Troy Rollo
Chairman
CAUBE.AU
Level 4
1 James Place
North Sydney NSW 2060

Submission for "Inquiry into the Privacy Amendment (Private Sector) Bill 2000"

May 2000

C A U B E . AU

The Coalition Against Unsolicited Bulk Email, Australia

http://www.caube.org.au/

Background

The Coalition Against Unsolicited Bulk Email is an all-volunteer grassroots organisation dedicated to representing consumers on the issue of Unsolicited Bulk Email (UBE), also known as "email spam", or simply "spam". CAUBE.AU is closely affiliated with the Coalition Against Unsolicited Comercial Email (CAUCE), the equivalent organisation in the United States.

The CAUBE.AU web site is the most comprehensive source of information on spam available in Australia, and is the most comprehensive source of business oriented educational material on spam in the world.

Having undertaken almost no publicity campaign to date, CAUBE.AU currently has approximately 500 confirmed members.

Introduction

The Coalition Against Unsolicited Bulk Email concentrates on one specific aspect of the privacy issue – direct marketing via electronic mail. As such our concerns are limited to two specific privacy principles, and to the overall implementation which has a direct impact on the effectiveness of those two principles.

The relevant principles for CAUBE.AU are the first principle – Collection, and the second principle – Use and Disclosure, and in particular principle 2.1(c) which governs the use of privacy information for direct marketing.

In his second reading speech, the Minister stated:

> *"The bill is one element of the government's strategy to ensure that full advantage is taken of the opportunities presented by electronic commerce and the information economy for Australian business and Australian consumers. The Australian public has expressed concern about the security of personal information when doing business online. This concern, if not addressed, has the potential to significantly influence consumer choices about whether or not to participate in electronic commerce."*

It must be noted that, despite this statement, the bill as it stands does not make any effort to deal with the unique aspects of electronic commerce which have resulted in these

heightened concerns on the part of the public. In fact it has taken principles which were drafted almost entirely prior to the widespread use of electronic commerce, and attempted to impose these principles on electronic commerce without any apparent critical evaluation of the continuing applicability of those principles as they stand.

When addressing the desire of Australians for privacy, it is also important to know what aspects of privacy are most important to them. The Privacy Commissioner's 1995 study, "Consumer Attitudes to Privacy", stated:

> *"When it comes to using our personal information responsibly, commercial organisations arouse our suspicion more than government…*
> *"Australians seem to have a particular aversion to their personal privacy being invaded by companies selling products…*
> *"When asked how much they trusted particular organisations, in every survey mail order companies have been least trusted."*

It is clear from this study that in fact unwanted marketing intrusions are a central, if not the central, privacy concern of Australians. As such a complete treatment of privacy must include careful consideration of direct marketing, and if the bill is intended to address consumer concerns regarding privacy in electronic commerce, this means properly addressing the issue of spam in particular.

The Privacy Amendment (Private Sector) Bill 2000 provides a blanket exemption for small business on compliance cost grounds. While the protection of small business is in itself a laudable goal, small business has in fact been the source of many and significant privacy violations, and as such a blanket exemption invites wholesale disrespect for consumer privacy by small businesses. There are numerous aspects of the privacy principles which impose no real compliance cost on the business, and as such there is no reason why so much of the principles as do not result in an excessive compliance cost should not apply to small businesses. Indeed, associations, including unincorporated associations, are not exempted in this bill, even though such associations frequently have even less capacity to deal with compliance costs than small business.

The Privacy Aspect of Spam

The privacy aspect of spam centers on the inability of the consumer to control the spam. The concern began with spammers sending millions of spam emails to recipients they don't even know, and has grown to cover businesses that disregard the wish of their customers to be left alone.

Simple mathematics tells us that allowing people to spam others that they have no business relationship is not viable. Because the cost of sending millions of copies of spam is near zero, if we allow it we can expect everybody with something to sell to use it. A simple glance at the two volume Yellow Pages of our capital cities, or the Saturday morning broadsheets, gives some insight to the number of potential spammers. This makes it plain to anybody that even with spammers being required to provide an opt-out facility, the one shot that they get would result in electronic mail boxes ceasing to be viable very quickly if this behaviour were taken as acceptable.

Several studies have shown that consumers are averse to both varieties of spam, with the groundbreaking study being the April 1999 edition of Cognitiative, Inc's quarterly study *Pulse of the Customer*[1], which revealed that:

> *"One-third of all respondents say they dislike sales-oriented email so much that it actually makes them avoid the vendor who sends them. Companies may actually be losing business by taking this type of action."*

[1] http://www.cognitiative.com/contentPages/Pulse_Rpt_archive.html

This study dealt primarily with unexpected marketing intrusions from companies that the recipient had actually dealt with previously.

Interestingly, while various studies have shown that between 33% and 65% of customers will be turned off if they receive sales material via electronic mail that they were not expecting, empirical evidence shows that in a "forced choice" scenario as recommended by CAUBE.AU[2], vendors can get a 90% opt-in rate. In other words, by giving control to the customer, a vendor can actually get a larger real audience. What's more, customers who have affirmatively requested the email are even more receptive to the email, and actually look forward to receiving it.

In an interview with Salon magazine[3], Hans Peter Brøndmo, founder of Post Communications, a company specialising in using electronic mail for customer relationship management and marketing, said:

> *"I do believe that the onus should be on the marketer to ensure that the customer understands the terms. There should be a 'check here if you agree to the terms' -- so the customer actively says, 'Yeah, I know what's going on.'…*
>
> *"And, by the way, I have the numbers to prove to companies that they're better off if they use positive opt-in. They might have slightly fewer names in the database, but the total economic return of positive opt-in is way better."*

It is clearly an irony that direct marketing lobbyists worldwide are telling people that it is OK to use opt-out. Unfortunately, the facts show that they are not doing their members any favours by doing this. In fact, they are doing their members a great disservice by advocating an inferior approach to customer relationship management – inferior for the business and inferior for the customer.

Our own Privacy Commissioner, Malcolm Crompton, has summed up the importance to businesses of giving the customer control of the relationship and of their information:

> *"Ultimately, the future of e-commerce will be based on trust and consumer confidence. When your competitor is only a 'mouse-click away', trust will be a strong competitive advantage"*

Dr Ann Cavoukian, Information and Privacy Commissioner of Ontario, put it even more simply:

> *"Whoever builds the most trust, wins. In an online world, this translates into which companies can protect their customers' privacy the best, win."*

Companies that understand the Internet, understand that the more control they give to their customers, the more they can make their customers trust them, the more they will win and keep customers. A plan to give customers control of the relationship is the cornerstone of any online business strategy that seeks ongoing, sustainable success.

It is in this light then, where consumer privacy is in the interests of both businesses and consumers, that we consider the Privacy Amendment (Private Sector) Bill 2000.

The Privacy Principles

CAUBE.AU is concerned with two aspects of the privacy principles, both of which could be better tuned to deal with the unique circumstances which exist in electronic commerce without imposing any penalty on business. The privacy principles that concern CAUBE.AU are Principle 1 – Collection, and Principle 2 – Use and disclosure, in particular Principle 2.1(c), which relates to the use of material for direct marketing.

[2] http://www.caube.org.au/buspref.htm
[3] http://www.salon.com/tech/view/2000/04/17/brondmo/index2.html

Principle 2.1(c) in particular has been subject to some loose and clearly incorrect interpretation in industry code recommendations.

Principle 1 – Collection

Principle 1.3 reads:

> 1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, **the organisation must take reasonable steps to ensure that the individual is aware of**:
>
> (a) the identity of the organisation and how to contact it; and
> (b) the fact that he or she is able to gain access to the information; and
> **(c) the purposes for which the information is collected**; and
> (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
> (e) any law that requires the particular information to be collected; and
> (f) the main consequences (if any) for the individual if all or part of the information is not provided

As written, there is wide scope for determination of what is reasonable. When collecting information on the web, a business might argue that information buried in a five hundred line privacy policy in the smallest available font is sufficient to "ensure that the individual is aware of" these things. In reality, online businesses more frequently use privacy policies as a method of saying to the consumer in overly verbose wording that they really have no privacy at all when giving information to that business. Some privacy policies are even written in complex legalese, which makes it difficult for typical consumers to understand what the policy says.

This principle should be expanded to specify that the consumer is informed in concise, consumer oriented language, and that where technology allows, the user should be given the opportunity to affirmatively indicate that they are aware of these things:

> 1.4 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, **the organisation must take reasonable steps to ensure that the individual is aware of**:
>
> (a) the identity of the organisation and how to contact it; and
> (b) the fact that he or she is able to gain access to the information; and
> **(c) the purposes for which the information is collected**; and
> (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
> (e) any law that requires the particular information to be collected; and
> (f) the main consequences (if any) for the individual if all or part of the information is not provided
>
> <u>The organisation must supply this information in concise, consumer oriented language. When the information is collected on a written or electronic form, items (c) and (d) must be provided conspicuously on the form, and the other items may be provided by reference to another part of the form.</u>
>
> <u>Where technology allows without prohibitive expense, the organisation must provide for the user to affirmatively indicate by taking a deliberate action that they are aware of and understand the items of which they have been made aware.</u>

The requirement for concise, consumer oriented language aims to avoid the obscuring of the statement in complex legalese that the consumer cannot understand, and to ensure that the business does not attempt to produce privacy policies so long that nobody has

time to read them. The privacy policies for Disney.Com and Amazon.Com, shown in Appendix A and Appendix B of this submission, are examples of ludicrously lengthy privacy policies which attempt through verbosity to hide the fact that these sites reserve the right to violate the customer's privacy. They even state that that the consumer agrees to these conditions simply by using the web site, without the consumer even having read the policy, and further state that if they change the policy that the user automatically agrees to the conditions by continuing to use the site.

The requirement for prominently placing items (c) and (d), which are, for the consumer, the key items that may influence their choice of vendor, is to ensure that the vendor does not place the items in an obscure location, or in fine print. Once again, burying these items in obscure locations is a common tactic used by vendors to attempt to claim that they have in fact provided the required statement.

Finally, the requirement that the vendor provide for the consumer to take a deliberate action to acknowledge that they are aware of the items merely clarifies the principle – there is a significant difference between merely providing a statement and "ensuring that the individual is aware." The latter inherently requires some actual feedback, rather than a passive statement. Without the active feedback, the organisation has ensured nothing.

Principle 2 – Use and Disclosure

Principle 2.1(c) reads:

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

On the face of it, 2.1(c)(i) states that where practicable, the consumer must be given the up front choice of whether their information may be used for the purposes of direct marketing. That is, if the organisation collects this information from the consumer, and it is practicable to ask for consent at the time of collection, then the organisation must either obtain such consent at the time of collection or not use that information.

Unfortunately, industry bodies, most notably the Australian Direct Marketing Association, have interpreted this clause to mean that the vendor does not need to seek the individual's consent at the time of collection, even if the vendor knows they will be using the information for direct marketing. They then treat it impracticable to seek consent before using the information for the purposes of direct marketing. By taking this approach, they seek to avoid having to obtain the individual's consent, thereby attempting to evade the intent of the provision.

2.1(c) needs to be changed to read:

> if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
>
> (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) where the organisation collected the information directly from that individual, it was impracticable to seek consent at the time of collection; and
(iii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
(iv) the individual has not made a request to the organisation not to receive direct marketing communications; and
(v) the organisation gives the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications

The insertion of the new subclause (ii) attempts to ensure that organisations do not seek to avoid the opportunity to obtain consent in order to claim that it is impracticable to obtain consent. To that end, it merely closes a loophole in the existing subclause (i).

In addition, 2.1(c) does not deal with the problems of unsolicited bulk email (spam) at all. In particular, clause 2.1(c) does not acknowledge that the recipient may bear some of the expense of the first contact, and as such, while the organisation may not charge for a request not to receive information, they nonetheless have forced the individual to bear an expense. Accordingly, a further clause should be added to 2.1(c) to prevent the use of such information for marketing where there would be a forced cost to the recipient:

if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
(ii) where the organisation collected the information directly from that individual, it was impracticable to seek consent at the time of collection; and
(iii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
(iv) the individual would not, in the normal course, be forced to incur a direct or indirect cost to receive the marketing communications; and
(v) the individual has not made a request to the organisation not to receive direct marketing communications; and
(vi) the organisation gives the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications

The explanatory memoranda for the bill acknowledge the cost imposition of unsolicited facsimile and electronic mail advertising, and more information on the costs of unsolicited bulk email is given in Appendix C.

The Small Business Exemption

The Bill as introduced contains a blanket exemption for small business, except those who handle "sensitive information". The reason cited for this by the Minister in his second reading speech is:

> *"while protecting privacy is an important goal, it must be balanced against the need to avoid unnecessary costs on small business. For this reason, only small businesses that pose a high risk to privacy will be required to comply with the legislation."*

While we agree with the need to protect small business from prohibitive compliance costs, this is not a reason for giving small businesses that do collect personal information a blanket exemption. For privacy principles where there is not a significant compliance cost, small business should be included. This is especially important given that the power of the Internet gives small businesses the ability to compete effectively with larger businesses – together with the same capacity to violate an individual's privacy.

The provisions of Principle 1 – Collection, and Principle 2 – Use and Disclosure, in particular, do not impose a significant cost on an organisation, and as such there should be no exemption for small business.

The Need to Specifically Include Certain Things as "Personal Information"

The Privacy Act 1998 currently defines personal information as:

> *"information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."*

While this does technically include contact information, such as the home address, telephone number and electronic mail address, some have expressed a concern that businesses may nevertheless not regard such information as personal information. It would therefore be of advantage to add a section of the form:

> Personal information includes, but is not limited to, the following information:
> (a) sensitive information;
> (b) an individual's home address and other contact information, whether otherwise associated with that individual in the organisation's record or not;
> (c) an individual's profession, income, and place of employment;
> (d) an individual's banking information;
> (e) information on an individual's purchases; and
> (f) any other information that is associated with an individual.
>
> Circumstances in which the identity of a person can be reasonably ascertained include, but are not limited to, the following:
> (g) the information is, or is recorded with, or is associated with, the name of an individual;
> (h) the information is, or is recorded with, or is associated with, contact information for an individual, including, but not limited to, an individual's address, telephone number, facsimile machine number, or electronic mail address; or
> (i) the information is, or is recorded with, or associated with, an individual's profession and place of employment.

The State of Privacy Policies and Privacy Policy Seals

On the Internet, privacy policies have evolved into long winded, convoluted documents drawn up by lawyers, which seek to confuse the consumer and hide the truth from them. It is a fundamental truth that a privacy policy that a typical individual cannot understand, or that is far too long for them to have time to read, is worse than no privacy policy at all, because such policies frequently seek to deceive the individual into thinking that the organisation will respect their privacy.

Case Study 1 – Disney

The privacy policy in Appendix A was taken from Disney's web site on the 7th of May, 2000. You will notice that after the introductory paragraph explaining the need for a privacy policy, the opening sentence is *"Disney Online and the GO Network's policy is to respect and protect the privacy of our users"*. That sounds promising, but what is really in this two thousand, two hundred and forty two word document?

> *"Information provided at the time of Registration or submission from a Guest … may be used for marketing and promotional purposes by Disney Online, the GO Network, and our affiliates or companies that have been prescreened by Disney Online and the GO Network… If a Guest objects to such use for any reason, he/she may stop that use -- either by e-mail request to guest.mail@online.disney.com or by modifying his/her member information online."*

In other words, unless you bother to read this lengthy document, and specifically tell them not to, you may receive unrequested and unwanted advertising material from Disney, their affiliates, and companies that have been "prescreened" – presumably by cash based means – by Disney.

The last paragraph is particularly telling of Disney's reprehensible lack of care for their customers' privacy:

> *"By using this site, you signify your assent to the Disney Online and the GO Network Privacy Policy. If you do not agree to this policy, please do not use our sites.* ***Your continued use of the Disney Online and GO Network sites following the posting of changes to these terms will mean you accept those changes****."*

Not only do they state that these terms apply even to people who have not read their incredibly long-winded document – they state that if you continue to use their web sites after they change the policy, you agree to the changes. It appears they expect every individual to read their entire two thousand, two hundred and forty two word privacy policy every time they visit the Disney web sites.

The Disney privacy policy fails completely to effectively communicate a privacy policy to the consumer. By writing such a long document, and in particular by stating that it is subject to change effectively without notice, they have guaranteed that visitors to their site will never read the document, and will certainly not be able to stay up to date on it. By doing this, they have successfully buried their intent to use the customer's information for marketing purposes.

Case Study 2 - Amazon

The privacy policy in Appendix B was taken from Amazon Books' web site on the 7th of May, 2000. Like the Disney policy, it opens with comforting words – *"At Amazon.com, we are committed to protecting your privacy."* Further examination reveals that the Amazon policy is even worse than the Disney policy.

While Amazon's policy is mercifully shorter than Disney's policy, it is still far too long to be of use to the consumer, weighing in at one thousand, three hundred and thirty two words.

Like Disney, Amazon promise that they *will* use personal information for marketing purposes. They also claim that use of the site consitutes agreement to the terms, and that continued use after any change in the terms constitutes agreement to the changes.

Amazon's policy, however, contains a far worse hidden thorn:

> *"Amazon.com does not sell, trade, or rent your personal information to others. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank e-mail message to never@amazon.com. (If you use more than one e-mail address to shop with us, send this message from each e-mail account you use.)"*

If you don't read their hefty privacy policy, as most people will not, then Amazon are reserving the "right" to sell their cusomers' personal information to third parties. This is a violation of the individual's right to privacy that most people would never have anticipated, especially from a company that says they *"are committed to respecting your privacy."*

As a policy to provide a genuine privacy guarantee to consumers, the Amazon policy fails miserably. As a policy to ensure that Amazon can violate the privacy of their customers, without their customers being aware in advance, the Amazon policy succeeds magnificently.

Privacy Policy Seals

When we talk about privacy policy seals, we are talking almost exclusively about TRUSTe, the grandfather of all privacy policy seals. Unfortunately, while consumers are led to believe that the TRUSTe seal is a guarantee that the site will respect their privacy, in fact it does not – the TRUSTe seal merely validates that the site has a privacy policy, that the stated policy states how the site will use the individual's personal information, and what the individual can do if they object.

The Disney and Amazon privacy policies previously examined are in fact certified by TRUSTe. These and other atrocious privacy policies that have been certified by TRUSTe have lead to an almost universally agreed one sentence summary of TRUSTe among privacy advocates – *"A TRUSTe logo is perhaps the most reliable possible indicator available that a site will violate your privacy."*

In fact in 1999 TRUSTe became so poorly regarded that in November, Stanton McCandlish, of the Electronic Frontier Foundation (EFF), which started TRUSTe, said:

> *"We did the "proof of concept" ourselves, by launching and spinning off TRUSTe. But TRUSTe was intended to be and is a separate, independent entity, and was created as an experiment. The experiment is in many ways a failure, and so now we observe and openly state that it is not enough."*

Miscellaneous

There are a number of other items that might be considered, although they do not relate directly to CAUBE.AU policy.

- The bill adds to the role of the Privacy Commissioner in a way that effectively casts the role as a type of ombudsman. As such, it may be appropriate to provide for the cost of operation of that role to be met by the businesses that are investigated. Not only would this be consistent with other private industry ombudsman programs, it would reduce the cash costs of the bill and provide an additional incentive for businesses to sign on to a code of practice where the cost of complaints may be lower.

- The use of the Federal Court as the sole venue for enforcement and damage recovery is an expensive option, both for the individual and for the business. In order to reduce the costs, provision could be made for damage recovery to a maximum value to be recovered in suitable state courts, including local and small claims courts.

Appendix A – Disney.Com's privacy policy

PRIVACY POLICY

THE INTERNET, PRIVACY, DISNEY ONLINE, AND THE GO NETWORK

The Internet contains a wealth of information; unfortunately, it may also contain personal details about you that you don't want everyone to know. For example, your real name (lots of people on the Internet use aliases, alter egos, or nicknames), street address, phone number, or e-mail address. When you go online, sites you visit may be gathering information about you without your knowledge. At Disney Online and the GO Network we strive to help our customers protect their privacy while using our services.

DISNEY ONLINE AND THE GO NETWORK'S PRIVACY POLICY

Disney Online and the GO Network's policy is to respect and protect the privacy of our users. This policy statement tells you how we collect information from you and how we use it. Using the Internet should be a fun experience and we want to help you make it so.

The information you provide for your personal Disney Online Account is shared among the GO Network sites, as it is our goal to make your visits to our sites easy and enjoyable. However, be assured that Disney Online and the GO Network will not disclose your personal information to third parties without your consent. Disney Online and the GO Network may disclose user information in special cases when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against someone who may be causing injury to or interference with (either intentionally or unintentionally) Disney Online and the GO Network's rights or property, other Disney Online and GO Network users, or anyone else that could be harmed by such activities. Disney Online and the GO Network may disclose user information when we believe in good faith that the law requires it.

Disney Online and the GO Network share aggregate information about our users with advertisers, business partners, sponsors, and other third parties. For example, we will say Disney Online's audience is x percent female and y percent male. This data is used to customize Disney Online and the GO Network content and advertising to deliver a better experience for our users.

There are cases where Disney Online may ask you for personal information such as your name, e-mail address, and birth date. For example, we request personal information when you register for a Disney Online Account, for online shopping or transactions, or for services that require registration or subscription (for example Disney's Club Blast). Disney Online needs to collect this information for fulfilling prizes, tracking/verifying compliance with Disney Online and the GO Network policies as well as federal, state, and local laws, and/or for editorial and feedback solicitation purposes.

In case you change your mind or some personal information changes (such as your ZIP code), we will endeavor to provide a way to correct, update, or remove the personal data you give us. You can do this at the member information page or by contacting our Customer Support organization at guest.mail@online.disney.com.

OPTING OUT

Information provided at the time of Registration or submission from a Guest who is 13 years of age or over may be used for marketing and promotional purposes by Disney Online, the GO Network, and our affiliates or companies that have been prescreened by Disney Online and the GO Network. To keep you in control of your personal information and the communications directed to you, we allow you to opt out of the following services: sharing your information in our member directory, receiving communications from Disney Online about new features or services, and receiving communications about offers from third-party companies that offer a product or service that we think would be of value to you. If a Guest objects to such use for any reason, he/she may stop that use -- either by e-mail request to guest.mail@online.disney.com or by modifying his/her member information online.

Information provided when purchasing products from any of our online stores may be used for marketing and promotional purposes and is subject to the opt-out processes described on, or linked to, each order form.

POLICIES FOR KIDS (INDIVIDUALS UNDER 13 YEARS OF AGE)

Disney Online and the GO Network encourage parents and guardians to spend time online with their children and to participate in the activities offered on the sites. No information should be submitted to or posted at Disney Online and the GO Network by Guests under 13 years of age without the consent of their parent or guardian.

Unless otherwise disclosed during collection, Disney Online and the GO Network do not provide any personally identifying information, regardless of its source, to any third party for any purpose whatsoever from our Guests under 13 years of age. All registrants receive an e-mail confirming their Registration. In addition, when a Guest under 13 registers, he/she is required to provide the e-mail address of his/her parent or guardian and that parent or guardian receives an e-mail alerting them to that Registration. Since all of Disney Online's free interactive activities are monitored by community policy experts, registered Guests under 13 years of age may participate in such activities upon Registration, unless their parent or guardian asks that their registration be invalidated. In order for the potential Member to use the GO Network interactive services, the parent or guardian must validate the account, as described in the e-mail. No information collected from Guests under 13 years of age is used for any marketing or promotional purposes whatsoever, either inside or outside Disney Online and the GO Network except as explicitly stated during registration for contests or promotions (and in that case, the information collected is used only for the specific contest or promotion).

Although Guests under 13 years of age may be allowed to participate in some contests and promotions, if such a Guest wins, notification and prizes are sent to the parent or guardian identified in the initial registration process. Publication of names, ages, or images for contest winners under 13 require parental or guardian consent.

We do not allow Guests under 13 years of age to be listed in our Member directory or to receive direct marketing communications from Disney Online and the GO Network or to be sent third-party offers.

POLICIES FOR TEENS (INDIVIDUALS 13 TO 17 YEARS OF AGE)

Teens are required to provide the e-mail address of a parent or guardian and a notification message is sent to the parent or guardian of all Guests who are 13 to 17 years of age, which identifies the information supplied at Registration and allows the parent or guardian to be aware of and participate in the Guest's online experience.

USE OF IP ADDRESSES

An IP address is a number that's automatically assigned to your computer whenever you're surfing the Web. Web servers -- the big computers that "serve up" Web pages -- automatically identify your computer by its IP address.
Disney Online and the GO Network collect IP addresses for the purposes of system administration, to report aggregate information to our advertisers, and to audit the use of our site. When Guests request pages from Disney Online and the GO Network sites, our servers log the Guests' IP addresses. We do not normally link IP addresses to anything personally identifiable, which means that a user's session will be logged, but the user remains anonymous to us. We can and will use IP addresses to identify a user when we feel it is necessary to enforce compliance with our house rules or terms of service or to protect our service, site, customers, or others.
Some services within Disney Online and the GO Network, such as certain message boards, may display IP addresses along with the message poster's name and message. Please review each service prior to use and only use those that disclose information you are comfortable with sharing.

USE OF COOKIES

What are cookies? Cookies are pieces of information that a Web site transfers to an individual's hard drive for record-keeping purposes. Cookies make Web-surfing easier for you by saving your preferences while you're at our site. We never save passwords or credit card information in cookies. The use of cookies is an industry standard -- you'll find them at most major Web sites.

By showing how and when Guests use a site, cookies help us see which areas are popular and which are not. Many improvements and updates to the site are based on such data as total number of visitors and pages viewed. This information is most easily tracked with cookies. We use the information from cookies to provide services better tailored to our users needs.

Disney Online and the GO Network have two primary uses for their cookies. First, we use them to specify unique preferences. For example, in GO Network's News Center, users can specify keywords across several news categories. This way you don't have to tell us over and over again about the kinds of news stories you want to see. Secondly, we use cookies to track user trends and patterns. This helps us better understand and improve areas of the Disney Online and the GO Network service that our users find valuable. While both of these activities depend on the use of a cookie, visitors to Disney Online and the GO Network always have the option of disabling cookies via their browser preferences. Information from cookies is sometimes attached to messages sent to our Customer Service department

Most browsers are initially set up to accept cookies. You can reset your browser to refuse all cookies or indicate when a cookie is being sent. However, note that some parts of the Disney Online and the GO Network service will not function properly or may be considerably slower if you refuse cookies. For example, without cookies, you will not be able to set personalized news preferences or you may have difficulty completing shopping transactions, entering contests, or playing games.

You may occasionally get cookies from our advertisers. Disney Online and the GO Network do not control these cookies. The use of advertising cookies sent by third-party servers is standard in the Internet industry.

LINKS TO OTHER SITES

Users should be aware that when they are on Disney Online and the GO Network, they could be directed to other sites that are beyond our control. There are links to other sites from Disney Online and the GO Network pages that take you outside our service. For example, if you "click" on a banner advertisement or a Disney Online search result, the "click" takes you off the Disney Online site. This includes links from advertisers, Center sponsors, and partners that may use Disney Online or the GO Network's logo as part of a co-branding agreement. These other sites may send their own cookies to users, collect data, or solicit personal information.

Please keep in mind that whenever you give out personal information online --- for example, via message boards or chat --- that information can be collected and used by people you don't know. While Disney Online and the GO Network strive to protect their users' personal information and privacy, we cannot guarantee the security of any information you disclose online and you do so at your own risk.

Disney Online and the GO Network's policy does not extend to anything that is inherent in the operation of the Internet, and therefore beyond Disney Online and the GO Network's control, and is not to be applied in any manner contrary to applicable law or governmental regulation.

SECURITY

The importance of security for all personally identifiable information associated with our Guests is of utmost concern to us. We exercise great care in providing secure transmission of your information from your PC to our servers. Unfortunately, no data transmission over the Internet can be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, Disney Online and the GO Network can't ensure or warrant the security of any information you transmit to us or from our online products or services, and you do so at your own risk. Once we receive your transmission, we make our best effort to ensure its security on our systems. When credit card information is transmitted we use industry standard, SSL (secure socket layer) encryption.
Your Disney Online and GO Network Account is password-protected so that only you can access it and view the member information relevant to the account. We recommend that you do not divulge your password to anyone. Disney Online and the GO Network will never ask you for your password in an unsolicited phone call or e-mail. Ultimately, you are responsible for maintaining the secrecy of your passwords and any account information.

Remember to sign out of your Disney Online or GO Network Account and close your browser window when you have finished your work. This is to ensure that others cannot access your personal information and correspondence if your computer is accessible to others or if you share a computer with someone else or are using a computer in a public place like a library or Internet café.

YOUR ACCEPTANCE OF THESE TERMS

By using this site, you signify your assent to the Disney Online and the GO Network Privacy Policy. If you do not agree to this policy, please do not use our sites. Your continued use of the Disney Online and GO Network sites following the posting of changes to these terms will mean you accept those changes.

If you have questions or concerns regarding this Web site's privacy statement, you should first contact the company as follows: Privacy Policy Coordinator, Buena Vista Internet Group, 500 S. Buena Vista Street, Burbank, California 91521-7690; telephone number: (818) 623-3200; or via e-mail. If you do not receive acknowledgment of your inquiry or your inquiry has not been satisfactorily addressed, you should then contact TRUSTe (http://www.truste.org/users/users_contact.html).

Appendix B – Amazon.Com's Privacy Policy

At Amazon.com, we are committed to protecting your privacy. We use the information we collect about you to process orders and to provide a more personalized shopping experience. Please read on for more details about our privacy policy.

What information do we collect? How do we use it?

- When you order, we need to know your name, e-mail address, mailing address, credit card number, and expiration date. This allows us to process and fulfill your order and to notify you of your order status.
- When you sign up for our Personal Notification Services (Amazon.com Delivers, Alerts, and Oprah®), we need only an e-mail address--which we use to send the information you requested.
- When you submit a customer review, we also ask for your e-mail address, although you can choose not to have your e-mail address displayed with your review.
- When you enter a contest or other promotional feature, we may ask for your name, address, and e-mail address so we can administer the contest and notify winners.
- We personalize your shopping experience by using your purchases to shape our recommendations about the books, CDs, and other merchandise that might be of interest to you. We also monitor customer traffic patterns and site usage to help us develop the design and layout of the store.
- We may also use the information we collect to occasionally notify you about important functionality changes to the Web site, new Amazon.com services, and special offers we think you'll find valuable. If you would rather not receive this information, visit your Amazon.com Subscriptions page to change your preferences. Make sure to change your preferences for each account or e-mail address you have left with us.
- When you send a greeting through the Amazon.com e-Cards service, we ask for your e-mail address and that of the recipient in order to complete your request. Amazon.com will never disclose or send promotional e-mail to recipient addresses provided only to the Amazon.com e-Cards service.
- For Purchase Circles, we group the items we send to particular ZIP and postal codes, and the items ordered from each domain name. We then aggregate this anonymous data and apply an algorithm that constructs bestseller lists of items that are more popular with each specific group than with the general population. None of the data is associated with any individual's name. If you or your company or organization doesn't want to participate in Purchase Circles, click here for more information.
- When you create a Wish List, we ask for your name, shipping address, and an optional personal description. We use your name and personal description to identify your Wish List; we use your name and shipping address to process and fulfill your Wish List orders. You can also choose to provide e-mail addresses of friends and family with whom you would like to share your list. We'll e-mail the recipients that you choose to tell them about your Wish List and its contents, and how they can easily access it. Amazon.com will not disclose or send promotional e-mails to those recipient addresses provided only to the Wish List service.
- If you create an All About You area, you provide your name, a nickname, your e-mail address, and an optional personal description. This information is used to identify your All About You area to those who visit it. (You can hide your name and e-mail address when you create or edit your All About You area.) Using the Favorite People feature, you can share information about selected past purchases from Amazon.com with friends and family. If you choose to do this, we may ask you to provide the e-mail addresses of those people. We'll e-mail the recipients with whom you choose to share this sales information, and inform them how they can easily access your All About You area. Amazon.com will not disclose or send promotional e-mails to those recipient addresses provided only to the All About You service.
- We have recently developed relationships with a select group of high-quality online stores, and if you shop at these stores by using a link from our store to theirs or by participating in a joint promotion (for example, we may send you a complimentary gift certificate or coupon for use in their stores), we may receive aggregate or

otherwise anonymous statistical information about your shopping trip to these stores. We treat this information with the same care as we treat other information that you entrust to Amazon.com, and it is fully protected by our privacy policy.

- If you register as an Amazon.com Discussion Boards member, your registration information (i.e., your e-mail address and nickname) will be submitted directly to RemarQ Communities, Inc., the operator of our discussion board service, in order to host our discussion boards. RemarQ will not disclose your information, and your information will remain fully protected by Amazon.com's privacy policy.

How does Amazon.com protect customer information?

When you place orders or access your account information, we offer the use of a secure server. The secure server software (SSL) encrypts all information you input before it is sent to us. Furthermore, all of the customer data we collect is protected against unauthorized access.

What about "cookies"?

"Cookies" are small pieces of information that are stored by your browser on your computer's hard drive. Our cookies do not contain any personally identifying information, but they do enable us to provide features such as 1-Click(sm) shopping and to store items in your shopping cart between visits. Most Web browsers automatically accept cookies, but you can usually change your browser to prevent that. Even without a cookie, you can still use most of the features in our store, including placing items in your shopping cart and purchasing them.

Will Amazon.com disclose the information it collects to outside parties?

Amazon.com does not sell, trade, or rent your personal information to others. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank e-mail message to never@amazon.com. (If you use more than one e-mail address to shop with us, send this message from each e-mail account you use.) Also, Amazon.com may provide aggregate statistics about our customers, sales, traffic patterns, and related site information to reputable third-party vendors, but these statistics will include no personally identifying information. Amazon.com may release account information when we believe, in good faith, that such release is reasonably necessary to (i) comply with law, (ii) enforce or apply the terms of any of our user agreements or (iii) protect the rights, property or safety of Amazon.com, our users, or others.

How does Amazon.com allow customers to update or change the information it collects?

You may update or change information related to your Amazon.com account by accessing your Amazon.com Subscriptions section of the Web site with your e-mail account and password. For other questions related to updating or changing your account information, please send e-mail to feedback@amazon.com.

In summary

We are committed to protecting your privacy. We use the information we collect on the site to make shopping at Amazon.com possible and to enhance your overall shopping experience. We do not sell, trade, or rent your personal information to others. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank e-mail message to never@amazon.com. If you never want to receive any announcements or special offers from us, visit your Amazon.com Subscriptions page to change your preferences. Remember to change your preferences for each of the e-mail accounts you have given us.

Your consent

By using our Web site, you consent to the collection and use of this information by Amazon.com. If we decide to change our privacy policy, we will post those changes on this page so that you are always aware of what information we collect, how we use it, and under what circumstances we disclose it.

Tell us what you think

Amazon.com welcomes your questions and comments about privacy. Please send e-mail to feedback@amazon.com.

Appendix C – The costs of Unsolicited Bulk Email

The Various Costs of Spam

Unsolicited Bulk Email, also known as spam, costs the community at large in numerous ways, while costing the spammers practically nothing. The ways in which spam costs the community at large are:

1. transmission costs;
2. storage costs;
3. recipient time costs;
4. utility of medium costs; and
5. freedom of choice costs.

An analysis of the impact of any given strategy on the problem must include an analysis of the effects of that strategy on each of these costs.

Transmission Costs

While most people find it difficult to believe, it costs real money to transmit data on the Internet. The data is transmitted over wires, optic fibre, satellite, radio, and other transmission mechanisms. All of these transmission mechanisms are often referred to as "pipes."

All kinds of data pipes cost money to build and maintain, and like the plumbing devices of the same name, data pipes have a limited capacity. At a certain point, if you want to get more data from A to B, you have to install more pipes.

Communications specialists will often refer to the capacity of data pipes as "bandwidth". Hence the term "waste of bandwidth", which refers to any data forced through the pipes which is of little or no value, and which displaces other data with more value. Data that wastes bandwidth increases the cost of the Internet by forcing ISPs to buy more, bigger and more expensive pipes.

In general, data transmitted on the Internet is of benefit to the recipient of that data. For example, when you browse a web page, download files, listen to audio clips, or view movie trailers, you are receiving far more data than you are sending.

The pricing of Internet services in Australia reflects this fact – Australian backbone Internet Service Providers charge their customers according to the amount of data they receive. Telstra BigPond Direct (BPD) is the largest backbone ISP in Australia, and BPD charges their customers $0.19 per megabyte of data they receive, with no charges for sending data.

In the case of spam, the sender is the advertiser, and the recipient is the advertiser's target. Clearly with any form of advertising, the intended beneficiary is the advertiser. Yet clearly when the advertisement is being transmitted across the Internet, the cost of transmitting that advertisement is borne by the recipient. When the recipient has no choice about receiving an advertisement, that expense is quite literally theft by the advertiser from the recipient of the advertisement.

BigPond Direct's customers are businesses and second tier Internet Service Providers. Businesses incur these costs directly, and ISPs pass the costs on to the consumer in the form of more or higher access charges, or in the form of inferior service.

Storage Costs

The measurable costs of spam do not stop at the transmission costs. ISPs need to store the spam on their systems. Electronic mail servers store a separate copy of each email for each recipient on that server. This reflects the fact that email was designed for person-to-

person messages rather than broadcast messages – each recipient gets a private copy of the message.

Disk space currently costs approximately $34 per gigabyte for home computers, and significantly more than that for server computers which are normally used by ISPs. If an ISP is storing a lot of spam for its customers, it needs to add more disk space to allow for this, and the extra disk space costs money. Once again, the ISPs pass these costs on to their users.

Recipient Time Costs

Each spam a recipient receives costs the recipient time. At a minimum, the recipient must identify the item as spam and delete it. While this may not seem like a lot of time for one person and one spam, cumulatively, over many spams, or many recipients, or both, the time costs dwarf the costs to the sender.

If a recipient is expected to reply to a message to be added to an opt-out list for each vendor, the time cost is multiplied. As spam increases, this cost increases to the point where the cost to an individual becomes significant. Accordingly, any solution that does not seek to place real limits on spam risks adding significantly to these costs.

Utility of Medium Costs

As the volume of spam increases, it becomes more and more difficult to find legitimate communications among all of the spam. Even at current levels, it is quite common for even the most experienced people to delete a legitimate message accidentally when deleting spam, and to open a spam message thinking it is legitimate.

There have also been significant cases of people closing down email accounts with ISPs because they were unable to use their electronic mail box due to it being drowned in spam. In extreme cases, new users to the Internet have given up and simply stopped using the Internet due to the perception that there is no way to stop the spam. That in itself demonstrates the severe damage that spam has done to consumer confidence.

Freedom of Choice Costs

Because the individual consumer pays for their Internet access[*], it is clearly their fundamental right to choose how their electronic mail box will be used. They have the ownership of their electronic mail box, and consequently they have the exclusive right to determine what should go in it.

When a spammer sends out unsolicited bulk email, that spammer robs the choice from the consumer. An after the fact opportunity to opt-out does not change that – the consumer's freedom to choose has already been taken away.

Spammers in effect attempt to claim a superior title to the mail boxes of consumers. This is a situation that is clearly unjustifiable.

In essence, spammers don't just steal the resources, money and time of the community – they steal the right of the individual to be left alone. In the United States, Judge William O. Douglas, Justice of the Supreme Court, said in 1952 "The right to be let alone is indeed the beginning of all freedom." Any solution that ignores this fact is in reality no solution at all.

[*] While some free ISPs exist, funded by on-screen advertising, this business model has usually proven not to be viable in the long term. Somebody forcing advertising into email boxes hosted at free ISPs would, of course, be stealing service from the ISP itself in the most literal possible way. Somebody forcing advertising on somebody who has opted not to use a free ISP is also forcing advertising on somebody who has, in effect, already opted not to receive advertising.

Sender Costs vs. Recipient Costs

An inescapable attribute of spam is that it is far more expensive for society as a whole than it is for the spammer themselves. The proportion of the cost to society that is imposed without any choice on the part of the recipients can be viewed as a subsidy for the benefit of the spammer. While spammers like to claim that other forms of legal advertising do this, the reality is that no form of advertising results in even a tiny fraction of the subsidy that spammers take.

CAUBE.AU has undertook a spam survey between February 1999 and February 2000, using addresses that were placed in public places for the sole purpose of getting those addresses on the spam lists. In the full spam survey, the average size of a spam is 5KB.

If we take an example of a single spammer sending a single average sized spam to one million recipients (a small number in spam terms – two Australians were recently charged with securities related violations after allegedly sending four million spams touting an American stock) the costs are:

	Sender	**Recipient**
Data Transmitted	5000MB	
Message Transmission Costs[+]		$950.00
Transmission Overheads	320MB	320MB
Overheads Cost	$60.80[$]	$60.80
Data Storage	5000 bytes	5000 MB
Data Storage Cost[†]	$0.0017	$169.53
Human Resource Time to Send	1 hour	
Human Resource Time to identify as spam[‡]		1389 hours
Monetary Cost of Time[#]	$21.94	$30,480.22
Utility of Medium Cost		Impossible to Estimate
Freedom of Choice Cost		Priceless
Total value of estimable costs	$82.74	$31,660.55
Forced Subsidy		**38,265%**

So here we have a single spammer, sending a single spam to one million recipients, incurring costs to himself of just over a hundred dollars, while inflicting a cumulative cost to the community of over thirty thousand dollars. The wider community actually ends up being forced to paying a large subsidy to the spammer. Even if we discount the monetary cost of time, the cumulative cost to the community is almost twelve hundred dollars – still more than an order of magnitude more than the cost to the spammer.

[+] Based on a transmission cost of $0.19 per megabyte received.

[$] Spammers rarely actually incur this cost, preferring instead to transmit from a service which does not bill this cost directly but instead has an acceptable uses policy prohibiting such use. In this case, the cost is passed on to other customers of the ISP.

[†] Based on a disk space cost of $33.90 per gigabyte.

[‡] Based on the assumption that it takes 5 seconds to see, recognise, and delete without reading, a spam.

[#] Based on an average gross weekly employee income of $844 per week in 1996-1997, not indexed to inflation, from the Australian Bureau of Statistics