Outblaze Limited
Suite 1166-1168 Cyberport 2
100 Cyberport Road
Hong Kong

March 20, 2006

Communications and Technology Branch
Commerce, Industry and Technology Bureau
2/F Murray Building
Garden Road
Hong Kong
(Attention: Assistant Secretary (B))

(Submitted via email to uem@citb.gov.hk)

Dear members of CITB,

We wish to offer our comments in response to the Consultation Paper on Legislative Proposals to Contain the Problem of Unsolicited Electronic Messages issued by The Commerce, Industry and Technology Bureau in January 2006.

Outblaze is broadly supportive of the adoption of anti-spam legislation in Hong Kong, especially anti-spam legislation based on the successful Australian Anti Spam Act of 2003. We welcome the adoption of an anti-spam law in our territory, and we consider it essential to curb the menace of spam. We do, however, wish to express strong reservations on legislative proposals based on the opt-out approach.

A note on the economics of spam: Why opt-out is not feasible

As we previously expressed in our response[1] to OFTA's consultation paper[2] on a proposed anti-spam law, we regret the determination of the Hong Kong SAR to choose opt-out versus opt-in as the basis of proposed anti-spam legislation. We feel it is necessary to point out that, while ostensibly business-friendly, legislation based on opt-out has a high likelihood of proving problematic for multiple parties.

Opt-out email campaigns are based on the assumption that email marketers are entitled to send

[1] http://www.outblaze.com/antispam/Outblaze_Response_to_OFTA_spam_consultation_paper.pdf
[1] http://www.ofta.gov.hk/report-paper-guide/paper/consultation/20040625.pdf

unsolicited bulk email messages to internet users, with the provision that any user who expresses a wish not to receive such email messages may request to be removed from the email marketer's list; in such cases marketers are theoretically under obligation to honour all requests for removal.

Unsolicited Bulk Email (UBE) messaging enjoys strong support among email marketers for one important reason above all others: the costs incurred by the senders of UBE are disproportionately (and deceptively) low, rendering UBE campaigns extremely attractive marketing investments. The problem arises when one considers that the collective costs incurred by ISPs, businesses, and individuals who receive, store and download UBEs are far greater than those incurred by email marketers.

Traditional off-line marketing methods like bulk postal mail and telemarketing are based on a "sender pays" model: the sender must bear marketing costs. **In the case of UBE, however, there is a nearly 100% transfer of messaging cost from marketer to recipient:** service providers, businesses, and email users are forced to bear the majority of the costs for the marketing efforts to which they are (willingly or unwillingly) exposed. UBE's artificially low costs to senders are the result of a transfer of marketing costs from marketers to the unwitting recipients, each of whom has no choice but to bear a fractional part of the total campaign costs.

This cost transfer, originating from a legacy of trust in the current architecture of the Internet and global email systems, remains in place thanks to two factors: one is the widespread ignorance with regards to the mechanics and economics of email, and the other is the strong lobbying of various powerful marketing and business groups interested in extending the status quo (in which large sums of money are exempted from marketing budgets because consumers and service providers are forced to subsidize marketing efforts).

An opt-out approach to the problem of spam in effect argues for a continuation of the present (and iniquitous) *de facto* subsidy of marketers' email campaigns by the recipients of those campaigns. The main problems we are concerned with are the fundamental unfairness of asking a recipient of unsolicited marketing to pay for being advertised to, and the high possibility for abuse in such an approach.

In traditional off-line bulk mail, marketers must organize and pay for the distribution of their materials, usually by paying for postage or, in the case of telemarketing, telephone charges and personnel costs. On the Internet, owing to the aforementioned design legacy of operation on a trusted network, charging for bulk email is currently not feasible.

There are a few proposed online stamp and similar payment schemes for email under investigation

(e.g., the e-postage scheme of Daum Corporation in Korea, or the Goodmail system under trial by AOL and Yahoo). The effectiveness of such methods has yet to be measured but is estimated to be, at best, limited, and the costs appear to outweigh the benefits, with the (currently) sole exception of certification and delivery assurance for high value "transactional" email such as airline tickets, online billing notifications, and bank statements.

Today it remains entirely too simple for any entity (business or individual) to market products and services for free by sending unsolicited bulk emails to large numbers of users. An opt-out based approach to addressing the spam problem will do little or nothing to reduce this problem: the recipients of UBE will continue to indirectly (and unknowingly) subsidize marketing efforts targeted at them, even if the opt-out system is otherwise free from abuse.

The sole costs marketers face when sending email solicitations are basic Internet connectivity and the cost of email-sending software. Further downstream, however, email needs to be handled, filtered, sorted, moved, and stored, substantially raising costs for bandwidth, disk space, administration, and technical support. Mail server operators must meet these extra costs and charge their users higher fees in order to avoid operational deficits.

Succinctly put, email users are paying higher Internet fees in order to be able to receive spam. The vast majority of users are unaware of this arrangement.

As long as this unfair transfer of cost from bulk emailer to end-user is possible, there can be no such thing as legitimate unsolicited commercial email. Contrary to the definition being put forward by several marketing associations, in particular the US based Direct Marketing Association (DMA), spam is not just email with pornographic or fraudulent content; spam is **all** unsolicited bulk mail *irrespective* of its content. The **operational** problems and costs brought about by spam remain exactly the same regardless of the nature of the content being transmitted (email needs to be sorted, filtered, handled, moved, stored, and processed no matter what its contents). On the user end, spam remains an annoyance and a detriment to productivity regardless of the contents of messages.

An opt-out approach puts email users and operators at risk of considerable inconvenience and expense, especially when we consider that the protective aspects of the telemarketing "Do Not Call" list do not extend to email: there is no meaningful "Do Not Email" list, nor is there likely to be one in the future. Despite the utility of such a list at first glance, after closer examination the US Federal Trade Commission and the CITB have reached similar conclusions on the infeasibility of a Do Not Email list.

In the context of the US CAN-SPAM opt-out based act, we must point out that an opt-out system under the present circumstances effectively forces email users to manually unsubscribe from every single marketer that has their email address on file. There are tens of thousands of businesses operating in Hong Kong, ranging from corner shops to Fortune 100 companies. The codification of an opt-out anti-spam law will encourage high numbers of marketers and aspiring marketers to launch unsolicited email marketing campaigns of their own.

On one hand this may be seen as a development of some value, because it is likely to stimulate business activity to some degree while keeping marketing costs *for businesses* relatively low. On the other hand, if users were to receive email solicitations from even a small fraction of these businesses, they would find their mailboxes flooded with advertisements and would need to manually unsubscribe from each advertisement by clicking on a URL, sending an email to a particular address, or actually having to call a telephone number or write a letter to request removal from a marketing list.

We therefore believe the best possible solution to the spam problem is to require that commercial email be solicited, either directly between a consumer and a marketer, or via an opt-in process in which an end-user explicitly and unequivocally agrees to receive email offers and announcements. Opt-out is merely a half-measure for the existing problem because end-users are only entitled to send a request for removal from a distribution list once they are already on it – in other words, they must submit to the harassment and added costs of unsolicited bulk email each and every time a marketer puts their email addresses on a marketing list – and there is no shortage either of marketing lists or of marketers.

One of the most important rules that email users are encouraged to follow is to avoid responding to spam, because the response usually alerts the spammer (by email or by web link to a purported unsubscribe web page) that a particular email account is “active”. Once an account is determined to be active its value jumps considerably for marketers, and is more likely to be sold or traded to other marketers. Several years ago professional spammers co-opted the opt-out process in to an efficient system for confirming the validity of email addresses, long before any country made it a legal requirement to provide opt-out options. It is therefore rather puzzling to see the opt-out approach being proposed and defended yet again when in the past it has failed so clearly and consistently.

As one of the world's largest email and anti-spam operators, it is our duty to emphasize that opt-out is not a viable solution to the problem of spam, and we strongly suggest that an opt-in approach be pursued, possibly with the proviso of a prior business relationship being adequate evidence to qualify a marketing campaign as opt-in.

Circumstances and examples where opt-out of email addresses is infeasible

- Many providers of mobile telephony or "push email" now provide email interfaces to their standard SMS or other text messaging service. Email sent to a particular email address may actually be forwarded to the user's mobile phone or handheld device.

    - Therefore, providing a Do Not Call exclusion list for (say) telephone numbers while not providing a similar system for email is likely to result in email users receiving spam on telephony devices, potentially increasing roaming data transfer charges for the questionable privilege of receiving spam

- Many opt-out email lists, particularly those compiled by purchasing mailing lists or harvesting email addresses, contain an inordinately high percentage of invalid and non-existent email addresses. Even legitimately compiled mailing lists (if not properly pruned by automatically unsubscribing persistently bouncing addresses) will over a period of time accumulate a sizeable number of invalid email addresses. It is self evident that an email address that does not exist at all cannot reasonably be expected to opt-out from a mailing list.

    - However, email providers and email server operators are still forced to receive and process email destined for non-existent addresses before finally "bouncing" the email back to its origin (the online equivalent of "return to sender, no such addressee here")

- Unscrupulous spammers treat opt-out requests as signals that the email addresses they are targeting do indeed exist and are being actively read and replied to (i.e., they are "active"). Typically, email addresses that opt out of unsolicited bulk email find themselves receiving *more* spam, not less (hence the conventional wisdom of never replying to spam).

Suggested additional measures to adopt in case of approval of an anti-spam law based on opt-out

We note that the Hong Kong government appears intent on implementing the proposed anti-spam opt-out legislation. We would therefore like to suggest a number of measures that will mitigate several gross abuses of the opt-out process common among spam operations, and would further suggest that the Hong Kong Government put these safeguards in place to protect the privacy and interest of email users. Although it would be preferable to commit to opt-in initiatives, given the

current circumstances we believe it is important to achieve an equitable balance between a business-friendly law and one that protects the interests of email users, service providers, and network operators.

In order to protect the privacy of users, adequate data protection measures must be in place and must be cited in relevant anti-spam legislation. Overzealous marketers must be prohibited from sharing or selling user data without user consent. Measures to assure data privacy include:

- Prohibition of the harvesting, sale and purchase of email addresses for the purpose of sending unsolicited bulk email.
- Legislation that clearly restricts the repurposing of collected email addresses.
- Imposition of severe restrictions on sharing email addresses with any entity other than those clearly stipulated in prominently published privacy policy available on the marketer's web site.

Sharing an email address should only be possible with the explicit consent of the owner of the address. It is our position that personal user data (such as marketing preferences or profiles that the email marketer may have built up) is strictly private and must fall under the aegis of privacy and data protection laws.

Opt-out requests must be, as far as possible, honored instantly and automatically on receipt. Further, while we are aware that a Do Not Email list remains infeasible, the proposed Do Not Call list for telephone and fax must be extended to email in select cases, especially at a domain level. Of particular importance are domains belonging to providers of mobile or push email services as discussed above, and corporate email domains for which company policy mandates that employees use their email address only for work related purposes. In such cases it should be possible for the domain owner or service provider to add their entire domain to a Do Not Call or other centrally managed suppression list.

We strongly endorse the suggestion that senders of bulk email control their email sending rates, and we also suggest that they provide facilities / preferences settings for their list members to determine the frequency at which they expect to receive marketing emails (this in order to avoid straining the recipients' mail servers, or causing inconvenience by sending too many emails to a mailbox).

We stress that simply reducing the number of emails that people are allowed to send in a fixed interval of time is not an adequate solution, especially as several spam systems now utilize the concept of "horizontal scaling" to get around rate limit restrictions on the amount of email that they

are allowed to send out. Instead of sending out several thousand emails per account per day, a spammer may open up several thousand accounts and send no more than twenty emails per account per day. We therefore applaud the decision to restrict the practice of allowing "scripted" or automated creation of accounts.

The use and distribution of "spamware" – bulk email sending software that is primarily used to send spam, and has characteristics that are only of use to spammers, must be prohibited. A Virginia state law[3] that prohibits the use or sale of spamware is noteworthy; its wording may serve as a reasonable starting point for a similar Hong Kong provision.

Features that are commonly found in bulk email software that is used by spammers include but are not limited to the following:

- Header cloaking, or forgery of the "From:" and/or "Reply-to:" fields or other parts of the email header (message routing information) or any similar measure that attempts to obscure the true origin of an email in an attempt to hide the identity and origin of the spammer, and to misdirect complaints about spam to the wrong internet provider

- "Direct to MX" email sending, which uses a local bulk mail-sending engine to bypass an internet provider's SMTP servers in an attempt to avoid detection by anyone monitoring email sending patterns

- The misuse of open relays, open proxies, insecure scripts, or other insecure computers in order to send out spam email. Additionally, it would be beneficial to include the installation of so-called "malware", "spyware", "trojan horses", "spambots" and other programs in this category

- Automatic gathering of email addresses by "harvesting" - that is, by operating a script or program that will search through mailing lists or websites in order to obtain lists of email

---

3 http://www.spamlaws.com/state/va.shtml
VIRGINIA CODE TITLE 18.2, CRIMES AND OFFENSES GENERALLY CHAPTER 5. CRIMES AGAINST PROPERTY, ARTICLE 7.1. COMPUTER CRIMES, SECTIONS 18.2-152.2, 152.3:1, 152.4, 152.12 (2003)

§ 18.2-152.3:1
A. Any person who: ...

2. Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or **use** other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information is guilty of a Class 1 misdemeanor.

addresses that will then be added to a bulk email database

- The purchase or use of harvested email addresses, typically sold on the Internet as “millions CDs” with lists of up to millions of email addresses that may not actually exist

It should be noted that some of these tactics are already listed as offenses in the proposed bill, and we suggest that the use of “spamware” scripts or programs be explicit prohibited (to cover the various tools and techniques that are commonly used to commit what are already recognized as spam offenses).

We appreciate the legislative proposals that render an employer liable to prosecution for spam offenses committed by his/her agents, affiliates, or employees. These must of course take into consideration due diligence taken by the employer to prevent employees, affiliates, and agents from sending spam. We stress the example of so-called “affiliate spam”, “pay per click” schemes, and similar others in which affiliates are encouraged to advertise on behalf of their employer, and are paid a commission based on the number of orders they sell or the number of click-throughs or page visits they generate for their employer's website.

Affiliate spam, in which affiliates send out bulk email in an attempt to recruit new members and boost earning rates, is a significant problem and disconcertingly similar to various Ponzi and pyramid schemes, even sharing some of the same incentives. Earnings from a single sale or click-through to the employer's web site in an affiliate scheme is typically a trivially low amount, and therefore affiliates need to generate a high number of sales or click-throughs before they can earn significant sums; one easy way to generate sales and click-throughs is with high-volume marketing efforts such as unsolicited bulk email.

Artificial boosting of revenues from various affiliate programs is also a potent motivator for the practice of installing spyware or malware that automatically generates visits to a website by manipulating unwitting users' web browsers.

We strongly recommend close examination of claims of due diligence made by affiliate programs and operators of other work from home schemes that employ affiliates to advertise, and whose affiliates engage in unsolicited telephone, fax and/or email messaging. A preliminary indication of the validity of due diligence claims can be obtained by determining whether active membership in an affiliate scheme can be shown to earn anywhere near the amount that the affiliate scheme claims.

It must be determined whether it is possible for participants in affiliate programs to earn

subsistence wages, let alone the huge earnings claimed in the scheme testimonials. If an affiliate program does not pass this simple testing procedure it is likely that its claims of due diligence are invalid, and any defense of due diligence made by an employer may be evaluated in this light and with reference to relevant laws that prohibit pyramid and Ponzi schemes.

Conclusion

Although an opt-in approach would be considerably more effective, practical, and better serving to the public, Outblaze is in agreement with a substantial part of the draft bill and endorses these provisions with the caveats noted in this document. We strongly regret the apparent preference for opt-out rather than opt-in, and we note that the opt-out approach to date has failed to mitigate spam, however if supported by an adequate framework and properly enforced we believe the opt-out approach stands a chance to reduce the spam problem in the territory. It is our duty to note that opt-out laws set a bare-minimum standard of behavior for bulk emailers, and leave room for behavior that may cause the volume of spam to increase rather than decrease.

Sincerely,

Outblaze Limited