goods and services by electronic messages, they should be required to obtain the recipient's prior consent.
- The exemption for unsolicited bulk messages that contain "factual information" and also have commercial aspect is large enough to drive a truck through. It should be deleted. It is inappropriate that legislation, in effect, compel individuals to receive and pay for unsolicited information sent to their email address (whether the government thinks it is "beneficial" information or not).
- If the exemptions for senders of legislatively authorised "designated" spam are not deleted, these senders must not be exempt from the requirement to provide a functional unsubscribe facility.
- The provision concerning inferred consent to receive spam by "conspicuous publication" of an electronic address presents serious problems for, at the least, self−employed persons and small business owners. The inference from conspicuous publication should be reversed.
- The supply, acquisition and use of address−harvesting software and harvested address lists should also be prohibited in relation to the purpose of sending "designated" spam (if the designated spam provisions are not deleted) and all other unsolicited electronic messages, not only the narrow category of messages referred to in Section 16(1).
- The prohibitions on supply, acquisition and use of address−harvesting software and harvested address lists should apply to government bodies (which are currently exempted from these prohibitions).
- The protection from civil proceedings provision for ISPs and other electronic message service providers must be changed so that it applies only to anti−spam filtering services provided with the prior consent of the customer, that is, where a customer has voluntarily opted in to having their electronic messages spam−filtered by their ISP or other provider.
- The possible benefit of the currently proposed law in minimising receipt of spam is outweighed by its potential to result in unnecessary invasions of the privacy of innocent individual's homes and possessions and/or their imprisonment, prohibit ordinary electronic messages and its authorisation of "designated" spam.
- The proposed legislation should not be enacted without amendments to resolve the issues and problems raised above.

▲ Go to Contents List

About EFA

Electronic Frontiers Australia Inc. ("EFA") is a non−profit national organisation representing Internet users concerned with on−line rights and freedoms. EFA was established in 1994, is independent of government and commerce, and is funded by membership subscriptions and

donations from individuals and organisations with an altruistic interest in promoting online civil liberties.

Our major objectives are to protect and promote the civil liberties of users of computer based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA has long been an advocate for the privacy rights of users of the Internet and other computer based communication systems. We believe that users have a fundamental right to be left alone and to have control over how personal information about them is collected, used and disclosed. EFA believes legislation designed to minimise spam is desirable because spammers give no regard to individuals' privacy rights and preferences.

▲ Go to Contents List

Introduction

EFA supports the general intent of the *Spam Bill 2003* insofar as it is intended to reduce the quantity of unsolicited bulk commercial electronic messages.

However, we are concerned that the Bill will prohibit single messages that are not generally regarded as spam. We are also concerned that exemptions for "designated" spam and "conspicuous publication" of work−related addresses may result in the law being as effective in increasing spam as in reducing it.

EFA is strongly opposed to following provisions of the *Spam (Consequential Amendments) Bill 2003*:

- the search and seizure provisions that empower government employees and police to search and seize an individual's computer and other possessions *without* a search warrant and *without* the consent of the relevant individual; and
- the search and seizure powers (both with and without a warrant) that are applicable to the premises and possessions of a *recipient* of spam who is not suspected of having breached the *Spam Act 2003*; and
- the assistance order provisions that enable a suspect or other person who has forgotten or lost a password, encryption key or other information to be imprisoned for six months, although even a person found guilty of breach of the *Spam Act 2003* is not subject to imprisonment.

We are under the impression that there has been no prior public consultation on the search and seizure, and assistance order, provisions. These matters were not mentioned during an August meeting in which NOIE briefed EFA on a then draft Bill, nor in the summary document provided by NOIE. The provisions appear to have been developed not by NOIE, but by a governmental division that has little understanding and knowledge concerning information technology issues.

We note that some proponents of the Bills consider the proposed laws should be enacted poste haste on the basis that known flaws and definitional issues can be fixed in the future via case law and regulations. EFA considers such an approach to law−making is wrong. The result of such an approach is that individuals who are accused of breaching the law fund the clarification of the law, even when a Court rules that the individual's activity did not breach the law.

We are also aware that some proponents of the Bills regard some issues of concern to EFA as unimportant because they do not believe those provisions would be used or enforced. EFA considers a law enacted on the assumption that it would only be applied selectively is a bad law. Such laws are open to abuse and also bring the law and the Parliament's competence into disrepute. If particular provisions of the proposed law would not be used, they should be deleted from the Bills.

EFA opposes the enactment of the Bills in their current form. The proposed legislation should not be enacted without amendments to resolve the issues and problems raised herein.

▲ Go to Contents List

Search and Seizure Powers

EFA is highly concerned by proposed search and seizure powers set out in the *Spam (Consequential Amendments) Bill 2003* ("SCA Bill") that do not require a warrant.

Inspectors (who are ACA appointed full−time, part−time or temporary Commonwealth or State Government employees and police officers) would be empowered to enter and search homes *without* a warrant and *without* the consent of the relevant occupier of the home, that is, without the consent of the owner of the things (computers, files, documents, etc) to be searched and potentially seized.

These provisions fail to strike an appropriate balance between enforcing the proposed law and the privacy of individuals and families, including the privacy of people who are not suspects.

The SCA Bill proposes to empower inspectors to conduct two types of searches, both of which may be conducted with, and without, a warrant:

1. Searches **relating to breaches** of the *Spam Act 2003* may be conducted either:
    a. **with a search warrant** issued by a magistrate (s.535) if an inspector suspects on reasonable grounds that there **may** be something related to breach of the Spam Act 2003 on any land, or in or on any premises, vessel, aircraft or vehicle, or
    b. **without a search warrant**, with the consent of the **owner or occupier** (s.542) of the land, premises, vessel, aircraft or vehicle, if an inspector suspects on reasonable grounds that there **is** on any land, or on or in any premises, vessel, aircraft or vehicle "anything connected with" a particular breach of the Spam Act 2003.

    In either instance, an inspector may enter; search; break open and search a cupboard, drawer, chest, trunk, box, package or other receptacle, whether a fixture or not; and examine and seize anything that the inspector suspects on reasonable grounds to be "connected with" the offence or breach (s.542(2)).

2. Searches **to monitor compliance** with the *Spam Act 2003* ("for the purpose of finding out whether the *Spam Act 2003* has been complied with") may be conducted:
    a. **with a monitoring warrant** issued by a magistrate (s.547D), or
    b. **without a warrant**, with the consent of the **occupier** (s.547A).

    In either instance, an inspector may enter any premises and exercise the monitoring powers (s.547D(5)(a) and s.547A) set out in s.547B which include:

        (a) to search the premises;
        (b) to inspect and take photographs, or make sketches, of the premises or any

substance or thing at the premises (including operate equipment at the premises to determine whether it or a disk, tape or other storage device contains relevant information (s.574B(2)) and if so put the information in documentary form or on a storage device and remove it from the premises (s.574B(3));
(c) to inspect any document kept at the premises;
(d) to remove, or make copies of, any such document;
(e) to take onto the premises such equipment and materials as the inspector requires for the purpose of exercising powers in relation to the premises;
(f) to secure a thing, until a warrant is obtained to seize it,
(g) to secure a computer, until an order under section 547J (an access assistance order) is obtained in relation to it.

Note: Items (e) to (g) above are new powers that inspectors do not currently have in relation to enforcement of Part 21 − Technical Regulations. The powers in item (b) above to operate equipment, copy and remove information on disks etc. are also new powers.

Searches without a warrant

EFA strongly opposes the provisions empowering inspectors to conduct searches **without** a warrant for the reasons set out below.

Section 542 (searches relating to breaches of the Spam Act) will give inspectors the power to enter and search homes and property therein without a warrant and without the consent of the owner of the things (computers, files, documents, etc) to be searched and potentially seized and without the consent of the occupier. For example an inspector could enter a home with the consent of the landlord (the owner) and search the tenants' computers and other possessions. In addition, in the case of a residence shared by several people (e.g. joint owners/tenants, flat mates, family, etc.), an inspector could enter the home with the consent of one occupier and search possessions belonging to a different occupier, and computers used by more than one person.

Sections 547A and 547B (searches to monitor compliance with the Spam Act) also give inspectors the power to enter and search homes and property therein without a warrant and without the consent of the relevant occupier, although they do not allow inspectors to conduct searches with the consent of a landlord, only of one of the occupiers. (It is unclear why searches relating to breaches (s.542) may be conducted with the consent of the owner/landlord, but not searches to monitor compliance (s.547)).

The above circumstances apparently arise because inspectors' existing powers to enter and search premises with the consent of the owner or occupier are to be extended to suspected breaches of the *Spam Act 2003*. However, inspectors' existing powers are limited to enforcement of Part 21 of the *Telecommunications Act 1997* dealing with technical regulations. As such, they are only empowered to conduct searches in peoples' home to investigate matters such as whether illegal customer telephone equipment and/or cabling has been connected to the telecommunications network and/or compliance with the conditions of a connection permit. These matters can normally be ascertained without searching individuals' filing cabinets and cupboards, and certainly without searching individuals' computers and email etc.

The existing search powers are therefore far less privacy intrusive than those proposed in the Bill which permit inspectors to search through people's personal possessions such as their computers and email without a warrant. While arguably inspectors may have such powers presently, it seems most

unlikely an inspector could legitimately claim a necessity to search a computer to see whether illegal telephones or cabling were installed in the premises.

Furthermore, a search of a suspect's computer (including email etc) is very likely to invade the privacy of innocent people who have been in contact with the suspect at some time, and innocent people who use the same computer as a suspect. In this regard, the proposed search powers are as privacy invasive as interception of a telephone call − during which the conversation of people who are not suspects are monitored as well. This is a primary reason for the special and strict rules applicable to issue of a telecommunications interception warrant. It is completely inappropriate to permit inspectors to search email without a warrant of any type. Judicial scrutiny is required to minimise the potential for invasion of the privacy of non−suspects and innocent persons without adequate justification.

In addition, under Sections 547A and 547B (searches to monitor compliance with the Spam Act), an inspector will be empowered to enter and search a residence without a warrant in circumstances in which they would not be able to obtain a monitoring warrant. The SCA Bill states that monitoring warrants must not be issued by a magistrate unless an individual who ordinarily resides at the premises has either been found by the Federal Court in the last 10 years to have breached the *Spam Act 2003* or has previously given an undertaking to comply (s.547D(4)). Contrary to these provisions however, an inspector will be empowered to enter and search a residence, *without* a warrant, when:

- no person who ordinarily resides at the premises has previously been found to have breached the *Spam Act 2003* or has given an undertaking to comply; or
- it is more than 10 years since the Court finding or undertaking was given.

This situation is unsatisfactory because inspectors' powers in relation to monitoring compliance by a prior offender appear to be more extensive than in relation to searches associated with a person who is not a prior offender. It appears these more extensive powers, which are able to be used without a warrant in circumstances in which a warrant could not be obtained, could be conveniently used to conduct searches associated with persons who are **not** prior offenders. While any evidence obtained in such circumstances may not be admissible in a Court, the proposed law should not facilitate or enable the potential use of the extra privacy invasive monitoring powers in relation to non prior offenders.

Recommendations:

1. The entry, search and seizure provisions **relating to breaches** of the *Spam Act 2003* must be amended to require a search warrant issued by a magistrate.

2. The entry, search and seizure provisions **relating to monitoring compliance** with the *Spam Act 2003* must be amended to require a monitoring warrant issued by a magistrate.

   In the highly unsatisfactory event that the provisions **relating to monitoring compliance** are not amended to require a warrant, they must be amended so that entry, search and seizure *without* a monitoring warrant is not permitted in circumstances in which the SCA Bill states a magistrate must not issue a monitoring warrant.

Searches of innocent recipients homes and possessions

Both Sections 535 (with search warrant) and 542 (without search warrant) enable searches of the homes and other premises of ***recipients*** of spam.

This situation appears to arise because the entry and search powers are not limited to premises/property associated with a suspect, but apply to:

- "anything that may afford evidence about a breach" (s.535(1)), and
- a "thing" that is "connected with a particular breach" (s.542(1)).
  The SCA Bill states that "a thing is connected with a breach of the *Spam Act 2003* if it is ... a thing that may afford evidence about the breach" (s.541A).

Obviously, an unsolicited commercial electronic message that has been received is a thing that may afford evidence about a breach. While it may be considered unlikely that inspectors would search the homes of recipients of spam, it is essential that the law specifically not allow that to occur without the consent of the relevant individual, e.g. the owner of the computer, email or "thing", as applicable, to be searched.

EFA notes that some proponents of the Bills regard the provision enabling search of innocent recipients' homes and possessions as unimportant because they do not expect the law would be used for that purpose. EFA considers a law enacted on the basis that it would only be applied selectively is a bad law. Such laws are not only open to abuse, they bring the law and the Parliament's competence into disrepute. If particular provisions of the proposed law would not be used, they should be deleted from the Bills.

EFA is aware it has been claimed that recipients of spam should not be outside the scope of the search and seizure provisions because spammers would include themselves on their own mailing lists and claim "recipient" status. This argument is unpersuasive because it is readily possible to avoid that situation without permitting searches of the property and possessions of recipients of spam who are not suspected on reasonable grounds of being in breach of the law.

Recommendation:

1. The entry, search and seizure provisions must be amended to ensure that a search cannot be conducted (whether with or without a warrant) of the premises or possessions of anyone other than a person who is suspected on reasonable grounds of being in breach of the *Spam Act 2003*.

Searches of stored messages/ISP equipment without a warrant

In addition, the enactment of the *Spam Act 2003* would apparently have the effect of authorising an Internet Service Provider ("ISP") to allow an ACA inspector (i.e. a civil penalty−enforcement agency employee) to search the ISP's customers' email boxes (possibly including the actual content of messages) without a warrant under the existing "reasonably necessary assistance" provisions of Section 282(2) ("Law enforcement and protection of public revenue") of the *Telecommunications Act 1997*.

In this regard, the removal of the owner/occupier consent provisions (as recommended earlier herein) may be insufficient to ensure a warrant is required for searches of communications information held by ISPs because the existing provisions of Section 282 of the *Telecommunications Act 1997* appear to be applicable to investigation of suspected breaches of the *Spam Act 2003*.

EFA has long been of the view that Sections 282(1) and (2) of the *Telecommunications Act 1997* require amendment to ensure that the content of messages cannot be accessed by law enforcement agencies without a warrant, in order to adequately protect Internet users' privacy and minimise the potential for "fishing trips" without a warrant. Whether or not Sections 282(1) and (2) authorise disclosure of the *content* of communications (as distinct from, for example, the 'To' and 'From' fields of messages) has long been a recognised grey area of the *Telecommunications Act 1997*. (See for example Section 4.3 of the *Telecommunications Interception Policy Review − May 1999* issued by the Attorney−General's Department.)

Recommendation:

1. Sections 282(1) and (2) of the *Telecommunications Act 1997* must be amended to ensure that carriage service providers (includes ISPs) and other electronic message service providers (as defined in the SCA Bill) are not permitted to allow inspectors to conduct searches associated with the *Spam Act 2003* of their customers', or any other persons', communications without a warrant.

▲ Go to Contents List

Assistance Orders compelling disclosure of encryption keys and passwords and imprisonment penalties

EFA is strongly opposed to the assistance order provisions in Section 547J of the SCA Bill which enable a person who has lost or forgotten a password or encryption key to be imprisoned for six months.

Section 547J empowers a magistrate to issue an order compelling a person who is "reasonably suspected of having been involved in a breach" to disclose encryption keys and/or passwords and any other any information or assistance that is considered "reasonable and necessary" to allow an inspector "to do one or more of the following:

(a) access data held in, or accessible from, a computer that is on those premises;
(b) copy the data to a data storage device;
(c) convert the data into documentary form."

The penalty for failure to provide the information or assistance is imprisonment for six months.

A person who is merely suspected of having been "involved in" sending one single unsolicited commercial electronic message could be the subject of an order and imprisoned for six months if they decline, or are unable, to provide the required information or assistance.

It is completely absurd that a person who is merely suspected of having been involved in a breach could be imprisoned for six months for failing to provide information or assistance to an investigator, when they could not be imprisoned even if they were found guilty of having committed the suspected breach.

These provisions are a great example of overkill. They are almost identical to those in the *Cybercrime Act 2001*, notwithstanding that sending unsolicited commercial electronic messages will not be a *criminal* offence.

The only difference between the assistance order provisions of the Spam Bills and the *Cybercrime Act* is that an order would be obtainable in relation to a larger number of people under the *Spam Act 2003* than under the *Cybercrime Act*. The *Cybercrime Act* provision is limited to persons "reasonably suspected of having **committed an offence**" while the Spam Bill provision applies to persons "reasonably suspected of having been **involved in the breach**".

These types of assistance orders have long been controversial in relation to criminal offences and are even more controversial in relation to non−criminal offences. As the drafters of the Model Criminal Code stated (in Chapter 4 of the MCC Report):

> *The issues involved are both difficult on a technical level and controversial in relation to the protection of individual human rights and the rights of corporate entities.*

The matter of assistance orders is aimed squarely at the problems presented by security passwords and, more particularly, encrypted data. One of the major problems is the cursory treatment of the requirement for persons to reveal encryption keys.

There may sometimes be legitimate reasons why a private key or plain text could not be handed over to an ACA inspector or law enforcement agency, and it would be difficult for the subject of an assistance order to provide proof that they did not possess or have access to a key or plain text. The prospect of users of encryption being jailed despite having genuinely lost their private keys is a major and quite legitimate concern. Any legislation containing such provisions should, at the very least, provide an indication as to how those served with assistance orders requiring plain text or encryption keys can successfully prove that they cannot comply with the order.

It is also of concern that these requirements will rapidly fall behind the technology that is being used for encryption and data protection. For example, various biometrics around voice recognition (that may not work with a shaky voice), various movement registers such as keystrokes, mouse movements, etc. All of these could very be feasibly be "lost" by an individual during the stress of an investigation.

Furthermore, the 1997 OECD cryptography guidelines, which Australia has adopted, specifically recognize the fundamental right of privacy in relation to encrypted data:

> *Article 5. The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.*

A further problem is that a single encryption key often serves the dual purpose of ensuring confidentiality and providing secure authentication of the signatory to a document (through a digital signature). Revealing the key (or the passphrase thereto) can therefore compromise the integrity of the owner's digital signature. (It should be noted that a person on whom the assistance order is served is not assumed to have committed a breach.)

In addition, increasing numbers of individuals are becoming conscious of the risks of disclosure of private and/or business information in the case of loss or theft of computers and therefore encrypt the entire hard drive of the computer. It is completely unreasonable that a person can be required to give up the "keys to the castle" to provide an investigator with access to a single piece of email or data.

Clearly there is tension between privacy rights and legitimate law enforcement needs. An approach needs to be found that balances these issues, or at least recognises in the law that an offence is not automatically criminalised in the event of failure to provide assistance.

In its present implementation, the law enforcement provisions in the Bill totally fail to address these potential problems, or even acknowledge that the measures proposed are controversial.

The law enforcement provisions may also have the effect of over−riding the common law privilege against self−incrimination. This situation could arise where a person was compelled to reveal a password or encryption key as a requirement of an assistance order. The right to silence is a long−standing right in most jurisdictions and it is unacceptable that it should be potentially over−ridden in the Bill without strong justification. There does not appear to be any strong justification for such provisions in relation to non−criminal offences such as those in the Spam Bill.

Recommendation:

1. The assistance order provisions must be deleted.
2. In the completely unsatisfactory event that the assistance order provisions are not deleted, amendments to the proposed provisions must be made to:
    - ♦ address the issues and problems raised above; and
    - ♦ apply only to persons reasonably suspected of having **committed** a breach; and
    - ♦ apply only in instances where the suspected breach concerns the sending of **bulk** unsolicited messages, not a single message or a few messages; and
    - ♦ change the penalty for failure to provide assistance/information (including keys and passwords) from imprisonment to a pecuniary penalty that is no more than the minimum pecuniary penalty applicable to the suspected breach.

▲ Go to Contents List

Designated Commercial Electronic Messages

Exempt Bodies

EFA considers the exemptions for government bodies, political parties, religious organisations, charities or charitable institutions and educational institutions (based both in Australia and overseas) to be undesirable and completely unnecessary.

The Explanatory Memorandum states that the exemptions permitting the bodies to send unsolicited commercial messages: "aims to ensure that there is no unintended restriction on government to citizen or government to business communication, nor any restriction on religious or political speech". However, while such an aim has legitimacy in principle, it is not relevant to the exemptions.

The sole purpose of the exemptions authorising various types of bodies to send **unsolicited** electronic messages **"relating to goods and services"**. The proposed law does not prohibit those bodies, nor anyone else, from sending unsolicited **non**−commercial messages. Furthermore, without the special exemption, the proposed law would not prevent the bodies from sending commercial electronic messages to individuals with whom they have an existing or prior relationship and the individual's consent has been inferred in their provision of an electronic address to the body.

Moreover, the exemption results in transportation of unsolicited commercial messages being financed by unwilling recipients of "legalised" spam.

The exceptions would, for example, enable government agencies to shift the cost of providing services to their "clients" (i.e. citizens) from the agency to the recipient. For example, the Australian Tax Office could send huge files containing the latest GST Booklet, or Annual Tax Guide, resulting in the recipient being forced to pay the cost of receiving it in their Internet access fees. If the ATO wishes to send such information electronically, they should be required to obtain the recipient's prior consent. Further, the ATO would not even be required to provide a functional unsubscribe facility.

The Explanatory Memorandum states: "Local government often provides services on a fee−for−service basis which are essential to the community, but electronic messaging about them might potentially be restricted, but for this exclusion". Again, if local government wants to shift their communication costs to the recipients of their messages, they should be required to obtain consent.

(It also seems questionable whether government business enterprises would be covered by this exception. If so, it may give such entities an unfair competitive advantage over the private sector.)

EFA cannot perceive of any reason why citizens should be forced to receive and pay for unsolicited electronic messages **relating to goods and services** from government bodies, without the recipient's consent.

Similarly, the sole purpose of the exemption for political parties, religious organisations, charities and charitable institutions, and educational institutions, is to authorise such bodies to send unsolicited direct marketing messages advertising their publications and other products, school and church fetes, etc. There is no legitimate reason why individuals should be forced to receive and pay for unsolicited electronic messages **relating to goods and services** from any of these bodies, without the recipient's consent.

Furthermore, we note the exemption also applies to organisations based overseas and the comments of the UK Parliamentary All Party Internet Working Group in their 6 October 2003 Spam Report:

> "120. There are, however, some differences [in the proposed 'Spam Act 2003'] from the European Directive. The proposed legislation does not restrict a business to only advertising its own, similar, products. It also explicitly excludes messages sent by 'government bodies, registered political parties, religious organisations, and charities'.
> 121. We are unaware of how many charities there might be in Australia, but in the UK there are about 188,000. There will also be a fair number of government bodies, political parties and religious organisations. Although we can see the political attractiveness of exempting bodies such as charities from anti−spam legislation, we fear that this may prove to be short−sighted if a significant number of them misinterpret the legislation as meaning that spam from all of them would be in any sense acceptable to the recipients."

Moreover, it unacceptable that the exempt bodies are also exempt from the requirement to provide a functional unsubscribe facility the same as that applicable to commercial messages sent with the recipient's consent. There is no reason why bodies that are permitted to send commercial messages, *without* consent, should not be required to provide a functional means by which recipients can notify the body that they do not wish to receive their unsolicited commercial messages. Where a law

creates a presumption that consent exists, a person must be able to easily withdraw consent.

It is also unacceptable that the bodies are exempt from the prohibitions on use of address harvesting software and harvested address lists. The prohibitions do not apply to the use of such software and lists for the purpose of sending unsolicited but "designated" commercial messages.

Recommendation:

1. The exemptions for government bodies, political parties, religious organisations, charities and charitable institutions, and educational institutions, must be deleted.

Exempt Factual Information Messages

The Explanatory Memorandum states that the exemption for messages containing "factual information":

> "*is designed to ensure that messages which may be seen to have some form of commercial element, but which are primarily aimed at providing factual information are not covered by the rules relating to commercial electronic messages in clauses 16 and 18 of the Bill. Many firms and organisations provide newsletters and updates of this type which are of benefit to sections of the general or business community and it is not intended to prevent this beneficial activity.*"

and provides various examples including:

- "*an electronic message from a private law firm which includes an information sheet outlining the effects of a particular court decision*";
- "*an electronic version of a neighbourhood watch newsletter which is sponsored by the local newsagent*";
- "*an electronic newsletter from the local chamber of commerce which is sponsored by one of their members*".

EFA considers the exemption for "factual information" messages is large enough to drive a truck through.

These "factual information" messages are obviously intended to advertise and promote the sender or sponsor of the message and their goods or services. EFA sees no reason why individuals should be forced to receive and pay for *unsolicited* "factual information" messages from hundreds of law firms discussing court decisions, nor from hundreds of real estate agents discussing the state of the market, etc. However, the proposed law legitimises and authorises exactly that situation.

Moreover, it is inappropriate that legislation, in effect, compel individuals to receive and pay for information whether the government thinks it is "beneficial" information or not. Legislation should not consent on individuals' behalf to receiving "factual information" or any other type of information.

Furthermore, it is unlikely that spammers will have any difficulty writing a paragraph containing "factual information" for the purpose of being able to send a "designated" unsolicited message. The specified permitted "additional information" includes "the name, logo and contact details of the individual or organisation who authorised the sending of the message" and "if the message is sponsored−the name, logo and contact details of the sponsor" and various other information. The "additional information" is of itself sufficient to advertise goods and services, etc. The inclusion of a

contact email address will of course include the domain, that is, the website address. A logo can be designed to in effect advertise the product. The name of the organisation can also advertise the goods or services, etc.

It is also unacceptable that senders of such unsolicited messages are exempt from the requirement to provide a functional unsubscribe facility and exempt from the prohibitions on use of address harvesting software and harvested address lists.

Recommendation:

1. The exemption for factual information messages having a commercial element must be deleted.

▲ Go to Contents List

Unsolicited Commercial Electronic Messages

EFA is highly concerned that the *Spam Act 2003* will prohibit the sending of messages that are not commonly regarded as spam.

The proposed legislation does not target the sending of unsolicited messages in bulk, nor the sending of unsolicited form messages indiscriminately by automated means.

Instead, it prohibits the sending of a single *commercial electronic message* that has an *Australian link* (s.7) and is not a *designated commercial electronic message* (sch.1) (s.16(1)). The prohibition does not apply if the recipient consented (as defined in Sch.2) to the sending of the message. However, the definition of consent is narrow and a sender who wishes to rely on consent having been received bears an evidential burden in relation to that matter.

In our analysis, the legislation will prohibit the sending of various types of ordinary electronic messages as a result of the applicability of the proposed law to a single message, combined with the definitions of a "commercial electronic message" and "consent".

We outline the relevant aspects of the definitions below, followed by example case scenarios.

Definition of commercial electronic message

A *commercial electronic message* is defined to mean a message where it would be concluded (from the content, links, contact information, etc. in the message) that the message has one of the following purposes:

- to offer to supply, or to advertise or promote, any of the following:
  - ♦ goods or services; or
  - ♦ land or an interest in land; or
  - ♦ a business opportunity or investment opportunity; or
- to advertise or promote a supplier, or prospective supplier, of any of the above; or
- to assist or enable a person, by a deception, to dishonestly obtain property belonging to another person or a financial advantage from another person, or dishonestly obtain a gain from another person; or
- a purpose specified in the regulations.

A message is a *commercial electronic message* if it has one of the above purposes, whether or not that is the primary or sole purpose of the message. In this regard, the Explanatory Memorandum states: "if the message itself contains nothing of a 'commercial nature', but it provides a link to a web page which is 'commercial in nature' then this will be a commercial message for the purposes of this Bill". (In relation to this aspect, see Case Scenario 4 later herein.)

The definition of a *commercial electronic message* covers a wide range of messages that are not generally regarded as spam, including messages that are unquestionably ordinary email, because:

- the definition is based on analysis of the content of a message, including determination of whether a small portion of the content has a commercial aspect;
- it is irrelevant whether or not there is a relationship between the sender and the organisation (or individual) that may receive financial or other benefit as a result of promotion or advertising of their goods, services, etc.;
- the intent and purpose of the sender in sending the message is irrelevant.

We recognise the above arises from due regard to avoiding loopholes for spammers, but we consider insufficient consideration has been given to the effect on ordinary email (see Case Scenarios later herein).

While *commercial electronic messages* may be sent with consent of the recipient, the definition of consent does not overcome the undesirable consequences arising from the definition of a *commercial electronic message* and the applicability of the legislation to a single message.

Definition of Consent

Consent, for the purposes of the proposed Act, "*means:*

> *(a) express consent; or*
> *(b) consent that can reasonably be inferred from:*
> *(i) the conduct; and*
> *(ii) the business and other relationships;*
> *of the individual or organisation concerned.*" (Sch.2(2))

Express consent means the individual has given explicit consent to the particular sender. According to the Explanatory Memorandum it applies when "the person has specifically requested such material (either verbally or in writing) from the sender". This is the commonly understood meaning of express consent and is appropriate.

Inferred consent means consent that can reasonably be inferred from the conduct **and** the business and other (e.g. family) relationships of the recipient concerned. It is clear from the Explanatory Memorandum ("EM") that the "and" between (b)(i) and (ii) above is intentional, that is, unless there is a prior relationship (including prior contact) between the recipient and the sender (person or organisation), consent cannot be inferred (unless the "conspicuous publication" exception, discussed later herein, is applicable).

In the Explanatory Memorandum, all examples of inferred consent refer to situations where the recipient and sender have a prior relationship (at the least, have been in prior contact) **and** the recipient has specifically provided their electronic address to the sender (person or organisation) **and** from that conduct (i.e. provision of address) the recipient's consent may be inferred. (However, provision of an address in the foregoing circumstances would not constitute inferred consent to sending of **all** types of commercial messages.) In this regard, the EM states inter alia that:

"For example if the person has an existing business relationship with the sender and as part of that relationship has knowingly and directly provided an electronic address to the sender, then it would be reasonable to infer that the person has consented to receiving commercial electronic messages from the sender."
and
"The effect of [the defence provision in Subclause 16(2)] is that a person may send another person commercial electronic messages where that other person has consented to receiving it. It therefore enables persons to send commercial electronic messages to persons with whom they have a pre−existing business relationship."

Case Scenarios

The above definitions result in prohibition of single messages that are not generally regarded as spam as discussed in the case scenarios below.

EFA is aware that some proponents of the Bills consider that known flaws and definitional issues as demonstrated in the case scenarios are irrelevant because they do not believe the provisions would be used or enforced in that way, and/or that the problems can be fixed in the future via case law and regulations. EFA considers such an approach to law−making is wrong. The result of such an approach is that individuals who are accused of breaching the law fund the clarification of the law, even when a Court rules that the individual's activity did not breach the law.

Furthermore, a law enacted on the assumption that citizens will not comply with ridiculous aspects of it anyway, and/or on the assumption that it would only be enforced selectively, is a bad law. Such laws are open to abuse and also bring the law and the Parliament's competence into disrepute.

Case Scenario 1:

An individual has a personal (not business) web site and publishes their resume on it with their personal (not work−related) email address, for example: xybloggs@yahoo.com.au. The individual may, for example, be an unemployed person, or an employed person who is nevertheless interested in full or part−time contract, consultancy or job offers.

Another person (or organisation/company) wishes to email the individual to offer a business opportunity, for example, a contract for work that is directly relevant to the experience and skills set out in the individual's resume.

The message would be caught by the definition of "commercial electronic message" because its purpose is to offer a business opportunity. (Note: "business" is specially defined in the *Spam Act 2003* to vary the ordinary meaning of "business" so that it is not necessary to establish that a commercial enterprise is carried on in a regular, repetitive or continuous manner.)

A contract for work/consultancy or employment would constitute a "business opportunity" − if it would not, then neither would many messages that unquestionably are spam such as: "Work from home selling this or that"; "Make money advertising these porn sites on your own site"; etc, etc.

The proposed law would apparently prohibit sending of the above message because:

1. the law applies to a *single* message no matter how carefully and relevantly targeted; and

2. the sender would not be able to rely on the defence that the individual had given consent *as currently defined in the Bill* because:
    a. Express consent only applies when the individual has given explicit consent to the particular sender; and
    b. Consent cannot be inferred unless, as discussed earlier herein, there is a prior relationship between the sender and recipient.
3. the sender would not be able to rely on the exception applicable to "conspicuous publication" of an electronic address because the individual's published electronic address is not a work related address, i.e. it is not the address of an employee, officer, etc. of an organisation (Sch.2(4)(2)).

Case Scenario 2:

An individual has a personal (not business) web site providing information about a particular topic and also publishes a list of recommended books on the same topic. The individual's personal (not work related) email address, for example: xybloggs@yahoo.com.au, is also available on the site.

A new book about exactly the same topic is published and the author's public relations company wishes to send the individual an email message offering the person a copy of the new book.

Such a message would be caught by the proposed law because the purpose of the message is clearly to promote a book (that is, a good as in "goods and services") and the same situation applies as in Case Scenario 1 above, irrespective that such a message is not commonly considered to be spam.

Case Scenario 3:

An individual has a personal web site containing a number of articles written by them about one or more topics.

A publisher of a magazine or author of a proposed book wishes to email the individual offering to pay them for the right to re−publish one of their articles in a magazine or book.

Such a message would be caught by the proposed law because the purpose of the message is to offer a business opportunity, and the same situation applies as in Case Scenario 1 above, irrespective that such a message is not commonly considered to be spam.

Case Scenario 4:

The fundamental problem with the definition of *commercial electronic message*, as defined in the proposed law, and prohibition on sending a single message to a specific individual is demonstrated in this example.

An individual sends an unsolicited message to another person on a topic that is not of a 'commercial nature', but includes a signature (.sig) section containing a link to the web site of the company that employs the sender, or, a self−employed person sends an unsolicited message on a topic that is not of a 'commercial nature' but contains a link to their business web site in the signature of the message. The message responds to comments made by the recipient on their personal web site, or in an offline publication, etc.

Such messages are a *commercial electronic message* as defined in the Bill because although "the message itself contains nothing of a 'commercial nature'", it "provides a link to a web

page which is 'commercial in nature'". This is an example stated in the Explanatory Memorandum.

The sending of unsolicited "commercial electronic messages" of the above nature may or may not be prohibited depending on subjective analysis of the other content of the message. Where there is no other information that can be seen to have a purpose of promoting the company or business, the message may come within the exemption for "designated commercial electronic messages" if it consists of "factual information". It appears it would not be exempt if it consists of the sender's opinions or non−factual information.

If the message is not an exempt "designated" factual information message and the message is sent to an individual with whom the sender had no prior relationship, but which was in response to comments made by the recipient on their personal web site, the message would be sent in breach of the proposed law. Consent, as defined in the Bill, of the recipient cannot be inferred unless there is a prior relationship between the sender and recipient or the exception concerning the "conspicuous publication" of a recipient's work−related address is applicable.

There are numerous similar scenarios arising principally as a result of the Spam Bill's objective of regulating every message that has a commercial aspect rather than dealing with the sending of unsolicited direct marketing messages.

We note that it is considered by some proponents that the proposed Australian legislation could 'lead the way' internationally. However, we are aware that the proposed Australian legislation is considered less than ideal by, for example, the UK (Parliamentary) All Party Internet Working Group according to their Spam Report released on 6 October 2003.

We also note that the UK *Privacy and Electronic Communications (EC Directive) Regulations 2003* will become effective on 11 December 2003 in compliance with the EU *Directive on Privacy and Electronic Communications (2002/58/EC)*. This UK legislation appears to be quite remarkably clear, without convoluted provisions giving rise to unintended consequences. It states:

"Use of electronic mail for direct marketing purposes
22. − (1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.
(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.
(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where −
(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;
(b) the direct marketing is in respect of that person's similar products and services only; and
(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication."

EFA considers it extremely unlikely that the proposed Australian legislation with be more effective in reducing spam than the UK legislation, however, the Australian legislation will prohibit messages that are not spam, in part because it does not prohibit only unsolicited direct marketing. It also prohibits single messages sent by individuals that can be interpreted as 'promoting' some product or service irrespective of whether there is any financial or other benefit to the sender in promoting or recommending same.

EFA questions why the Australian Government apparently considers it necessary to implement a complex and subjective law applicable to all messages that may be perceived to have a 'commercial aspect' given that the vast majority of spam that has a 'commercial aspect' obviously has the purpose of direct marketing.

Recommendation:

1. The proposed legislation must be amended to either:
   - ♦ exclude its applicability to the sending of a single message to a particular individual where such a message is not part of a bulk mailing and/or is not sent by automated, indiscriminate means; or
   - ♦ prohibit the sending of unsolicited messages for the purposes of direct marketing, instead of regulating every message that has a 'commercial aspect'.

   If amendments of the above type are not implemented, the Spam Bill must not enacted. In our view, the only other possible solution to the problem of restricting ordinary email is to amend the definition of consent. However, such an amendment would be likely to result in a loophole for spammers and also result in senders of ordinary email potentially being required to prove they had consent to send a message that is not generally regarded as being spam. Such a situation is not acceptable.

2. The definition of "consent" in Section 2 of Schedule 2 must be changed so that it is readily apparent that there does not have to be both a 'business' **and** an 'other' (e.g. family) relationship. It presently states:

   > *"2 Basic definition*
   > *For the purposes of this Act, consent means:*
   > *(a) express consent; or*
   > *(b) consent that can reasonably be inferred from:*
   > *(i) the conduct; and*
   > *(ii) the business and other relationships;*
   > *of the individual or organisation concerned."*

   In s.2(b)(ii), the word "and" should be changed to "or", that is, to "the business or other relationships".

▲ Go to Contents List

Conspicuous Publication Exemption

EFA notes that although the proposed law generally establishes an opt−in regime, an opt−out regime is applied to work−related electronic addresses that have been conspicuously published.

The "conspicuous publication" exception is seriously flawed.

The exception provides that a person is taken to have consented to the sending of unsolicited commercial electronic messages to them:

- if their work related "electronic address has been conspicuously published" (on the Internet or in a hard copy publication or elsewhere offline); and
- "the publication [of the address] is not accompanied by a statement to the effect that the [person] does not want to receive unsolicited commercial electronic messages at that electronic address; or a statement to similar effect" (the EM provides examples of statements such as "No spam", "No UCE");

- and the person is:
  - ♦ a particular employee, director or officer of an organisation; or
  - ♦ a particular partner in a partnership; or
  - ♦ a particular holder of a statutory or other office; or
  - ♦ a particular self−employed individual

  and the unsolicited message is "relevant to the work−related business, functions or duties" of the person and "it would be reasonable to assume that the publication [of their work related address] occurred with the agreement of" the **person**.

- or the person is:
  - ♦ an individual from time to time holding, occupying or performing the duties of, a particular office or position within the operations of an organisation; or
  - ♦ an individual, or a group of individuals, from time to time performing a particular function, or fulfilling a particular role, within the operations of an organisation.

  and the unsolicited message is "relevant to the office or position concerned", or to "the function or role concerned" and "it would be reasonable to assume that the publication [of their work related address] occurred with the agreement of" the **organisation**.

These provisions present significant difficulties for people who have work−related electronic addresses.

- It is impractical, and in numerous instances impossible, for individuals to retrospectively deny use of a published electronic address by adding "No Spam" or "No UCE" statements:

  - ♦ Electronic addresses are already published on CD ROMs, in books, journals, magazines and newspapers, in printed telephone directories, etc. where it will be reasonable to assume that the person consented to the publication but which cannot be changed.

    Also, with regard to the future EFA questions whether, for example, Telstra will be required to accompany mobile telephone numbers with "No spam" (re SMS) statements in printed telephone directories, CD ROMs and their web site directories and whether Telstra will be permitted to charge fees for doing so, as is the case in relation to non−publication of silent numbers.

  - ♦ Addresses are also already published on web sites over which the individual has no control, or which do not have provision for giving effect to the person's wishes. EFA questions whether, for example, government web sites will be required to promptly add "No spam" statements on request of the individuals whose address are published on their sites. For example, the Austrade site which acknowledges the problem of spam being received by their clients whose electronic addresses are published on the site.

- The matter of what is relevant to a person's job function is just as open to interpretation as the matter of what is spam. For example, the "work−related business, functions or duties" of self−employed persons and small business owners can readily be interpreted to include everything related to managing **any type** of business. The "conspicuous publication" exception therefore enables such persons to be spammed with advertisements for e.g. insurance, office equipment, computer supplies, printer cartridges, business software, seminars about marketing, etc, etc, in addition to goods and services relevant to their **specific type** of business.
- An individual may wish to receive commercial messages that are directly relevant to their specific type of business but not indiscriminately targeted commercial bulk email. An accompanying statement of the type provided for in the proposed law, such as "No UCE", does not provide for this situation.

In addition, the clause stating "it would be reasonable to assume that the publication [of the work−related address] occurred with the agreement of [the person]" may have unintended consequences. EFA considers any such clause should be phrased in a manner that clearly applies a test of what a reasonable person would consider reasonable to assume. The current phrasing may suggest to spammers that the test is what the spammer thinks it is reasonable to assume.

Recommendation:

1. The inference from conspicuous publication of a work−related address should be reversed.

   The legislation should provide that consent may only be inferred from publication of an electronic address when it is accompanied by a statement to the effect that "This address may be used for ..." in which the person has designated the type of information they wish to receive, or is accompanied by a statement such as "UCE accepted".

   The absence of an accompanying statement should mean: "This address is to contact me or my organisation about the products and services that we can provide to you. It is not to used for the marketing of your own products or services."

▲ Go to Contents List

Address Harvesting Software and Lists

EFA notes with concern that the prohibitions concerning address−harvesting software and address−harvest lists do not apply to either of the following:

- their supply by, or acquisition or use by, a government body i.e. a department, agency, authority or instrumentality (the prohibitions only apply to a "person" which means an individual, a partnership, and a body politic or corporate);
- their supply or acquisition or use for the purpose of sending unsolicited ***designated*** *commercial electronic messages*.

This means that the software and/or lists is permitted to be supplied to, acquired by and used by:

- government bodies for any purpose;

- political parties, religious organisations, charities and charitable institutions, educational institutions for the purpose of sending unsolicited ***designated*** *commercial electronic messages*;
- any organisation or individual for the purpose of sending unsolicited ***designated*** *commercial electronic messages* that consist of primarily "factual information";
- any organisation or individual for the purpose of sending unsolicited bulk email that is not a *commercial electronic message* as defined in the Bill.

Recommendations:

1. The prohibitions on supply, acquisition and use of address−harvesting software and address−harvest lists should apply to government bodies.
2. The supply, acquisition and use of address−harvesting software and address−harvest lists should be prohibited in relation to the purpose of sending "designated" and **all** unsolicited electronic messages, not only the narrow category of messages covered by Section 16.

Go to Contents List

Service Provider Protection from Civil Proceedings

The SCA Bill amends the *Telecommunications Act 1997* to extend the matters that may be dealt with by industry codes and industry standards to include procedures to be followed by service providers "in dealing with unsolicited commercial electronic messages (including procedures relating to the provision or use of regularly updated software for filtering unsolicited commercial electronic messages)" (proposed s.113(3)(q)).

It also gives providers protection from civil proceedings "in respect of anything done by the provider in connection with" procedures in a registered code or standard for dealing with unsolicited commercial electronic messages (proposed s.137)

The Explanatory Memorandum states: "This will provide significant reassurance to these service providers regarding a common concern that they may attract civil liability for undertaking reasonable spam−filtering activity. It will provide an incentive for the development and the uptake of compliant code(s), in order to obtain the indemnity offered."

The proposed provisions would enable the industry to develop a Code that could be registered by the ACA and would then be enforceable against all ISPs and other electronic messaging service providers, irrespective of whether customers, i.e. the recipients of messages, wished their email to be spam filtered by their service provider or not. Also, it should be recognised that some people prefer to configure and use their own spam filtering system rather than a service provided by an ISP. Although the *Telecommunications Act 1997* requires the industry to issue any draft code for public consultation, there is no requirement for the industry or the ACA to remove any provisions opposed by even a majority of members of the public.

It appears the proposed immunity from any civil proceedings may be sufficiently broad to give providers protection in relation to failure to provide contracted services, for example, non−delivery of email to a recipient that is **not** an "unsolicited commercial electronic message", if that occurred as a result of complying with procedures in an industry code or standard. Further, if a customer wished to change providers with a view to being able to receive messages being blocked by their current provider's spam filtering system, the customer would probably have to pay their current ISP one or month's fees under the ISP's terms and conditions of termination of their account. It appears an

existing right to decline to pay such fees due to non−provision of contracted service may in effect be over−ridden by the protection from civil liability provisions.

Extreme care would need to be taken in the development and registration of any Code to ensure it would not have the effect of undermining existing consumer protections and rights. However, there is no surety that a largely self−regulatory industry code would be sufficiently cautiously developed and/or implemented.

The essence of any "safe harbour" provision is a trade−off − if the entity complies with a certain set of standards then immunity is granted for acts done in good faith. An ISP or other electronic messaging service provider who spam−filtered a customer's email without their consent and thereby caused foreseeable loss should not receive immunity.

Recommendation:

1. The provision providing protection from civil proceedings must be changed so that, in relation to proceedings by a service provider's customers, the protection applies only to anti−spam filtering services provided with the prior consent of the customer, that is, when a customer has voluntarily opted in to having their electronic messages spam−filtered by the service provider.

Go to Contents List

Penalties

EFA observes that the ACA will be empowered to issue an infringement notice to a person alleging a breach of the *Spam Act 2003*, and requiring the person to pay a pecuniary penalty or else the matter will be taken to Court. It appears the ACA will not be required to give the person any evidence of the alleged breach, merely "brief details" consisting of the date of the alleged contravention and the civil penalty provision that was allegedly contravened (Sch.3(4)).

EFA considers the pecuniary penalties payable by means of an ACA infringement notice are inappropriately high for a case such as the sending of one single unsolicited message by a non−prior offender. For example, the ACA could issue an infringement notice to a person who has never committed a prior breach, alleging the person sent one single commercial electronic message, and requiring them to pay $440 or else the matter will be taken to Court.

While it may be unlikely that the ACA would issue an infringement notice to such a person, or take them to Court, as discussed earlier herein EFA has significant concerns about the application of the law to a single message that has a commercial aspect and about potential definitional issues concerning what is or is not a commercial aspect.

Recommendation:

1. The provisions should be amended so that the ACA is not permitted to do more than give a formal warning to a first time offender who is alleged to have sent a single message in contravention of s.16.

Go to Contents List

Conclusion

The proposed legislation is not suitable for enactment in its current form.

The search and seizure powers must be subject to issue of a judicial warrant and must not be applicable to property and possessions belonging to *recipients* of spam who are not suspected on reasonable grounds of breach of the Act. The provisions enabling a suspect or other person to be imprisoned for forgetting a password or other information must be deleted. Such provisions are completely absurd in legislation that does not involve imprisonment even if a person is found guilty.

The purpose of the proposed law is supposed to be prohibiting spam, not ordinary messages. However, it would legitimise and authorise the sending of "designated" spam (unsolicited bulk commercial messages), and would prohibit the sending of some ordinary messages that are not generally regarded as spam.

The legislation should be applicable to the sending of all unsolicited commercial electronic messages in bulk. It should not treat a single message sent to a specific individual as spam merely because the message has some form of commercial aspect.

The possible benefit of the currently proposed law in minimising receipt of spam is outweighed by its potential to result in unnecessary invasions of the privacy of innocent individual's homes and possessions and/or their imprisonment, prohibit ordinary electronic messages and its authorisation of "designated" spam.

▲ Go to Contents List