



**Symantec Brightmail Software  
Response to Discussion Paper  
Ministry of Economic Development**

**Introduction**

Email is ultimately the killer application of the Internet. Everyone uses email to communicate. Yet email is starting to have problems whether it be spam, or viruses or threats. Protecting the email infrastructure and make it something we can continue to use is critical to users and businesses globally.

Yet it is going to take a four pronged approach to achieve this protection. What is going to be required is that organisations work across the legislative framework to ensure strong laws are in place that can target viruses writers and spammers and make sure that there are significant penalties for them if they continue to commit these kinds of acts.

Technology is also a key component of the solution as the issue in email (and now with instant messaging and short messaging systems) is fundamentally a technology problem. The email protocol and other communications devices were developed without thinking about identity theft, spam, or viruses. They were developed as tools to communicate with people who may be across the city or across the world.

Lastly it's important to educate end-users and help them to understand how they can protect themselves whilst they are online, on email or using communications devices, against some of these threats.

To support any form of legislation, spam firstly needs to be clearly defined as end-users, commercial enterprises and ISPs look at it in different ways. Symantec Brightmail defines spam as Unsolicited Bulk Email. The opposite of "solicited" email that you receive from business associates and personal contacts – or have "Opted-In" to receive from trusted newsletter or business resources.

By commencing with this as the first step to supportive legislation, definitions and requirements can already be undertaken. Regardless of the individual requirements of the legislation, governments must work on a global basis if legislation is to have any impact on reducing spam.

**Background**

**1. Do you consider spam to be an important issue? Has it significantly affected you in any way?**

[see answer below]

**2. Do you think legislation has a role to play alongside other complementary measures?**

With spam levels over 64% and now spam technology now emerging as a way to deliver malicious code, spam is a security threat that is causing significant cost to businesses. The



problem of spam is very real and countries around the globe are looking at ways to safeguard end-users and reduce the level of spam.

Many governments are working or have implemented forms of legislation, but the first step in doing so is to clearly define what spam is, as end-users, commercial enterprises and ISPs look at it in different ways. Symantec Brightmail defines spam as Unsolicited Bulk Email. The opposite of "solicited" email that you receive from business associates and personal contacts – or have "Opted-In" to receive from trusted newsletter or business resources.

By commencing with this as the first step to supportive legislation, definitions and requirements can already be undertaken. Regardless of the individual requirements of the legislation, governments must work on a global basis if legislation is to have any impact on reducing spam.

Although legislation is a very important step in addressing the issue of spam, legislation alone isn't the answer. To mitigate spam, governments and corporations need to deploy a combination of legislation, education, best practices, international co-operation and leading technology.

In doing so, they can ensure that spam levels are reduced and by working across the legislative framework can enforce strong laws that will bring spam writers to justice and alleviate the problem of spam.

### **Existing legal framework**

#### **3. Do you consider existing privacy protections in this area sufficient?**

[see answer below]

#### **4. Do you agree that stand-alone anti-spam legislation is preferable to reliance on the Harassment Act?**

The issue of spam is no longer simply that of a privacy invasion or a form of harassment but one potentially fraudulent and destructive in nature. Spam is now emerging as way to deliver malicious code and this is a security threat, which is causing significant cost to businesses and consumers. Hence the need for stand-alone anti-spam legislation is critical to supporting the reduction of spam on a global basis.

In the past 5 years alone, Identity Theft has cost businesses and consumers US \$60 billion. When you consider 2.25 billion fraudulent messages were sent in February 2004 alone, and identity theft has grown over 79% from June 2002 to June 2003\*, every organisation is open to attack. Privacy and harassment legislation won't support the identification of spammers involved in this type of behaviour and therefore they can't be stopped.

\*According to Gartner



### **Legislative issues**

5. What message mediums should be caught by the legislation (e.g. email, short message services using mobile phones, Internet instant messaging, faxes, telephones (telemarketing), physical mail delivery)?

Symantec Brightmail believes communications methods supported by the Internet including e-mail, short message services and instant messaging, should be covered by the legislation.

6. Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?

Symantec Brightmail does not have a position on this.

7. Should the messages caught by the legislation be of a commercial advertising and promotional nature only or should other types of messages be caught? Should there be exceptions and if so what should be exempted?

Symantec Brightmail does not have a position on this.

8. Should the legislation extend to coverage of acts done overseas? If so, what acts should be covered?

The Australian authorities responsible for the development, implementation and adherence to anti-spam legislation are working on a worldwide basis to sign memorandums of understanding. As spam is a global problem and the majority of spam comes from outside Australia's borders, global agreements will provide law enforcement capabilities across borders and maximise the opportunity to reduce spam levels.

9. Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation? Should there be express exceptions such as for telecommunications companies and ISPs?

Symantec Brightmail does not have a position on this.

### **The consent issue – opt-in or opt-out**

10. Should New Zealand adopt an opt-in, double opt-in or opt-out approach in legislating against spam? Why?

[see answer below]

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

[see answer below]

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



Opt-in legislation based on actual or inferred consent strengthens legislation as opt-out offers a number of potential loopholes. One of the critical elements in reducing spam to a manageable level is the education of end-users. To date, end-users have been advised by government agencies and anti-spam groups not to respond to opt-out clauses, as spammers often use these techniques to confirm the e-mail address is real and will in-turn use this to direct more spam.

Although opt-out is utilised in the US, it was initially decided-upon in the US based on concerns raised by marketing associations. However, the spam legislation isn't about supporting the requirements of marketers but the levels of spam and it has been proven in other areas of the globe that marketers can continue to run their businesses and adhere to opt-in legislation by implementing best-practice methodologies into their businesses.

For instance, inferred consent can be based upon organisations that deliver materials via e-mail to those who have an existing business relationship. These e-mails typically aren't of a commercial nature, but the e-mail is a channel for information delivery only. The outcome is the ability for the legislation to support spam reduction and prosecution of spammers without loss of business for legitimate marketers.

### **Transparency Issues**

13. Should there be a requirement for commercial electronic messages to include a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the sender, and to ensure that such electronic address is functional?  
[see answer below]
14. Should there be a requirement that commercial electronic messages provide accurate header and subject information?  
[see answer below]
15. Should there be a requirement for the labeling of advertising or adult messages?

The identification of spammers is critical in the ability to prosecute offenders and stop fraudulent activities. Although spammers may not adhere to the requirements of labeling, legitimate marketers would and this in itself provides end-users with the ability to easily remove spam and unwanted e-mails from their in-boxes.

### **Privacy Issues - Address Harvesting**

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

Address harvesting, based on the privacy act alone is illegal as consent is not provided. However, to gain protection from spammers undertaking these activities it needs to be incorporated in all anti-spam legislation, as spam is a global issue and governments need to be working in conjunction with one another on a global basis to stop this increasing problem.



### **Enforcement Issues**

17. Who should be able to bring an action against an alleged spammer?

Symantec Brightmail does not have a position on this.

18. What agency should have the enforcement role under the legislation?

Symantec Brightmail does not have a position on this.

19. What should be the available penalties and remedies for breaches of anti-spam legislation and what should be the maximum fine or pecuniary penalty?

Symantec Brightmail believes the penalties should be severe to act as a deterrent to spammers. In the case of Australia they can be high as A\$1 million dollars.

20. Should contraventions give rise to criminal or civil penalties?

Symantec Brightmail does not have a position on this.

21. Should the responsible enforcement agency be given the ability to obtain search warrants conferring powers of entry, search and seizure?

Yes, as the enforcement bodies need to have the ability to be able to act upon the legislation.