NATIONAL PARTY COMMUNICATIONS &
INFORMATION TECHNOLOGY POLICY COMMITTEE

SUBMISSION TO HOUSE OF REPRESENATIVES STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS REGARDING THE:

INQUIRY INTO PRIVACY AMENDMENT (Private Sector) Bill 2000

Contact details:
Chairman
Garry R. Ford
10 Clifford St
STAFFORD 4053
Ph (07) 3857 1203

NATIONAL PARTY COMMUNICATIONS & INFORMATION TECHNOLOGY POLICY COMMITTEE

10 Clifford Street Stafford, 4053 Phone/fax (07) 3857 1203 E-mail - coal_comms_pol@merddyn.apana.org.au

CHAIRMAN: Garry R. Ford, esq.,J.P.,P.G. Dip. A. ,B.A.,B.Ed.,F.R.Hist.S.Q.,M.A.C.E.,M.A.E.T.A.

12 May 2000

The Chairman, Mr Kevin Andrews, M.P.,
and members of the House of Representatives
Legal and Constitutional Affairs Standing Committee,
Parliament House
CANBERRA, 2600.

Dear Committee members,

The submission from the National Party Communications and Information Technology Policy Committee on the Privacy Amendment (Private Sector) Bill 2000 is hereby submitted for your consideration.

Garry R. Ford
Chairman

SUBMISSION TO HOUSE OF REPRESENATIVES STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS REGARDING THE:

INQUIRY INTO PRIVACY AMENDMENT (Private Sector) Bill 2000

Error! Not a valid heading level range.

SUBMISSION TO HOUSE OF REPRESENATIVES STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS REGARDING THE:

INQUIRY INTO PRIVACY AMENDMENT (Private Sector) Bill 2000

EXECUTIVE SUMMARY

The major problem with the proposed legislation is that **National Privacy Principle 2.1 (c)** is "opt out" for electronic forms of communication. This means people must pay to receive direct marketing E-mails without knowing what is in them first. Advertising costs shift from the seller to the prospective buyer. This also happens to a lesser degree with facsimiles. People do not have to pay to receive other forms of junk mail or telemarketing calls, so why lessen the standards with by proposing NPP 2.1 (c) as worded.

This problem can be easily fixed by the insertion of a new clause (iv) into NPP 2.1 (c) –

"(iv) there is no monetary cost to the individual, either directly or indirectly within their communication package, to receive the initial communication from the organisation; and"

and then renumber existing sub-clause (iv) to sub-clause (v).

Most Direct Marketers are responsible business people and do not use these objectionable practices, but those that do cause considerable damage to the operation of the Internet. Access is considerably slowed thus hindering its use by all, including others using E-Commerce legitimately. Sending "opt out" SPAM really defeats the purpose of direct marketing in the long term and destroys the prospects for E-Commerce in the long term.

Because dealing with Direct Marketing E-Mails, otherwise known as SPAM, is costly to Internet Service Providers (ISPs), these costs must be passed on to consumers. This makes using the Internet more expensive for all. The eventuality is that many sites are blocked thus denying legitimate users access to and from those sites and the information contained in them. There is also a finite limit to how much disruption to traffic the Internet can have before it crashes. It can cost ISPs millions of dollars yearly to deal with these crashes. The recent "I Love You" SPAM which also contained a virus shows just how out of control SPAM can get and what damage it can potentially do to the Internet and E-Commerce.

Severe penalties must be inflicted upon those who engage in such practices as SPAM. These need negotiation on an International level, as well as applying locally. Thought has to be given to making more aspects of the legislation extra-territorial in this regard, especially in relation to recovering damages from those persons responsible who reside overseas.

Finally, as most of those who send SPAM would fall within the definition of Small Business used in the Bill, these exemptions for small business need removal. Compliance costs for such businesses are not at all great providing the only have to comply with the minimum standards and not develop their own individual 'codes of practice' and that the legislation does not apply retrospectively to archived material.

SUBMISSION TO HOUSE OF REPRESENATIVES STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS REGARDING THE:

INQUIRY INTO PRIVACY AMENDMENT (Private Sector) Bill 2000

Firstly, the National Party Communications and Information Technology Policy Committee (the Committee) must congratulate the Government and in particular the Attorney-General and his Departments, particularly the Office of the Privacy Commissioner, for the splendid work that has been done in preparing this bill - *The Privacy Amendment (Private Sector) Bill 2000*.

The National Party Communications and Information Technology Policy Committee consists of a small core of party members and a large number of senior expert persons from the various aspects of the communications industries. All members and advisors donate their time and expertise. There are also sub-committees that investigate particular aspects of the industry such as privacy or censorship.

The Committee first proposed an extension to privacy legislation in 1992 and following close working with key players around the world, particularly in the European Union nations and the United States of America, drew up a policy document dealing with *privacy* and the individual in the *Information Age* in 1994. This became a policy of the Coalition's Communications Committee and it was very pleasing to the Committee when the Federal Coalition at the 1996 Federal Election proposed such a privacy policy. This legislation now before the House and the subject of this Committee of Inquiry is the result of that election promise. It is very similar to the Committee's proposed policy, almost in its entirety.

INTRODUCTION

1. The Privacy Amendment (Private Sector) Bill 2000 (the Bill) is arguably the most important item of business the Australian Parliament has ever discussed as he it will affect the lives of ALL Australians for generations to come. If key areas not correct from the start, they will be very difficult to correct at a later date: Pandora's box will have been opened. It is for this reason this Committee is taking the unusual step of presenting this submission to this inquiry.

2. At times, simply one or two words can be the difference between successful and disastrous legislation. Unfortunately, that is the case in point here.

3. The Committee is of the view that the problem has been caused by a lack of a very detailed technical knowledge of the workings of the Internet rather than a deliberate attempt to permit Direct Marketing businesses to pass on their advertising costs to ALL consumers, rather than just their customers.

THE MAJOR PROBLEM WITH THE PROPOSED LEGISLATION
National Privacy Principle 2.1 (c)

"OPT IN" VERSUS "OPT OUT"

4. The Committee's initial policy document proposed an "opt in" principle for all electronic direct marketing contacts. This legislation proposes and "opt out" principle in *National Privacy Principle 2.1 (c).*

5. The conceptual difference is merely one word, however the consequential difference is a complete change to the basic structure of marketing in Australia and elsewhere. By choosing an "opt out" principle in this Bill as the minimum standard, the Government is saying to all businesses and others - it is legal to pass your advertising costs on to ALL Australians, and even residents of other countries, whether they are customers or not and whether they want to receive advice regarding your products or services or not. This is an entirely new concept at law.

6. Such a marketing strategy being legalised is a bonus for direct marketers, but a disaster for ALL Australians, and people of other nations, who have to bear the cost of those direct marketers' advertising, whether they want to or not.

7. The problem has arisen because of the laudable desire to make the legislation technologically neutral, something the Committee's original document was not.

THE CURRENT SITUATION WITH DIRECT MARKETING

8. Direct marketing comes in two flavours, information and contact that costs you nothing but time to deal with – letterbox drops and telemarketing – and the other that costs the recipient money to receive – E-mails and facsimiles.

9. Currently, an "opt out" principle exists for telemarketing and letterbox deliveries. You register with the Direct Marketing Association the fact you do not wish contact or place "No Junk Mail" notices on your letterbox. This registration currently lasts only two years. Unfortunately, not all organisations respect your wishes and registration only applies to organisations that are members of the Direct Marketing Association.

10. The Committee believes that no person should be compelled to pay to receive something before knowing what it is. Unfortunately, this is precisely what an "opt out" principle results in when it is applied to electronic forms of communication such as E-mails and facsimiles. It is impossible to know what you are paying to receive before you receive it.

11. The Committee knows of one rural Queenslander who received a 2Mb junk E-mail over an STD phone line. That would have cost the lady in question around 50c for the E-mail, plus the STD phone charges for the hour or more it took to download on a slow rural Internet link. Why should she be forced to pay around $2 to receive advertising she does not want? True, this is an extreme example, but on average, it would cost around 0.4c for each junk E-mail (SPAM) received based on bulk

download charges of 20c a megabyte (built into your ISP charges) plus any phone line charges. Many people are already receiving over ten pieces of SPAM a day. Likewise, faxes cost you, paper, ink and electricity to receive. It is for these reasons the Committee proposed an "opt in" principle for electronic communications.

WHAT THE BILL PROPOSES

12. The Bill's drafters did not wish to change the current standards for Direct Marketing. They also wanted the legislation technological neutral. The result was *National Privacy Principle 2 - Use and Disclosure, 2.1(*c*)*, which unfortunately sets the minimum standard at "opting out" and also says it is acceptable for direct marketers to contact everybody once off, even if it costs those people money to receive that unwanted first contact. See sub-clause (iv).

> **2. Use and disclosure**
>
> 2.1 An organization must not use or disclose personal information about an individual for a purpose (the secondary purpose) other that the primary purpose of collection unless:
>
> **…**
>
> (c) if the information is not sensitive information and the use of the information is for the secondary purposes of direct marketing:
>
> (i) it is impractical for the organization to seek the individuals consent before that particular use; and
>
> (ii) the organization will not charge the individual for giving effect to a request by the individual to the organization not to receive direct market communications; and
>
> (iii) the individual has not made a request to the organization not to receive direct marketing communications; and
>
> (iv) **the organization gives the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications;** or

WHY THIS IS THE WRONG CHOICE (briefly)

13. As it currently stands, this principle is totally unacceptable as it means a person is forced to pay to receive unwanted communications, even if it is only once. These costs were referred to in paragraph 11 above.

14. Currently an organization or person cannot send mail without paying the postage beforehand. If letters are inadvertently postage without a stamp or incorrect postage the sender is expected to pay the postage after being notified, or the receiver can be asked to pay the postage difference, if they wish to take delivery of the article. In practice, Australia Post rarely recovers these costs.

15. Likewise, a phone call cannot be made without the payment of the required fee beforehand, either at a pay phone or on the subscriber's meter. True, a person can be asked to accept a reverse call charge, but they are given this option first, before the connection is made and knowing who is calling.

16. Thus, even with the existing "opt out" principle, the recipient does not bear the costs of receipt unless he chooses to in the above exceptional cases. However, not only does the proposed legislation have the minimum standard say it is legal to make people pay first, it also in effect reduces the existing current standards for mail and phone calls. The Committee definitely does not think the drafters intended that to be the case!

17. Unless this error is corrected, it will mean the use of SPAM E-mails will increase dramatically costing ALL Australians more for their Internet connections and hindering the development of the Internet as a place where commerce is conducted.

18. **It will in fact hinder Direct Marketing rather than help it as ISPs block more sites and prospective customers refuse to deal with companies that use this form of marketing.**

THE COMMITTEE'S PROPOSED SOLUTION

19. This major problem with the legislation is very easily corrected by the insertion of one new sub-clause in *National Privacy Principle 2.1(c).*

20. After sub-clause (iii) insert a new sub-clause (iv)

> **"(iv) there is no monetary cost to the individual, either directly or indirectly within their communication package, to receive the initial communication from the organisation; and"**

and then renumber existing sub-clause (iv) to sub-clause (v).

21. This solution preserves the technology neutrality of the Bill, does not lessen the existing standards, and ensures the direct costs of a marketers advertising are not shifted from the vendor to ultimately all Australians.

22. Full details of why all Australians are affected, how the Internet works and costs apportioned, and why the legislation as it stands will destroy E-Commerce rather than help it, are set out in the argument attached.

23. This is one area where once a policy is instigated, it will be very hard to reverse, as the government of the United States of America is now finding out.

OTHER PROBLEM AREAS

A. Scope of the legislation – The minimum *National Privacy Principles* (NPP) should apply to everyone. Small business should not be exempted by *clause 16D.*
B. NPP 6.4 to NPP 6.6 make it possible for organisations to opt out of providing and correcting information.
C. *Nobreached* situations in 6B Breach of an approved privacy code.
D. C*lause 13D* practices outside Australia.
E. Penalties

A. Scope of Legislation

24. The Committee does not believe that requiring small business (under $3million turnover) to comply will place an onerous compliance cost upon them as long as archived material does not have to comply until it is re-activated. Most businesses today used computer for record keeping in any case. It is simply a matter of ensuring all records are kept safe and secure.

25. There will be very few small businesses that do not have sensitive information of one kind or another on customers, even if it be only credit account or banking details, therefore it makes sense to require all to abide by at least the minimum principles. There should be no need for every small business to develop an individual "Code of Practice", if this approach is followed

26. Further, it is mainly those types of small businesses that are proposed being exempted by the legislation that currently abuse their trust by on-selling customer lists, sending SPAM E-mails and junk facsimiles. Large respectable corporations do not market through SPAM and junk facsimiles usually, as they know this is very counter productive in the long term. Many small businesses starting out use these methods, particularly E-mails, because it costs them nothing to advertise and they have no existing customer base: they can only increase from nothing. They see it as a cheap method of start up and advertising.

B. NPPs 6.4 to 6.6

27. These principles are a problem area as they cover access to information and correction of information.

28. NPP 6.4 says the charges for information must not be excessive. Who determines what is excessive? In general, if an organisation is going to keep information on a person they must be prepared to supply it upon request. How do you calculate the costs involved? Do you charge for time for retrieval? Do you charge for copying? All these and more are possible charges that are not adequately covered in this principle as it is.

29. The Committee is of the view that there should be no charges for accessing personal information up to the statutory seven-year period, providing the inquirer has not already been given full access to all the information on a previous occasion. Neither should there be a charge for access to ensure records have been changed as requested. Should the inquirer wish to take away copies of the information, then a reasonable

photocopying charge, comparable with commercial copying centre charges, should be able to be levied per page copied. (Likewise, any postage charges.)

30. NPP 6.4 should reflect the above in its wording. Unless it does, the Committee feels there will be too much variation between each of 'Code of Practice' and consumers will never be certain of their rights. Simplicity is what should be being aimed for, not complexity.

31. NPPs 6.5 and 6.6 both fall short in that "reasonable steps" is not defined. As worded the clauses are ambiguous. The Committee believes that this means there is a let out for the organisation – "It's too costly or difficult to change, so we won't do so". They could claim that the expense/time makes it unreasonable to change the information. This is not what the drafters intended surely. What is intended is that the organization should take all reasonable steps to correct or append information.

32. Perhaps a better wording would be that "the organization must correct / append the information unless they can clearly demonstrate doing so would be too onerous a task".

C. No breached situations Clause 6B4 and
D. 13D Overseas Act required by foreign law.

33. This is an area of some concern to the Committee regarding matters outside Australia. Several countries, including the United States of America and even Australia already make extra-territorial laws under certain circumstances. There is probably no easy solution here other than to ensure that adequate safeguards are in NPP 9 and that businesses do not deal with countries that do not provide such safeguards, or operate in countries that are likely to use what in effect is a loophole, in an unintended manner.

34. The Committee envisages that some small insignificant country could legislate in such a manner that organisations must disclose certain sensitive information about all their clients to do business in such previously mentioned country. That country could then in effect set itself up as an information exchange earning a license fee from businesses operating in that country, so those businesses can exchange information outside of the laws of Australia and other nations.

35. Is there a way to protect Australian data from such a situation? Activities under these clauses must be closely monitored. It would be preferable to have further restrictions placed in them such as "and the Australian Government has specifically authorised the release of the information through treaties or other means."

36. The Committee believes this is not an unreasonable approach to take in light of the globalisation of law the Internet is bringing about as the planet heads towards more international co-operation in law making. *Information Exchange Treaties* already exist in various forms – Interpol, Intelligence Services, etc. Perhaps the scope of these should be broadened to include other aspects of information to compliment NPP 9.

E. Penalties

37. The whole concept of penalties in the Bill must be examined closely to ensure they are adequate and DO discourage the committing of offences under the Bill. In particular, there must be significant penalties for breaching NPP 2.1(c) as some forms of electronic abuse can cost the Internet industry millions, if not billions, of dollars world-wide.

38. The recent "I love you" virus is a good example of the damage that can be done under NPP 2.1 (c). Most SPAM E-mails use very similar methods of dissemination to reach their targets as the "I Love You" virus.

39. The matter of penalties is covered in more detail in the "Detailed Argument" section.

OTHER AREAS THAT NEED COVERING IF NOT ALREADY ADEQUATELY COVERED BY THE PROPOSED BILL

40. There are other specific areas that are related to privacy issues, which must be adequately addressed to ensure the privacy protection package provided by the Government is complete.

    (a) Information held on computer equipment repossessed or otherwise legally seized from the user of the equipment, must be protected from being accessed without the owners permission. The Committee believes the Bill covers this, but this should be carefully checked by the Inquiry to ensure it is.

    (b) Storage of information obtained from caller ID on phones must be regulated. One of the major selling points of caller ID to businesses is the ability to store caller details. This practice can have both pros and cons. The main problems arise when wrong numbers are dialled or the person using the phone is not the owner of the line. Probably adequately covered indirectly, but not directly addressed. NPP 1 does cover this but perhaps specific reference could be made to this practice in the notes.

    (c) Use of automated dialling equipment to hack systems and for telemarketing purposes. Possibly not within the scope of the bill, but is important since it is by using such equipment information can be illegally acquired and telemarketers contact people with "silent" numbers or who have requested no telemarketing contact. Again perhaps another note reference but attached to which principle – NPP 2.1?

    (d) Use of computer programs to gather information from other computers without the owner's of the information permissions is a serious crime as well as a privacy breach. It is very hard to guarantee information security if a computer is even only temporarily on a network. The responsibility is on the owner of the database to keep it secure, but there should be penalties for people who do breach this security. There is no such thing as a totally secure computer, especially if it is connected to the Internet even briefly. This Bill?

    (e) Forging of e-mail addresses and domains. Possibly not within the scope of the bill. It is however, a way in which spammers hide their sending address while still ensuring their message arrives safely at the unsuspecting recipient's computer. Such actions would breach the NPP 2.1 (c).

DETAILED ARGUMENT SUPPORTING THE COMMITTEE'S PROPOSED CHANGES

41. The National Party Communications and Information Technology Policy Committee consists of a small core of party members and a large number of senior expert persons from the various aspects of the communications industries. All members and advisors donate their time and expertise. There are also sub-committees that investigate particular aspects of the industry such as privacy or censorship. The consensus of the Committee is that communications should be apolitical in most of its aspects and accordingly advice is taken from all persons and organisations of all political views. This even includes the various unions involved. Several of those organisations have made separate submissions to this inquiry.

42. Privacy is the area the Committee views as needing to be apolitical to the greatest extreme in a democracy. The critical operant is the protection of freedom and rights of the individual balanced against the needs of government and industry. A solution must be reached that successful finds this balance point. Once this balance point is defined, in the context of a democracy, it will be impossible to modify it to any degree at a later date.

43. The Committee's Privacy policy was drawn up after consultation with advisors from around the world via the Internet and other forums such as international conferences. A comparison of views will show that there is almost unanimous thought world wide on the issues that need to be addressed and how the desired outcome is best achieved. This current Bill, the subject of this inquiry, is proof of that statement in itself. It is only in certain areas that there is a significant division in opinions. Other variations in opinion are caused by the benefits of hindsight.

44. The Committee strongly believes that earlier decisions made in other countries should not simply be blindly followed, if hindsight already shows such decisions have failed or are significantly harming the desired outcomes. It is for this reason that the Committee has made this submission to this Committee of Inquiry, in the hope that Australia will not make the same mistakes that the United States of America, in particular, has made regarding the Internet and the legalisation of Direct Marketers using SPAM

WHY NATIONAL PRIVACY PRINCIPLE 2.1(c) MUST BE MODIFIED

45. The United States of America is to the forefront in development of the Internet and its use, and thus has experienced the associated problems much earlier than other countries. Unfortunately, in the area of Privacy legislation, it is a long way behind other countries such as Australia.

46. One negative aspect of modern living is the fact that technology is now changing so fast, that legislation cannot keep up with mankind's progress. This is particularly the case with the Internet. This means law makers must approach the problem of control

and regulation of society from an entirely new angle. The drafters of this Bill have fully realised this fact and have made it technology neutral.

47. The American Government is yet to fully realise the benefits of technology neutrality and the implications for law making it brings. They are still trying to legislate for particular instances rather than in broad principles. This is particularly true with regard to the Internet.

48. Therefore, America should not be used as a model for this legislation for two reasons – lack of comparable legislation and its piecemeal approach to problems.

49. Unfortunately, it appears that the views of Direct Marketers as espoused in America, have filtered through into this legislation as a result of the drafters not fully appreciating the significance of the wording of NPP 2.3 (c) when it is applied to certain forms of communications i.e. E-mail, and to a lesser degree, facsimiles.

E- COMMERCE

50. Like America, Australia has recognised the enormous benefits E-Commerce can bring. These benefits will only eventuate however, if E-Commerce is not unduly hindered.

51. This is clearly recognised by the drafters of the Bill in the *Explanatory Memorandum* to the Bill.

> "Many potential misuses can impose a direct cost on the consumer. Spam email and direct marketing via bulk facsimile transmission are examples. If the transfer of an individuals email address or fax number (along with other information such as purchasing habits) results in that person receiving unsolicited communications, the nature of email and fax as a form of communication means that the cost of delivery will be largely born by the recipient. This is also the case with consumers cost in contacting the organization to request no further communications. ***Australian businesses may be more likely to initiate such practices in a self-regulatory framework.*** **[My emphasis]."**

52. "May be more likely" is really understating the problem! The American practice has shown that businesses WILL initiate such practices. Already such practices are occurring in Australia with several businesses sending facsimiles and SPAM. An example of a facsimile from a constant offending business in Victoria and that apparently ignores all requests for removal from its fax list is attached.

BILL ON CORRECT COURSE BUT!

53. The Committee fully endorses the approach to Privacy taken in the proposed Bill in principle: legislation and regulation should be the absolute minimum required to lessen red tape for business and keep compliance costs down.

54. Having said all that, in some cases the minimum standards require an initial higher benchmark because of the structure of the industry in question. The Direct Marketing Industry, and related marketing areas, is one such industry where higher initial benchmarks are required, rather than a lowering of existing ones. Australia cannot afford to wait and see if marketers will abuse a lowering of the standards: the American experience has already shown they will.

EXISTING BENCHMARKS WILL BE LOWERED BY NPP 2.1 (c) (as currently proposed by Bill.)

55. The existing restrictions on direct marketing are far more stringent than those proposed by this Bill. Currently it is not legal to make people pay to receive telemarketing phone calls, people have to agree to accept the reverse charges first, nor is it legal to send mail without a stamp – a tax is imposed on the sender and the recipient, if that person agrees to accept the mail item.

56. The proposed principle actually "implies" it will be legal to market in that manner, if an organisation is foolish enough to so do. It is essential therefore, that principle 2.1 (c) does not lower the existing standard but makes all communications meet the current existing standard at least. There is nothing in the Bill that says organizations MUST use higher standards than the minimum one stated in the Bill.

WHAT THE UNITED STATES OF AMERICA DID

57. In fact, in the guise of promoting E-Commerce the direct marketing lobby in America succeeded in having Congress legislate to allow direct markers the legal right to send out their SPAM to prospective customers once, providing they are given the option to opt out of further communications.

58. This unthought through policy has proved to be an unmitigated disaster that has seriously damaged the expansion of E-Commerce rather than helped it. Individual sites are being blocked by individuals and ISPs.

59. Internet Service Providers (ISPs) who permit spammers to use their facilities are also being blocked all because of the huge growth in SPAM resulting from the legalising of it in the United States of America. It now costs ISPs millions of dollars annually just to carry this traffic and it slows down the entire Internet speed for legitimate users. What further infuriates users is that the senders proudly state that you are being SPAMMED under US law, so you can do nothing about it. [Ha! Ha! Usually implied by the tone of the message.] This is spawning a very large anti-US movement on the Internet – the view is what right does the US Government have to say that it is legal for their citizens to steal from citizens outside of their territorial borders.

60. This is in reality theft, since people all over the world are being forced to pay for E-mails that in many cases have no relevance to them or their country, simply because the US Government has said such a practice is satisfactory in the US. No wonder such an anti-US feeling is developing on the Internet. **Do we want a similar backlash against Australia?**

61. The emails received below are indicative of the new industry that has sprung up in the US as a direct result of using an "opt out" principle for electronic direct marketing. These probably are international in reach. These senders use programs and other methods to compile email lists they then on-sell. I never subscribed to their lists or visited their sites, yet like most other members of the Australian Public Access Network Association Inc. (APANA), their junk E-mail was received. Many compliers use "sniffer" programs to visit web-sites and unprotected computer networks to steal

E-mail lists or use them to on-send copies from their computer using the sending addresses of their "temporary computer". Rapid advances in technologies mean it is extremely difficult for many organisations to keep their information always secure: even not having the information directly on-line does not guarantee complete security.

62. The recent "I Love you" virus which has caused billions of dollars damage to computer networks world wide uses EXACTLY the same methods of propagation as many SPAM E-mails. The only difference is that instead of just on sending to those on E-mail address lists, it does damage to the computer's programs as well.

Subject: **work related**

Date: **Sun, 26 Mar 2000 12:59:21 -0800**

From: **emailcd44@mail.com**

Reply-To: **sample@whynot.net**

To: **wexin@gfunk.com**

The all new exclusive Y2K highly targeted E-mail address cd volume #7 To mantain the quality of our lists only 50 copies of each volume are released to the public. There are only 27 copies left, and if you order within the next 24 hours you will get up to 40% off. Or If you are looking for quality bulk email service we provide many options.

Please choose a click on a link below.

http://EBlasts.homestead.com/

OR

http://CDPROMO.homestead.com/

NB the "to" and "from" addresses are forged / non traceable. You have to go to the "link" URL to actually order. This then captures more of your personal details via cookies and such and confirms your email address as authentic, if your browser is set up in the manner most people unwittingly do.

63. Forging addresses is done so that the message gets through but it is difficult to trace its origin and thus block in the future. Spammers regularly change addresses so a person cannot block them. A message has to be received once from an address before it can be blocked in the future.

64. Here is another example that illustrates the abuse of current US legislation by spammers (see bold portion at end). Previous legislation was also abused.

Subject: Just open and you'll see

Date: 29 Mar 00 2:43:38 AM

To: undisclosed-recipients:;

Tired of working for someone else and getting paid what "they" feel you're worth?

Tired of the "get-rich-quick" $5 fantasy programs?

Tired of the MLM "dream scene"?

Are you looking for a legitimate home-based enterprise that can generate you $10k - $20k + monthly?

THEN PLEASE CALL THIS TOLL FREE NUMBER 800-320-9895 EXT 7855

.THEN PLEASE CALL THIS TOLL FREE NUMBER 800-320-9895 EXT 7855

80% profit on all sales that pay you from $1250 - $6250 per sale

No personal selling or "convince me" tactics involved

No special skills or equipment required or "inventory" to keep

Complete information system in place does the explaining for you
FREE-enterprise in its purest form, not MLM or franchise
Full training and support in an environment of utmost integrity
Exceptional products, not "vitamins, lotions, and potions"
Lead generation system that brings qualified prospects to you
Multiple 6 figure income realistically attainable in the 1st year
3 year retirement program.....PERIOD!

This program is all about money....how to make it,
how to keep it, and how to make it work for you.
The call is FREE and there is absolutely no obligation
so what do you have to lose?

CALL TOLL FREE 1-800-320-9895 EXT. 7855
CALL TOLL FREE 1-800-320-9895 EXT. 7855
Please, serious inquires only. Thank you

==========

Under Bill s.1618 TITLE III passed by the 105th U.S. Congress
this letter can not be considered unsolicted e-mail as long as you are
on our opt-out list and we include**: Contact information & a Remove Link**
To be removed from future mailings please reply to:
demandfuture@yahoo.com
Marketed by UMG
umgmarketing@yahoo.com

65. Most of the organisations who send this type of E-mail would be exempted under the proposed clause 16D as they would be small businesses with under $3 million turnover, if they actually declare turnover. Many such people also have the removal via a 1900 style number! That is where they make the money from, they hope, as people phone in to be removed by a process that can involve transferring the call to international numbers and endless recorded messages, all being listened to at the consumers cost!

COMMITTEE NOT AGAINST DIRECT MARKETERS

66. It is not the intention of the Committee that direct marketing activities should be curtailed or electronic commerce hindered in any manner. In fact, as is explained below, unless what the committee suggests is implemented, electronic commerce will be seriously endangered, as people and ISPs will block more and more sites, as well as individuals, to stop receiving the unwanted SPAM that costs senders nothing, ISPs money to carry and recipients money to receive.

67. Rather than promote E-Commerce, this principle of "opting out" of receipt of junk electronic mail (faxes / E-mail) will in fact hinder its development as more and more

people take exception to its use. The Privacy Commissioner himself states this view on his web-site in " PRIVACY: IT and Internet privacy issues" .

68. The committee accepts advertisers have the right to contact prospective customers, providing there is no initial cost to those contacted. Once there is a cost involved, people will object strongly. Legitimate Direct Marketing organizations know this, but many "cowboy" type operations do not care and bring the whole industry into disrepute as a direct result.

WHY MINIMAL APPROACH WITH INDUSTRY CODES WILL NOT WORK WITH NPP 2.1(c)

69. Before proceeding further, the Committee stresses that the majority of businesses and marketers DO comply with industry "codes of practice" as they currently exist. Unfortunately, a large number of businesses are not members of those marketing associations and many regularly break those codes: there is currently no legal recourse for consumers when those codes are broken.

70. It is realised that the Bill does address this problem by having the NPPs apply where no industry code exists.

71. While not having "Codes of Practice" approved at the parliamentary level but simply registered under the proposed Bill, providing they meet at least the minimum standards, means they can be more flexible, it could lead to decisions being made which are contrary to the best interests of the population under certain circumstances. Bureaucratic rule is not always the best option in these cases, although the Committee accepts that is the best course of action in this case. However, it believes Parliament should set sufficiently high minimum standards to avoid the American situation occurring in Australia. Once something is permitted to happen, it is very difficult to then curtail that activity as the American experience shows.

72. It is for these reason that the Committee is of the view that it should be stated clearly in the guidelines (NPP 2.1 (c)) from the outset, that any blind (or other) direct marketing, by electronic form or otherwise, that costs the recipient money to receive, without the consumer FIRST requesting the same, should be banned. New sub-clause

> **"(iv) there is no monetary cost to the individual, either directly or indirectly within their communication package, to receive the initial communication from the organisation; and"**

73. The wording includes " directly" or " indirectly" because some ISPs charge per E-mail, some charge per megabyte downloaded, others charge an all-up fee that is calculated in a manner than includes such costs, while others charge in various combinations of these.

REASONS NEW SUB-CLAUSE (iv) NEEDED:

74. New sub-clause (iv) is needed because:

(a) It is not acceptable that people should pay even ONCE to receive communications they do not want. (This does NOT apply to official communications from Government and similar agencies). Ask the lady who received a 2Mb junk E-mail over a community area phone connection. The cost of receiving that would have been well over $2.00 in total with download time telephone charges and built in ISP volume charge.

(b) Industry developed codes will not necessarily stop this happening unless those codes specifically state you must "opt-in" to mail lists that cost money to receive or sub-clause (iv) above is included in the minimum NPP 2.1 (c) standard. In addition, there has to be meaningful penalties for breaching the code.

(c) Existing codes regarding telemarketing do NOT work. People are still pestered by telemarketers despite requesting otherwise AND having unlisted numbers.

(d) The proposed "opt-in" code for Internet Providers as proposed by their association will not work as spammers mostly 'hit and run'. The majority of "law biding" businesses will comply with the code. Most well-known and large businesses already work on an "opt-in" basis, not an "opt out" one for E-mails and facsimiles.

(e) Another problem with the Internet code is that most spammers currently use hotmail or yahoo accounts or the like – difficult/impossible for an ISP to enforce a code on them, or relay through other people's accounts. By the time the ISP is aware of the problem, they have long gone and changed ISPs or account details.

(f) This Internet code will NOT cover junk faxes, which now are being used increasingly, especially by charity groups, to make people share the costs of receiving their message. (Computer faxing makes this very easy). Many object strongly to involuntarily supporting charities they may totally disagree with the aims of, in this manner. See copy of a fax from a persistent offender attached.

ISP COSTINGS - HOW IT WORKS

75. All costing on the Internet is based on volume charging at some point in time. These charges are levied on the traffic to your computer or an ISPs server. Charges are calculated on the Megabyte volume downloaded, although some large ISPs also have upload charges from smaller ISPs if sufficient download charges are not met.

76. The overall result is that the point of arrival of information is where the charge is levied, not the point of sending. i.e. the Recipient pays. The charging is more complex however, as a charge is levied at each ISP / server along the route, that the information

passes through. This could be ten, twenty or more points between the sender and receiver.

77. Thus, it can be seen that it costs the sender nothing, but everyone else in the chain money to receive the information in question. If a message is self-replicating as well, these charges multiply as it goes. Even a single E-mail sent to a set mailing list, still costs the sender nothing, but everyone money and more importantly, bandwidth.

78. There is only a finite amount of traffic that can be carried on any Internet connection, whether it is a transpacific cable, satellite links, or your own phone line. Once the amount of traffic reaches a certain level, the speed of the connection falls off dramatically, and eventually the connection fails completely. i.e. the network crashes. The only way this can be alleviated is by increasing circuit capacity. i.e. bandwidth. This costs money that has to be passed on to consumers. SPAM unnecessarily uses bandwidth, especially when it in the form of "I Love You", and slows down the whole network for legitimate users. Unless the use of SPAM is curbed, increasing bandwidth will become too costly for the return and the intended use of the Internet for E-Commerce, will wither and die through congestion, just as happens on our roads today. There is a finite limit to the number of freeways that can be constructed, even on the Internet!

SMALL ISPs WILL BE SENT OUT OF BUSINESS

79. The huge costs of dealing with SPAM means that many small ISPs, especially in regional and rural areas, will be driven out of business. Their connection charges will become uncompetitive. Only two or three large players will eventually survive, as they alone will have the capital needed to upgrade to deal with SPAM, unless it is regulated from the beginning.

COMPENSATION TO ISPs FOR DEALING WITH SPAM

80. ISPs must be given the powers to "fine" those who send unsolicited direct mail for the privilege and more importantly, ISPs along the route the power to recover damages from offenders, through connection charges / billing accounts, etc. The Committee does not believe any code, which simply disconnects offenders, sufficient. By the time they are disconnected the damage has been done. Legislation is required to give any penalties levied the full backing of the law.

81. Further, many businesses (mainly new or emerging) now forge sending addresses when sending SPAM thus avoiding the backlash from recipients (and the cost of receiving these bounces and complaints) – the bounced mail and complaints are directed to completely innocent parties. This often causes the ISP's systems (and others on line) receiving these messages to crash from overloading of the system. Most of these people are now based in America, where "opt-out" SPAM is legal. They hide behind this fact. Many of these people also are operating frauds whereby you must phone a phone number to be removed. Of course, it is usually a 1900 style number that costs several dollars a minute, not a toll-free one! Recently, one such email promoting an on-line casino in California using forged apana domain sending addresses completely crippled APANA's operation for two days with bounced emails from people with SPAM blocks and complaints.

82. Such people cannot be prosecuted, in the US, because the American Government has said it is okay to send junk e-mail on an "opt out" basis similar to this proposed legislation. These spammers proudly display the message on the bottom of their e-mails stating this. The result is that many ISPs now block whole sites to avoid these problems as on average it costs ISPs around $7 million each yearly to deal with the problem. If this trend continues, E-commerce will be completely stifled.

83. Blocking whole sites or even ISPs who refuse to take action against spammers has a serious negative effect. It means many legitimate users are denied access to information on those sites because of the actions of spammers. After one recent SPAM / Mail bombing attack on APANA in Brisbane, a large phone company / ISP had to be blocked for several days before they would take action against the spammer. They ignored E-mail requests to take action, and it was only when millions of E-mails bounced back to their server with the consequential detrimental effect, did they take notice of the problem and rectify it. Thus, it is not only spammers who do the wrong thing, but also some large ISPs.

84. Thus while it might be alright to say we take the absolute minimal approach regarding privacy and let the industry groups decide higher standards, this assumes everyone in the industry, including non-members of the industry governing bodies, will comply. Experience in Australia with direct marketing has already shown that not to be the case, and the American experience has shown that it is definitely not the case with E-mails under similar laws to this one proposed.

WHO ARBITRATES BETWEEN CONFLICTING CODES

ISP code verses Direct Marketer Code

85. It is all very good to let the industry self-regulate, but there will be two industries at loggerheads over this issue – the Internet Industry versus direct marketers.

86. The Government must take the lead and set the benchmark higher, or at least at the same standard that already applies to telephone services and postal services, with regard to direct marketing material that costs the recipient money to receive.

E-POSTAGE – A SOLUTION?

87. The situation in America has now reached such chaos because of SPAM that a Bill to promote E-Postage is before Congress.

88. Because direct marketers have abandoned the traditional methods of direct marketing in favour of E-mail, as all the costs are born by the recipient, not the sender, the US Postal Service has noticed a marked decline in income.

89. While some say this decline in income is because individuals send E-mail more than postal mail now, this statement is most likely false. People send E-mail in far greater quantities than they ever did postal mail. In reality, the Committee believes E-mail is tending to replace the telephone as a form of communications, more than it is postal

mail. This is an area that requires careful research before any clear trend can be identified.

90. Nevertheless, the Bill before Congress is suggesting that a postage fee be paid on all E-mails to recover revenue loss and possibly as a measure to curb SPAM. Such a move is doomed to fail because of the nature of the Internet. You will still be able to send millions of E-mails for the cost of one E-mail. Refer to paragraphs 73 to 75 above.

ALTERNATIVE APPROACHES FOR DIRECT MARKETING NOT USING "OPT OUT" ONCE –OFF E-MAILS

91. There are ample other means open to marketers on the Internet:
    (a) Take out web advertising on often used web-pages. The advertiser would pay for the costs and interested clients then subscribe to their lists knowing what they are paying for.
    (b) Advertise in newspapers, magazines, on radio, TV, Web-TV, etc.
    (c) Drop leaflets in letterboxes.
    (d) Word of mouth.
    (e) Include advertising with other products sold e.g. on program CDs.
    (f) Use one of the free ISP services that include advertising as a requirement to obtain the free services.

92. There are no doubt several other options as well which do NOT shift the direct cost of advertising from the vendor to the purchaser, as Principle 2.1(c) does in its current form. There are no valid reasons why any marketer should be permitted by law to make everybody, even people who will never be a customer, pay to receive its advertising, that the marketer pays nothing to send. Let Australia not copy the United State's erroneous way in this regard.

PENALTIES

93. The Government must give the Internet industry (and consumers) a chance to recoup costs when the NPPs or registered Codes are broken. To a degree, the Bill does this through its access to the court system.

94. However, this can be expensive even at the Magistrates Court level. Set penalties for certain offences should be significant and clearly spelt out within the Bill to avoid the necessity to take court action. The power of determination should rest with the Privacy Commissioner who can impose penalties for breaches of certain codes or NPPs.

95. The sending of SPAM (and junk facsimiles to a lessor extent) is one of the main areas where such arbitrary power should exist. Currently a consumer or an Internet Service Provider would have to pursue the defendant through the court system to recover costs of carrying SPAM from a defendant.

96. There are no grey areas of law with regard to SPAM. It is very clearly identifiable by both receivers and ISPs. One single message can become millions of messages. These use up enormous bandwidth on the Internet, which costs the ISP money in both volume charges and extra capital outlay in equipment to carry. In addition, in some cases several ISPs' networks may be crashed by the SPAM in question. Downtime and repairs can again cost the ISP money. Pacific Bell had repair costs of around US$500,000 in March 1998 through three pieces of SPAM being sent simultaneously. The "I Love you" message is costing billions worldwide. These costs have to be passed on to ALL consumers through increased connection costs, or the ISP goes out of business.

97. Penalties imposed must be significant to deter spammers from what in effect is criminal activity [theft] (except in US where it is partially sanctioned). Principle 2.1 (c) as proposed by this Bill, would also sanction it. Further, these penalties must not only apply to local companies, something that is quite easy to accomplish, but also must be able to be collected from spammers located outside of Australia's jurisdiction.

98. In reality, this penalty regime would need to be worked out with the international ISP Industry and foreign governments since it crosses national boundaries. Perhaps like in the United States (and already in Australia for some crimes by Australians), it could be agreed that a prosecution be able to take place in Australia for this type of crime committed outside our borders against Australian businesses and residents. International treaties should be negotiated along the lines of existing extradition treaties or perhaps an international sanctions regime could be developed against countries that do not take action against offenders in their jurisdiction.

99. This Bill at least needs to specifically cover offences committed within Australia first, with the ability to expand internationally as such expansion becomes possible! Monies raised from the fines could be then apportioned between the ISPs according to their market share, thus returning the damages collected to those affected by spammers' actions.

CONCLUSION

100. The bottom line is that the American government made a serious error in its legislation – "opt out" rather than "opt-in" for E-mails and now the world is suffering. It has done considerable harm to the American ISP industry through added costs and the fact many sites and even providers are now blocked by people not wanting to receive SPAM. It has also spawned a large anti-US movement on the Internet. Many sites and ISPs are now have access blocked and messages from them are bounced, thus denying people useful information that could be located on them.

101. The Committee does not wish the same to happen in Australia and to Australia sites. Why run the risk when all that is needed is a benchmark for all direct marketing in keeping with the current standard – Stress in principle 2.1 (c) it is illegal to send communications that cost the recipient money to receive. New sub-clause -

"(iv) there is no monetary cost to the individual, either directly or indirectly within their communication package, to receive the initial communication from the organisation; and"

102. At present it is illegal to make the sender pay to receive communications under existing law regarding phone calls and postal services, so why should the existing law now be relaxed to enable marketers to force people to pay to receive possibly unwanted material, even once.

100. Finally, Meaningful penalties must be imposed on those people who want to send SPAM so that ISP costs are kept to a minimum for all, there will always be adequate bandwidth and E-Commerce will thus prosper, rather than be strangled by those who would prefer to have others bear their cost of advertising.

Thanks to the members of the House of Representatives Standing Committee on Legal and Constitutional Affairs for the opportunity to present the case for ensuring unsolicited Direct Marketing E-Mails, facsimiles are not legalised, and other matters related to the Privacy Amendment (Private Sector) Bill 2000.

Garry R. Ford,
Chairman
National Party
Communications and
Information Technology
Policy Committee

Dated 11 May 2000

OFFENDING FACSIMILE

WorldWideWeb Institute (Australia)

Australia – Canada – USA – Brazil – UK

SUBJECT: FREE 6 Page Web Site Creation and Free Domain Name Registration

If you do not have an Internet Web site presence, or would like to update your existing site, we would like to invite you to take advantage of our special offer of a Free 6 page Web site and Free Domain Registration program. This program includes creating a free website with professional graphics and links, as well as the free registration of an Internet Domain Address (URL) for your exclusive use worldwide. (www.yourcompany.com.au).

This is a genuine offer so we may assign work to our advanced web students from colleges and universities. At WorldWideWeb Institute (Australia) we provide work experience for advanced student designers and programmers in website applications. We have designed sites for thousands of US companies and have underway, hundreds of Australian sites, for companies like yours. We have many reference sites you can look at.

If you register with us early, and are accepted into our free web site program, your Free 6 page web site will contain exciting graphics, text, CGI programming (customised contact order forms) and active links. We work with your existing materials and use our skills to create an online business for you. All work is overseen by professional web designers to ensure quality at all times.

To take advantage of this offer, we ask that you:

1. Give WorldWideWeb Institute Australia and our students, permission to use your web site for our displays and seminars.
2. Host your site on our high-speed servers for a period of at least one year so we can guarantee to our students, an online portfolio and maintain a quality setup for your company.

This offer is limited by the amount of students available. WorldWideWeb Institute (Australia) will not perform services for companies involved with pornography, sex, or other practises deemed as unscrupulous.

Toll Free and No Obligation. Please fax back to **1-800-999-428** and one of our student co-ordinators will ring in the next 2 days. If you are very excited and wish to speak directly, please fax and then ring our office **1-800-999-469**. We look forward to talking with your shortly.

FREE DOMAIN NAME SEARCH – Fill out the Internet address you would like to own. We will check if the name is available for you.
EG. www.yourbusinessname.com.au or www.your-business-name.com.au

#1 www.(_____) #2.www.(_____)
Company Name:_____
Contact Name: _____
Phone: ( )_____ Fax: ( )_____
City/State: _____Best Time to Call you Back: _____

If you don't want to receive our faxes, please write your fax number across the top and refax back to us. Send fax to 1-800-999-428. Thank you.

52-62 Stud Road, Bayswater 3153 Victoria Australia ©WWWI
Phone: 1-800-999-469 Fax: 1-800-999-428
A.C.N. 085 268 999

NATIONAL PARTY COMMUNICATIONS & INFORMATION TECHNOLOGY POLICY COMMITTEE

10 Clifford Street Stafford, 4053 Phone/fax (07) 3857 1203 E-mail - coal_comms_pol@merddyn.apana.org.au

CHAIRMAN: Garry R. Ford, esq.,J.P.,P.G. Dip. A. ,B.A.,B.Ed.,F.R.Hist.S.Q.,M.A.C.E.,M.A.E.T.A.

12 May 2000

The Secretary
House of Representatives Standing Committee
on Legal and Constitutional Affairs
Parliament House
CANBERRA, 2600.

Dear Sir/Madam,

RE: **INQUIRY INTO PRIVACY AMENDMENT (Private Sector) Bill 2000**

Thank you for agreeing to the late acceptance of this submission. It was originally forwarded to Senator Boswell for presentation to the Environment, Communications, Information Technology and Arts Committee, because of an error on the Australian Parliament House website regarding this bill's current progress.

Please find enclosed the submission from the National Party Communications and Information Technology Policy Committee.

Yours faithfully,

Garry R. Ford,
Chairman
National Party Communications and
Information Technology
Policy Committee