

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

Submission for “Electronic Commerce – A Model For Business” – Second Round

February 2000

C A U B E . A U

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 Commercial 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 370 confirmed members.

Introduction

The December 1999 draft of the model proposes three possible methods for dealing with the problems of spam:

1. An opt-in approach – this is the preferred method of the CAUBE.AU membership;
2. A orthodox opt-out approach – in reality, opt-out means that the consumer has no option at all; and
3. An opt-out approach, with compulsory tagging of messages using a tag in the subject header.

There is a fourth option that has not been considered, and it is a significant option since it looks like this is the option that will be taken in the United States as being a reasonable balance between property protection rights and the strong protection of speech afforded to US citizens by their first amendment:

4. An opt-out approach, with the option for the operator of an Internet mail server to post the technical equivalent of a “no junk mail” sign on the mail server.

Spam is a problem that has proven to be highly resistant to effective resolution by technical and social means.

On the technical front, every single filter that has ever been devised has resulted in either a significant amount of spam getting through, a significant amount of legitimate mail being discarded, or a combination of both of these unwanted side effects. Even filters that work by intercepting email for a large number of recipients and discarding messages that come in large quantities have significant negative consequences. These side effects include the delaying legitimate email from reaching its final recipients, and the even more disastrous side effect of blocking opt-in email newsletters – a side effect that reportedly renders 5% of legitimate opt-in subscriptions undeliverable¹.

On the social front, spammers can easily obtain fresh access to the Internet, even after being disconnected for violating the Acceptable Usage Policies (AUPs) of Internet Service Providers. This renders such attempts to provide social disincentives to spamming largely ineffective.

The Various Costs of Spam

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

¹ <http://www.mediainfo.com/ephone/news/newshtm/stop/st012600.htm>

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

* 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.

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.

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 been conducting a spam survey over the past year, 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), 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% |

⁺ 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

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.

Australia's Contribution to the Problem

The CAUBE.AU spam survey has provided useful information on the extent of the Australian contribution to the spam problem. The survey addresses included both Australian (*.au) and United States (*.com) addresses, with some addresses posted to web pages, others used as the return address of a post to USENET news, and others seeded into network administrative databases. Each address appeared on only one USENET news posting, on one web page, or in one database.

Of the spam received at the survey addresses, 12% was clearly Australian in origin. 14% of spam received by the Australian addresses originated in Australia, and 8% of the spam received by United States addresses originated in Australia. Australian spammers represented approximately 10% of the spammers caught in the survey, but none of the Australian spammers used multiple addresses – which is common elsewhere – so the real figure may be higher than this.

The email address that received the most spam appeared as the first email address on a web page with multiple email addresses on it. That address received 136 spams, compared to 27 for the next most spammed address. It appears that somebody may have subscribed that address some pornographic mailing lists hoping to affect the results of the survey – the address in question received 119 of its spams from the same pornographic newsletter site, and none of the other addresses received spams from that site. When you take this address out of the survey, the Australian contribution to the spam problem rises to 16%.

The effectiveness of an email address exposure for attracting spam is almost identical for posting a single message to USENET as it is for posting the address to a single web page. While this survey did not attempt to measure the effects of repeatedly using the same address for posts to USENET, anecdotal evidence suggests that repeated posts to USENET result in proportionally more spam.

Since some of the addresses used to post to USENET were posted in groups in the Australian newsgroup heirarchy, it is worth measuring the ratios for spam sent to just the addresses seeded via web pages. When these addresses are considered in isolation, the surprising result is that Australian spam accounts for an incredible 18% of all spam received at those addresses.

If we consider only American (“.com”) addresses posted to a web page, Australian spam still accounts for 11% of all spam received.

As various states in the United States ban spam, there is a strong movement to contract the spam out to other countries. Australia is unfortunately the primary choice of destination for spammers taking this approach, as is shown by the note shown below, which was caught in the CAUBE.AU spam survey on 10th April 1999. This spam claimed to be from **gh5@nla.gov.au**, and was relayed through the National Library of Australia without permission. The real sender in this case appears to have been in Las Vegas.

**NEW - AUSTRALIAN BULK SERVE9 (sic) GUARANTEED NOT TO
BE CANCELLED. NO SETUP FEE. CALL FOR MORE
INFORMATION.**

Curiously, while spam has a reputation internationally as being the medium of pornographers, con artists, and pyramid scheme participants, not a single one of the

Australian spams caught in the survey fit this profile. The most prolific Australian spammers included an automobile sales web site, an online investment magazine and a real estate investment company. Other spammers included computer retailers, a tourism promoter and a Melbourne radio station.

Analysis of the Approaches to Classic Spam

Classic spam is any form of Unsolicited Bulk Email (UBE) which is sent between parties with no prior relationship. While the term “Unsolicited Commercial Email” is often used in the United States for constitutional reasons, there is no real reason for tolerating non-commercial abusive activity, nor is there any real reason for banning non-abusive commercial activity.

Because of this, we define email spam as any email (regardless of content) which is:

1. transmitted to a large number of recipients; and
2. some or all of those recipients have not explicitly and knowingly requested those messages.

Classic spam is email spam which is transmitted between parties with no prior relationship.

Orthodox Opt-Out

Opt-out means the consumer has no option at all. Orthodox opt-out guarantees every potential advertiser at least one shot at every potential recipient. It is therefore hardly surprising that marketers who would like to use spam as an advertising technique are in favor of opt-out.

The draft model states that “*A comparison with at least one other direct marketing technique (tele-marketing) would support an opt-out approach on functional equivalence grounds.*” This is, unfortunately, incorrect – tele-marketing is not functionally equivalent to spam. Tele-marketing entails significant costs to the sender. A human must make each telephone call, and the tele-marketer must pay for the cost of the telephone call itself. The cost of tele-marketing to the marketer is significant to the marketer, and is significantly higher to the marketer than the cost to the consumer receiving a tele-marketing call. This cost creates a self-limiting feedback loop which prevents tele-marketing from reaching economically unviable levels. Increases in tele-marketing reduce the responsiveness of consumers, and reduce the capacity of consumers to deal with and accept tele-marketing, thus reducing the return to the marketer eventually to the point where the marketers’ costs exceed the return.

In the case of spam, the costs to the marketer are negligible. It is as cheap for the marketer to send a spam to one million recipients as it is for them to send a spam to one recipient, and the realised cost of sending a spam to one recipient is itself negligible at around thirty dollars. At the recipient end, the cumulative cost in time, systems and network costs exceeds the costs to the sender by several orders of magnitude. Many spammers in fact boast that they only need one positive response to make a profit on a spam run. The result is that there is no feedback loop operating, and unchecked, spam would grow quickly to economically unviable levels.

Since the purpose of the model is to define what types of behaviour will be acceptable, and what kinds of behaviour will be unacceptable, defining an “opt-out” approach would be the same as stating that “It is acceptable to spam if you allow people to opt-out after the fact.”

If we start with the assumption that it is acceptable to spam under these conditions, we need to consider the number of potential advertisers. A good way to begin with this is to start by counting the entries in both the A-K and L-Z volumes of the Sydney Yellow Pages. Then move on to the Melbourne, Brisbane, Adelaide, Perth, Hobart, Darwin, and

Canberra editions, and when those are all done do the same for all the other cities and towns in Australia.

When you have finished counting entries in the Yellow Pages, start counting the classified advertisements in the Sydney Morning Herald. Each one of these advertisements represents somebody willing to pay more than the cost of a spam run for an advertisement. When you have finished with the Sydney Morning Herald, continue with the Age and all the other daily newspapers in Australia.

When you have finished counting all of these advertisements, estimate the number of these advertisers who would use spam for their advertising if spam is defined as acceptable behaviour. A good estimate for this is “approximately every single one of them.” After all, if it’s acceptable behaviour, and it costs next to nothing to reach many more people than any newspaper advertisement ever could, what advertiser wouldn’t use spam?

Since the orthodox opt-out approach guarantees each one of these advertisers at least one shot at each mail box, the number of spams in the electronic mail box of somebody unfortunate enough to be found by the spammers would be thousands per day. At this level, the electronic mail box would be unusable. The unfortunate recipient of the spams would be unable to read all of the advertisements (nor would they be able to find important messages hidden among all those spams), let alone respond to each of them to request removal.

The natural question to ask in response to this is “Why hasn’t this happened already.” This is a simple question with a simple answer – dedicated people, and Internet Service Providers (ISPs), are spending a great deal of time making sure that people know this behaviour is unacceptable, and ISPs are backing this up by terminating service to customers who spam.

Even if it there were only one new advertiser using spam per day, the fact that an unwilling recipient received the spam is proof in itself that the consumer never had any option but to receive spam.

A government statement that opt-out spamming was OK would be nothing short of a disaster – it would counter the work that has already been done to set the expectation that opt-out spamming is unacceptable. In fact, experience from the United States has shown that when an opt-out bill passed the Senate there, spammers started using that bill as justification for their activities, and continued to use that bill as such justification even after the bill was defeated in the House of Representatives. The pro spam lobby had also planned to use the bill as a basis to take legal action against ISPs that terminated service to spammers.

In addition, a statement endorsing opt-out would make Australia a very attractive place for overseas spammers to use to send their spam, and as such would ensure that Australia’s contribution to the global problem would grow to embarrassing levels.

Additionally, some spammers use opt-out requests to build lists of people who are known to read their email, and sell these lists to other spammers. Encouraging people to respond to opt-out instructions would result in their addresses being sold for these more valuable lists, and can actually result in them receiving more spam.

Costs of Spam in the Orthodox Opt-Out Model

In the orthodox opt-out model, none of the costs of a single spam are reduced, however the time cost to a recipient is increased, and the total number of spammers can be expected to increase.

Whereas the time cost of identifying and deleting a spam was estimated conservatively at 5 seconds, the time cost of responding to a spam to opt out would be at least 30 seconds.

This gives us the following values for the costs of a single spam run to one million recipients.

| | 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 | | 8214 hours |
| Monetary Cost of Time | \$21.94 | \$180248.02 |
| Utility of Medium Cost | | Impossible to Estimate |
| Freedom of Choice Cost | | Priceless |
| Total value of estimable costs | \$82.74 | \$181,428.35 |
| Forced Subsidy | | 219,275% |

Under a policy endorsing orthodox opt-out as the “best practice”, the total volume of spam can also be expected to increase, pushing the total cost of spam to society to ludicrous levels.

Tagged Opt-Out

Tagged opt-out improves the most visible part of the problems of spam by a small amount in some ways, while increasing the costs to the recipients in other ways. The theory behind tagged opt-out is that if end users can filter out the spam using tags in the subject heading, the problem goes away, otherwise known as the “out of sight, out of mind” approach.

Due to the nature of electronic mail protocols, somebody receiving an advertisement that is tagged in the subject is forced to receive the entire message. Once a server has started receiving the message contents, which contain the subject header, it must receive the entire remainder of the message. Any attempt to abort the connection without receiving all of the data will be interpreted by the sending system as a temporary failure, and it will try to send the message again later.

If the subject tagging is being anticipated as a method for the individual user to filter advertisements, the received spams must then be stored on the ISP’s mail servers, taking up valuable additional disk space, until the user retrieves their mail.

The use of subject header tags to identify spam implies a number of obvious results:

1. that users who do not want spam will be expected to filter out the spam so they never see it;
2. that because the user is theoretically filtering out the spam, they will not be sending opt-out messages to the senders of that spam (disregarding for a moment the fact that such opting out is impossible); and
3. that the senders are then entitled to keep sending more spam to those recipients.

The clear result of this is that a tagged opt-out regime would result in rapidly rising resource costs in terms of network usage, processor usage, and disk space usage. These are all real costs, and they are real costs that are being imposed on unwilling recipients.

Costs of Spam in the Tagged Opt-Out Model

While the tagged opt-out model can in principle eliminate the time taken to identify and remove spam, it should be noted that the recipients still bear fourteen times the costs of spam that the senders bear. Additionally, a tagged opt-out model is likely to increase the volume of spam significantly, in effect transferring a significant proportion of the time costs to realised monetary costs to the recipients.

| | 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 | | In theory eliminated |
| Monetary Cost of Time | \$21.94 | |
| Utility of Medium Cost | | In theory eliminated |
| Freedom of Choice Cost | | Still Significant |
| | | |
| Total value of estimable costs | <hr style="border-top: 1px solid black;"/> \$82.74 | <hr style="border-top: 1px solid black;"/> \$1180.33 |
| Forced Subsidy | | 1,427% |

The Mythical Global Opt-Out List

Spammers, and more recently, the Direct Marketing Association in the United States, have often touted global Opt-Out lists as the solution to the problems of spam. The major web sites offering global opt-out lists include:

www.deaa.org
www.e-mps.org
www.extractor.com/removes.htm
www.optlist.com
www.safeeps.com

Global opt-out lists have been a startling failure. The original global opt-out list, run by the Internet E-Mail Marketing Council (IEMMC) turned out to be a farce, with some of its key spammer sponsors flagrantly ignoring it, and with numerous allegations that brand-new addresses that were only used to opt-out on that list were subsequently spammed. The IEMMC opt-out list was discontinued when the Internet Service Provider sponsor of the list came to the realisation that the IEMMC was ineffective, and pulled the plug on the IEMMC and on its spammer sponsors.

Global opt-out lists have two fundamental problems – to be effective, there has to be exactly one such list, and consumers have to trust the list. There have been scores of global opt-out lists offered, with over a dozen available at any one time. Only one of these has shown any promise of being trusted by consumers.

In October 1998, in response to instructions from Congress to make further attempts to use non-legislative means to deal with the problems of spam, one spam fighter produced a new opt-out list called SAFEeps. SAFEeps was designed to overcome the problems of previous opt-out lists. It was operated by somebody who was trusted by both sides. It was operated in such a way that it could not be used as a fresh source of addresses. It had the endorsement of major Internet Service Providers and opponents of spamming.

Rodney Joffe, a long time member of the DMA, the former owner of Internet Service Provider “Genuity”, and a trusted participant in the anti-spam community, created

SAFEeps. Prior to starting SAFEeps, Joffe had been operating SAFEmps and SAFEtps – computerised services for cleaning lists against the DMA’s mail preference service and telemarketing preference service databases. These services were popular with the direct marketing community because they were the least expensive of all of the list cleaning services. Joffe had therefore already established the trust of the direct marketing industry. This was the first time a global opt-out list was created by somebody with established credibility in the direct marketing industry.

Supporters of SAFEeps at the time of its announcement included the major email service provider Hotmail and spamming software company Extractor Marketing. Hotmail was represented at the press conference announcing SAFEeps, endorsing SAFEeps as the best possible opportunity for a global opt-out database.

SAFEeps also had the conditional acceptance of groups opposed to spam. Joffe consulted with CAUCE and other anti-spam activists, and J.D. Falk, a board member of CAUCE said “We’re not sure this will work. But if any such scheme does work, it will probably be this one. If it doesn’t, at least it will prove that something like this will not work.”

The newest of the global opt-out lists is the e-MPS, the DMA site launched on the 10th of January.

The DMA originally announced that they would be introducing a global opt-out list for spam in July 1997². In December 1998, when the the DMA opt-out list was still not operational, a group of activists opposed to spam met with the DMA in Washington, DC to discuss the spam issue with the DMA. One of the activists present was Rodney Joffe, owner of SAFEeps.

As a result of that meeting, the activists proposed restructuring SAFEeps as a cooperative, with a board composed of representatives of the Internet Service Provider industry, the direct marketing industry, and consumer representatives. In addition, the activists prepared a proposed bill that would have enforced the use of that list, based on an understanding from the December meeting that the DMA would support such a bill.

On February 2nd, 1999, the DMA wrote to the activists stating that:

“We are concerned about the nationwide list proposed in the Draft. A legislatively mandated single national database could be aministratively and legally burdensome, expensive, and ineffective. The approach in the Torricelli Bill that does not mandate a single uniform database is preferable to The DMA....

“Additionally, The DMA does not support legislatively mandating adherence to "opt-out" lists.”

In effect, the DMA has stated that they prefer to have multiple databases, and that they oppose any legal requirement to use them. In this context then, the DMA’s opt-out list is worthless, since the only people who might use them are DMA members, and the DMA membership is generally aware that spamming is bad business, and are avoiding the practice entirely. So why did the DMA produce an opt-out list at all?

In fact, the DMA appear to have expended a great deal of effort avoiding creating an opt-out list. The SAFEeps opt-out system, a superior system in all respects, with a far more professional web site, was operational within 3 months of the first discussions proposing it. The DMA took 30 months – 10 times as long – to produce their service. Even by the most generous possible analysis, this can only indicate two possibilities – the first being that the DMA have the most incompetent staff imaginable, and the second being that they were deliberately delaying the service for use at the 11th hour in a desperate attempt to appear to be doing something constructive.

² <http://www.zdnet.com/intweek/print/970714/inwk0048.html>

Additionally, the DMA opt-out list does not pass the minimum requirements for such a list. The DMA is not trusted by consumers, they do not have the support of any section of the ISP industry, and they do not have any support from anti-spam groups. They do not even have the support of the direct marketing industry, with many players in the industry actively deriding the service. In fact, organisations deriding the DMA's efforts include the Internet Service Provider Consortium (ISPC), CAUCE, the Forum for Responsible and Ethical Email (FREE), JunkBusters, the Mail Abuse Protection System (MAPS), and most damning of all, DM News, the magazine of the direct marketing industry, whose feedback page³ on their web site directs people with enquiries about direct marketing to contact the DMA.

In the end, unless a single list is globally mandated, there is no such thing as a global opt-out list. Furthermore, given that such a list would itself have an intrinsic value if it were used in an inappropriate manner, it would have to be managed by an organisation that is trusted by consumers and by consumer representative groups. The DMA is not a trusted organisation.

The concept of a global opt-out list lacks support from both consumer organisations and lacks real commitment from the DMA. Consumer organisations have no faith in such lists, and consumers are unlikely to trust the DMA list. The DMA does not endorse a mandated single global list, and thereby makes it clear that their own e-mps is not intended to be in any respects a global list, but merely is intended to be one more of the many.

Costs of Spam in the Global Opt-Out List model

Since such a scheme appears to be essentially impossible, and not to be supported by either side in this issue, it can have no effect on costs.

Opt-In

The principle behind opt-in is simple, and this is the approach endorsed by all consumer representative organisations and by all responsible direct marketing experts.

In opt-in, no marketer may send email in bulk to recipients who they do not have a prior relationship with, and who have not explicitly requested the email. Opt-in gives consumers the exclusive right to decide how their electronic mail box will be used. The alternative – opt-out – gives marketers the exclusive right to decide how the consumer's electronic mailbox will be used. Clearly the consumer has a superior claim to this right.

When a spammer states that they believe opt-out is the appropriate method of controlling spam, they are in reality attempting to assert that the marketer has a superior claim to the consumer over what should go in the consumer's electronic mail box. That claim is quite clearly absurd.

Spammers oppose opt-in because it makes it harder for them to build up lists of people to market to. It does not, contrary to what they might claim, make it impossible – there are numerous services available that have successfully done this, and many vendors have done it themselves. The surprising assertion that spammers like to make is that they should not have to do any work, or incur any expense, in order to gain a business benefit from the rest of society.

Costs of Spam in the Opt-In Model

When we analyse the costs of spam in the opt-in model, considering the costs that the consumer is forced to bear, the inherent fairness of that system is striking. Since the

³ <http://www.dmnews.com/html/Feedback/>

consumer only receives spam when they have made the choice to receive it, there are effectively no forced costs imposed on the consumer.

| | Sender | Recipient |
|---|----------------|---------------------|
| Data Transmitted | 5000MB | |
| Message Transmission Costs | | Eliminated |
| Transmission Overheads | 320MB | Eliminated |
| Overheads Cost | \$60.80 | Eliminated |
| Data Storage | 5000 bytes | Eliminated |
| Data Storage Cost | \$0.0017 | Eliminated |
| Human Resource Time to Send | 1 hour | |
| Human Resource Time to identify as spam | | Eliminated |
| Monetary Cost of Time | \$21.94 | |
| Utility of Medium Cost | | Preserved – No Cost |
| Freedom of Choice Cost | | Preserved – No Cost |
| Total value of estimable costs | \$82.74 | \$0.00 |
| Forced Subsidy | | 0% |

The result is a forced subsidy of zero – which is without a doubt the fairest possible option. No person should be forced to bear any part of the discretionary business expense of another.

Premptive Opt-Out – The SMTP Banner

In 1998, CAUCE proposed a compromise position, known as the “SMTP Banner Notification Proposal”⁴. In this proposal, the operator of an Internet mail server can place key text in the banner message that is transmitted at the start of any mail transaction. The key text indicates any of the following:

| | |
|-----------------------|---|
| NO UCE | The site does not accept unsolicited email of a commercial nature without a prior and ongoing relationship. |
| UCE POLICY url | The site may accept UCE, subject to the policy displayed at the given URL. |
| NO UBE | The site does not accept unsolicited email transmitted in bulk without a prior and ongoing relationship. |
| UBE POLICY url | The site may accept UBE, subject to the policy displayed at the given URL. |

For example, the mail server for **cauce.org** provides the following SMTP banner:

```
220-unagi.cybernothing.org ESMTP mail server ready, pc.example.com [10.0.0.1]
220 [NO UBE C=US L=CA]
```

Accordingly, **cauce.org** does not accept unsolicited email sent in bulk, but will accept commercial email as long as it is not sent in bulk.

While the SMTP banner operates at the server level, it can be used to achieve per user settings for an Internet Service Provider. An ISP wishing to give the choice to its users can offer two domain names for electronic mail, and allow its customers to elect to have their email address enabled on the domain that permits UBE or UCE. For example, an

⁴ <http://www.cauce.org/proposal/index.html>

ISP with a domain name of “**example.com**” could create a subdomain called “**spamme.example.com**”. The user “fred@example.com” can elect to have email to “fred@spamme.example.com” either accepted or rejected, and if he chooses to have such mail accepted he can provide his email address in that form. In this way, individual consumers can make, and in effect publicise, their choice.

CAUCE, together with Troy Rollo, chairman of CAUBE.AU, have produced software that allows a person who plans to use UBE or UCE to check their list against the SMTP banner. This software is available free of charge, with source code. The licence for the software allows anybody to incorporate the software into their own programs without any fee or even acknowledgement.

The SMTP banner provides a workable method of expressing preferences that is available today, and does not require any centralised database.

Costs of Spam in the SMTP Banner Model

The costs of spam in the SMTP banner model have the potential to reduce the costs significantly, while leaving a small subsidy in place. In this case, we will consider only the costs related to the attempted transmission of a spam to one million users, all of whom are protected by an SMTP banner. In practice, this removes all forced costs from the recipients except transmission overheads, and even the transmission overheads are significantly reduced.

| | Sender | Recipient |
|---|----------------|---------------------|
| Data Transmitted | Eliminated | |
| Message Transmission Costs | | Eliminated |
| Transmission Overheads | 200MB | 200MB |
| Overheads Cost | \$38.00 | \$38.00 |
| Data Storage | 5000 bytes | Eliminated |
| Data Storage Cost | \$0.0017 | Eliminated |
| Human Resource Time to Send | 1 hour | |
| Human Resource Time to identify as spam | | Eliminated |
| Monetary Cost of Time | \$21.94 | |
| Utility of Medium Cost | | Preserved – No Cost |
| Freedom of Choice Cost | | Preserved – No Cost |
| Total value of estimable costs | \$59.94 | \$38.00 |
| Forced Subsidy | | 63% |

CAUBE.AU’s Recommendations for Classic Spam

The title of the document under consideration is “Building Consumer Confidence in Electronic Commerce: A Best Practice Model for Business.” Clearly given this title, only one of the options mentioned in the appendix to the December draft has any possibility of fitting within this document.

Opt-out, both in its orthodox and tagged forms, is neither the current best practice, nor is it capable of building consumer confidence. Best practice is clearly opt-in, and despite what the spammers would have people believe, this is the only approach endorsed by consumer groups, because it is the only approach that gives consumers confidence.

Even the direct marketing industry now acknowledges that the only ethical method of marketing by electronic mail is opt-in. On January 10th, 2000, Tad Clarke, editor in chief of DM News, a direct marketing magazine, wrote:

“... the launch today of [the DMA’s] E-Mail Preference Service isn’t the answer. Spammers won’t use E-MPS, and the companies responding properly to current market conditions don’t need it. Those conditions? Opt-in e-mail marketing”⁵

On December 29th, Elaine Murphy, CEO of HyperGold, wrote to the CEO of the DMA, stating:

“I am writing to you as a former executive in the mailing list industry, a former long-term member of the DMA and as the current owner of an Internet marketing and development company... It seems to me that your advocacy of [spamming] reflects badly on your organization and that your protection of it sends a message to the e-mail-knowledgeable public that you may not have intended.

“...Any prestige the DMA now enjoys with the business world at large will most certainly be tarnished when the scope of this expensive practice is realized.”⁶

On January 10th, Nick Osborne, a regular writer for e-commerce magazine “ClikZ”, wrote:

“The good news is that the Internet provides you with the largest and most connected network of prospective customers imaginable...”

“The bad news is that it's not your network...”

“When you understand that the network is theirs and not yours, you understand why opt-in email lists are the only way to do things and not just a fleeting fad.”⁷

The trend is clear, and it is difficult to find any responsible writers who state otherwise – opt-in is the current best practice, and in fact is considered the only way to do email marketing by responsible direct marketers. Accordingly, the only approach that can be defensibly endorsed in “Building Consumer Confidence in Electronic Commerce: A Best Practice Model for Business”, is opt-in. This should be a minimum requirement for industry codes relating to electronic commerce.

In addition, since the SMTP banner is available as an unambiguous “No Hawking” sign, and CAUCE and CAUBE.AU have produced public domain software (including source code) to check the SMTP banner, failure to respect this banner can only be seen as willfully trespassing, in the same way as a door-to-door salesperson ignoring a “No Hawking” sign would be trespassing. Accordingly, failure to respect the SMTP banner should be prohibited and subject to a substantial fine.

The Problem of Acquaintance Spam

Acquaintance spam is email spam that is sent between parties with a prior relationship. While CAUBE.AU is not recommending a legislative approach to dealing with acquaintance spam, this practice does already appear to be inconsistent with the National Privacy Principles, and does have a deleterious affect on consumer confidence. Furthermore, acquaintance spam is an extremely amateurish approach to customer relationship management that actually produces massively negative value for vendors using it compared to simple alternatives that give the consumers up-front choices.

⁵ <http://www.dmnews.com/articles/2000-01-10/5869.html>

⁶ <http://www.dmnews.com/articles/1999-12-27/5786.html>

⁷ <http://gt.clickz.com/cgi-bin/gt/cz/cz.html?article=1169>

There have recently been several studies on consumer attitudes to acquaintance spam. The groundbreaking study was the April 1999 edition of Cognitiative, Inc's quarterly study *Pulse of the Customer*⁸. Other studies have since been undertaken by Jupiter Communications, Intelliquest, and MessageMedia⁹.

The MessageMedia study consolidates some of the other studies, and states the attitudes of consumers clearly:

“Spam isn't necessarily defined by the type of content the messages contain; it is generally defined by whether the recipient thinks it's spam. If he wasn't expecting to hear from you – in other words if he didn't ask for the e-mail – it's spam... Sending unsolicited e-mail, even to existing customers... is viewed by many consumers as a violation of online privacy.”

Businesses worldwide are now starting to realise that acquaintance spam is incredibly bad for business, and that getting permission from your customers first – permission marketing – provides far bigger returns to the business anyway¹⁰.

The Effect of Acquaintance Spam on a Business

The Cognitiative study was the first to attempt to measure the reaction of consumers to acquaintance spam. In an effort to ensure that they were really measuring the attitudes of every day consumers, Cognitiative deliberately excluded employees of ISPs, computer hardware and software companies, market research firms and e-commerce companies. The Cognitiative study found 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.”

The study also reveals that only a small fraction of the people who react this way will tell the business. Most of the 33% will silently filter out the advertisements in their email software, while making a mental note to avoid that vendor.

The story changes when a web site uses the forced choice approach (described below). When an American hotel and casino chain introduced a forced choice, they found that they had an opt-in rate of over 91.5%. Since these people have chosen to receive the marketing material, they will actually look forward to it, and the vendor will not get filtered, nor will they lose the customer.

Dan Birchall, the administrator of the web site in question, came up with Birchall's laws of mass email to customers:

Birchall's first law: If you want people to complain when they get your e-mail, choose opt-out. If you want people to complain when they don't get your mail, choose opt-in.

Birchall's second law: If you choose opt-in, be sure you have a system in place that can handle, or easily be upgraded to handle, large numbers of loyal customers. If you choose opt-out, this won't be a concern.

Some quick arithmetic reveals that if a vendor takes a strictly opt-in approach to emailing their customers, around 25% of their customers will change from somebody who will actively avoid the vendor to somebody who will actively request email from the vendor

⁸ http://www.cognitiative.com/contentPages/Pulse_Rpt_archive.html

⁹ http://www.messagemedia.com/rc/case_studies.shtml

¹⁰ <http://news.cnet.com/news/0-1005-200-1539071.html>

and will become a loyal customer. Contrary to the fear of marketers, forced-choice actually produces significantly better results than requiring customers to opt-out.

The Effect of Acquaintance Spam on E-Commerce

Acquaintance spam operates to the severe detriment of e-commerce in general. It significantly erodes consumer confidence, and actually reduces the pool of consumers making purchases online.

The Cognitative study found that:

“Unsolicited email is considered an invasion of privacy and has actually become a serious problem for some customers, particularly among business customers. It often impacts people’s willingness to register on sites, an in some extreme cases has prevented people from buying online.”

According to MessageMedia, the Jupiter Communications study found that:

“64% of online customers are unlikely to trust a web site, even when the site promotes a privacy policy.”

They go on to report:

“Combine that with the results of another study, one in which Intelliquest found that 63% of respondents agreed with the statement ‘If I buy online, I’ll end up getting junk e-mail,’ and you can see why so many consumers use fake e-mail addresses when buying online.

“Therefore you need to give consumers a reason to trust you, and one of the best ways to build that trust is to use e-mail wisely...”

“Avoiding spam is also good business practice – when you spam, not only do you risk angering your customer base, you ultimately hinder the growth of e-commerce.”

Ultimately, vendors who spam their customers without asking make their customers think twice about buying online again. This stunts the growth of e-commerce by reducing the total size of the customer base.

The Best Practice Approach – Forced Choice

Historically, web sites have used a check-box to allow customers to opt-in or opt-out of email solicitations. Unfortunately, the check-box has a major flaw – if the customer does not change it, there is no way to tell if it was because they chose to leave it alone or because they didn’t notice it.

The best practice approach, and an approach that is rapidly becoming the standard, is to use a forced choice. This involves using radio buttons to indicate the consumer’s choice, with none of the radio buttons checked by default. If the consumer fails to make a choice, the web site can ask them to make the choice again when the customer submits the form.

More information on this approach can be found on the CAUBE.AU web site at <http://www.caube.org.au/buspref.htm>. In summary, a form that uses this best practice method will have a section on it that looks like figure 1.

| | |
|---|--|
| <input checked="" type="radio"/> Please don't send me any announcements. | If you check this, we will only send you order confirmation and status information. |
| <input type="radio"/> Send me critical announcements. | If you check this, we will also send you important announcements you really need to know, like a change in our web site name, or if we merge with another company so somebody else has your private details. You will not get other announcements. |
| <input checked="" type="radio"/> Yes, please send me all announcements! I want to receive special offers! | If you check this, we will send you all announcements , including important announcements and special offers , with discount vouchers for products at our online store. |

Figure 1 - A forced choice form

When a consumer completes a forced-choice form like this, not only can the vendor be sure that the consumer has made the choice, but they can be sure that the consumer has understood the choice they are making. Furthermore, this form makes it clear to the consumer that the vendor is serious about protecting their privacy – and this is a good way to win the trust of the consumer.

It should be noted that the National Privacy Principles state that:

2.1 An organisation should only use or disclose personal information for a purpose other than the primary purpose of collection (a 'secondary purpose') if:

- i. **the secondary purpose is related to the primary purpose of collection; and**
 - ii. the subject of the information would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
- a. **the individual has consented to the use or disclosure; or**
- i. the organisation uses the information for the purpose of direct marketing;
 - ii. **it is impracticable for the organisation to seek the individual's consent before using the information; and**
 - iii. the organisation gives the individual the express opportunity at the time of first contact, and thereafter upon request, and at no cost, to decline to receive any further direct marketing communications; and the organisation complies with the individual's wishes; ...

In effect, the privacy principles require that an organisation that plans to use personal information – such as an email address – for marketing purposes must seek the individual's consent before doing so where it is practicable. Seeking this consent on a web page when accepting an electronic mail address is not only practicable – it is trivial, and by far the most effective way to do this is with the forced-choice approach.

CAUBE.AU's Recommendations for Acquaintance Spam

In the context of "Building Consumer Confidence in Electronic Commerce: A Best Practice Model for Business," it is appropriate to deal in some way with acquaintance spam. There is ample evidence that it adversely affects consumer confidence, and the current best practice – which is also the most successful approach for customer retention – is forced-choice.

Accordingly, the document should mention forced-choice as the best practice for building email marketing lists from customer contacts and orders.

While CAUBE.AU does not believe that industry bodies would be willing to produce codes of practice that required forced-choice – to the detriment of their members – we do believe that “Building Consumer Confidence” should either require or strongly recommend that industry codes make mention of forced-choice being the best practice, and the approach that is likely to generate the best results both for their members’ businesses and the industry and e-commerce in general

Industry codes should at an absolute minimum mention that to use email addresses collected on a web site for marketing purposes, the member must give a clear option at the time of collection in order to be operating in accordance with the National Privacy Principles.

Conclusion

CAUBE.AU has specific recommendations in three areas in relation to spam:

1. in the case of unsolicited bulk email to parties with no previous and ongoing relationship with the sender, industry codes should require a strictly opt-in approach, as this is the widely acknowledged best practice at this time;
2. unsolicited bulk email sent in violation of an SMTP banner notice should be prohibited, with a substantial fine for violations; and
3. industry codes should make parties collecting email addresses on web sites aware of the best practice approach of forced choice, and the fact that this is in fact the most effective approach to customer retention, and the codes should strongly encourage the use of that approach. Codes should remind businesses that in default of the forced-choice approach, the National Privacy Principles mandate at a minimum that a clear opportunity to make a choice be provided at the time of collection.