



Comments of the
Computing Technology Industry Association (CompTIA)
For Consideration of the Hong Kong Government Anti Spam Legislation

Introduction

In June 2004, the Office of the Telecommunications Authority (OFTA) of the Government of the Hong Kong SAR China published a consultation document addressing proposals to control the problem of unsolicited electronic messages (commonly referred to as 'spam'). The Computing Technology Industry Association (CompTIA, www.comptia.org) a global business association with 20,000 member companies in 102 countries has an active Public Policy Department with an office in Hong Kong that opened in December 2003, and commenced operations with a Regional Director being appointed in January 2004, responsible for the region encompassing Japan to India to Australia.

The consultation document sets forth the position of OFTA and the Hong Kong SAR government with respect to spam, in whatever electronic format that it takes and outlines the problem quite comprehensively, which clearly jeopardizes Hong Kong's position as a global business centre. CompTIA welcomes the opportunity to comment on paragraphs 34, 71, 75, 78 and 83 and hereby submits the following comments and questions regarding the consultation document addressing proposals to control the problem of unsolicited electronic messages.

CompTIA welcomes OFTA's anti spam initiative and looks forward to working with OFTA and government of the Hong Kong SAR to develop and implement a successful anti-spam strategy.



Background – CompTIA

CompTIA is the world's largest information and communications technology (ICT) trade association with 20,000 member companies in 102 countries, with many having operations here in Hong Kong. CompTIA's members consist of software developers, IT hardware manufacturers; application service providers (ASP's); internet service providers (ISP's) and content firms; computer industry distributors and retailers; Computer resellers; as well as training, service, and telecommunications companies. Many of our members are SME's, like many companies in Hong Kong. The Association's members collectively employ thousands of people and produce billions of US dollars worth of goods and services each year.

The promotion of policies that enhance growth and competition within the computing world information technology sector is central to CompTIA's core function. Further, CompTIA's mission is to facilitate the development of vendor-neutral standards in such areas as technology workforce e-commerce, customer service, workforce development, and ICT workforce certification. These standards enable businesses to simplify practices, reduce expenses, and compete more effectively in an increasingly complex and interconnected world. More than 800,000 individuals worldwide have earned CompTIA ICT skills certifications in PC service, networking, document imaging, training, security, (including internet security), and Internet and server technologies.

CompTIA has an active Public Policy Department with a regional office in Hong Kong, as well as Washington, D.C, Brussels, Ottawa and Sao Paulo. The Public Policy Department



works to protect and advance the interests of the international technology community before legislative, executive and judicial branches of government, and regulatory agencies.

Spam – A global epidemic

Spam – Unsolicited commercial electronic messaging - is a global scourge that has increased significantly in 2004. While no reliable data is available, according to MessageLabs, a USW based company the average global ratio of spam to desired e-mails was up to 94.5% as of July 2004 compared to 52.8% in March 2004. This volume is threatening many legitimate businesses globally, including Hong Kong and the trust and infrastructure of the global economy is at risk.

While there are distinctions, spam and e-mail borne viruses cannot uniformly be treated any more as separate problems. In many cases the perpetrators of dangerous viruses; writers, spammers and individual and organized criminals are all converging. Although the governments consultation document encompasses all electronic messaging, that sent by packet switched networks – essentially the Internet - is by far the most pervasive in volume, in terms of malicious intent, cost to both consumers and to business and threat to the security of not only businesses in Hong Kong, but the government of Hong Kong itself. For example, terrorists have been suspected to use steganography encryption within email to communicate.

The high transmission capacity of fibre networks, ubiquity of broadband connections and sheer volume of traffic when combined with convergence, means that the problem will get worse unless immediate action is taken. CompTIA would therefore urge the government through the law enforcement authorities should also consider whether new authority or new techniques



are needed to address such dangerous software downloads as ‘trojans’, ‘worms’, and spyware/adware. Such software programs, normally downloaded without the end-users full knowledge and consent, are a major source of the problem network and individual website failures since they often lead to the creation of ‘zombies’ pc’s unwittingly networked into a grid compromised by a virus or hacker to automatically send spam or are used for denial of service attacks; while no reliable figures are available, estimates are that zombies are delivering 40 percent of spam across the globe thus propagating the initial spam, according to Sophos, an Internet security/research company.

With broadband and digital convergence, millions of more devices are propagating this problem and it will get worse unless governments act in association with Industry. Addressing the problem of unwanted and illegal use in this manner requires that the HK government recognize that the solution lies far more in cross-border law enforcement cooperation and industry - government cooperation than it does in new regulations. Therefore consultation with governments, industry, appropriate international bodies such as APEC, the OECD, (Please see OECD report appended to this submission from their discussions in Busan, Korea, September 2004), ICANN, and national bodies, (in particular with China), to be effective as well as industry trade associations, general business associations operating in the area of electronic communications. the collection of solutions should be therefore seamless across borders and involve the voluntary cooperation of many consumers and businesses and not be so onerous that it becomes worse than the disease.



Paragraph 34 – Addressing the scope of the problem; the costs.

Spam accounts for between 65 - 95% of all e-mail processed by mail servers, according to Industry sources (see attachments). Dealing with spam costs companies and individuals millions of hours in lost productivity and increasingly, through fraud also millions of dollars.

With respect to unsolicited fax messages, CompTIA believes that this problem has been largely superseded in Hong Kong by mass emailing – spam – and that in terms of a cost burden to business is less of a problem today than it has been over the past 15 years.

With respect to SMS messages, the service providers as they control the gateways appear to have this problem under control from a technical perspective at the moment, for example the problem was most prevalent in Japan, but it has now largely been solved, however legislation should also cover this medium.

Unsolicited Electronic Messages - Cost factors.

The Hong Kong Internet Service Providers Association has conducted a study of their members to attempt to quantify the problem within Hong Kong.

The HKISPA study concluded that Spam is causing a potential loss to the HK economy in the region of HKD9.7Billion pa. And the loss due to spam “absenteeism” HKD6.8Billion pa, or \$22Million per day / \$13 per employee, per day. (A copy is appended of the results).

In addition to the above, the cost issue was also debated at the OECD workshop on spam in their discussions in Busan, Korea September 2004, please see a copy of the report appended.



Paragraph 71 – Addressing a code of practice for industry to reduce spam.

The facts pointed out in para's 68 to 70 relating to the code of practices are currently voluntary and we believe that as they are in the best interests of legitimate providers of the underlying infrastructure, the FTNS and mobile operators, and the ISP's, should remain so as it is in their interests not to have their local networks burdened with essentially non - revenue traffic (in the case of fax or email) or customer revolt (and therefore churn) in respect of unsolicited SMS or voicemail messages. Any legislation in this field should take into account the interest of the legitimate bulk marketing industry, and the right to privacy of individuals and corporations. At the very least there should be the principle of 'opt-out' to bulk email and clear instructions with each bulk email on how to opt out with a single email response. The US Can-Spam Act is reasonable in this regard.

In addition with the digital convergence of devices that are able to receive unsolicited messages, the carriers should be free to concentrate in technical solutions in conjunction with the hardware and software industry to address the problem.

CompTIA is not able to comment on behalf of the bulk marketing industry and we would urge that their opinions be sought on this matter.

Paragraph 75 – Anti-spam education initiatives by industry to reduce spam.

As electronic messaging, in particular mobile phones and the internet is now pervasive in Hong Kong, government initiated education from primary school level on appropriate use should be considered, increasing to secondary school where good practices can be reinforced.



In particular industry can work with schools in developing an IT curriculum that can outline the benefits and dangers of the electronic connected society and ways to combat this. With Mobile phones and therefore SMS texting ubiquitous at secondary schools in Hong Kong this would have a positive effect.

CompTIA believes there is sufficient evidence to indicate that the use of pirated products, which are either unable to receive the security patches that are developed by software companies, or the users are unwilling to update them, are a substantial part of the problem. CompTIA would urge OFTA to make anti piracy a part of such education by pointing out to all users the false economy of using products that cannot be updated and will cause them losses. CompTIA believes the messages as outlined in Para's 72 and 73 are appropriate to Hong Kong, together with the respect for Intellectual Property above.

With respect to education initiatives by the industry, defined as those that operate networks that distribute electronic messaging in any form; manufactures of hardware; creators of software or content, it is CompTIA's position that efforts that they already have initiated be expanded. That is customer awareness programs be expanded through coalitions administered by the various trade industry associations. Appropriate tax incentives could be given to organizations that participate in such programs at a level which will incentivise the businesses to allocate additional resources to the problem. For example, a dedicated email address at OFTA where unsolicited emails/adware/spyware etc could be forwarded by the public for analysis (this can be mostly automated). This can also be shared so as to source IP address etc as well as ISP's so that their problems can also be addressed should be established.



In late 2003 CompTIA polled more than 900 multinational and US based organisations across a wide range of industries, including education, financial services, government, health care, IT, and manufacturing on aspects relating to IT security, in particular internet related security breaches.

The survey showed that organisations with at least one-quarter of their IT staff trained in security reported fewer security breaches (46.3 percent) than organisations with less IT staff trained in security (66.0 percent). Among those who have invested in IT security training, 80 percent feel that their security has improved; 70 percent of those who have invested in certification feel the same way. A copy of the results is appended to this submission.

With respect to specific forms and activities; the formation of an Industry/government/law-enforcement agency partnership that addresses the key problems – and keeps up to date - as part of such a coalition with specific programmes to reach out to schools and the community as a whole.

In order to accomplish the encouragement of, and support for industry cooperation (i.e. the non-law enforcement aspects) of this effort, the HK government should establish several advisory councils with software publishers, hardware vendors, ISP's, integrators/VARs, web-hosting services, Internet Café's, content providers and others that will each address in a detailed way practical solutions that involve consumer education, industry best practices, and technology tools.



There is a responsibility for Hong Kong based companies to take reasonable technical and staff training measures to ensure that they are not unwittingly compromised and become an unwilling part of the global spam problem. CompTIA would support the certification of IT security specialists that work within all corporations as part of the overall educational approach to limit the problem.

Paragraph 78 – Technical Solutions by Industry

CompTIA's diverse industry membership from Software to Hardware companies, Telecom Infrastructure Operators and System Integrators to maintenance organisations are allocating millions of dollars to address the problem from a technical level.

Areas that are being looked at include advanced filtering, port blocking, address filtering, blacklists/white lists, respondent blocking filters, advanced content filters (Bayesian/Heuristic rules systems), greymail folders, bulk email folders, SMTP authentication enhancements, steganography encryption detection, zombie neutralizing anti virus software, and many others. Innovative products that our industry members produce to combat this problem should be encouraged and supported by the HK Government and obviously should receive appropriate Intellectual Property Protection (IPR) thus providing an incentive for commercial organisations to invest in this area.

The inclusion of truthful header information on any mass messaging should be a priority matter of concern to the hk government. To whatever extent hk law enforcement authorities feel that they lack the authority to prosecute mass email senders who intentionally



disguise their identity, then new authorities should be developed for this narrow purpose. To the extent that hk law enforcement authorities believe that they have sufficient authority to prosecute mass unsolicited email senders who deliberately disguise their identity, but lack sufficient training/certification or other resources to do so, the hk government should re-allocate resources to this area of law enforcement as a very high priority.

In addition, it has been suggested by some of our members that an 'ADV' in the header would aid in identifying legitimate bulk marketing messages and to enable technical solutions such as advanced filters to stop illegal spam. Other headers e.g.; 'ASC' could be utilized to identify legitimate associations that send regular messages in bulk to their members.

With the advent of IPV6 and non roman character language support, technical solutions will need to be able to address this and any efforts to deal with spam will have to ensure that technical remedies can be implemented in various languages and scripts.

The development of technical solutions for this problem fits within the Digital 21 framework to encourage the growth of the knowledge economy within Hong Kong. Specifically the funds made available and administered by the Innovation and Technology Commission should be made available for R&D in this area, as suggested by CompTIA in its recent submission to the Commission.



Due to the international nature of the problem, ongoing consultation with standards setting bodies, industry/academic research partnerships such as PlaneNETlab <http://www.planet-lab.org/> and other international organisations and associations representing the stakeholders in the industry and end users should be encouraged on a regular basis by appropriate government bodies working in association with Industry.

Paragraph 83– Legislative approach to combat spam.

As is clear from the consultation document an effective anti-spam solution needs to be multi-faceted, but legislation (and enforcement) is a key component. Many advanced economies including some here in the region have already enacted anti-spam laws. As an advanced information based economy, Hong Kong urgently needs to consider whether there are any legislative components to addressing spam.

As pointed out in Para's 70 to 82 of the consultation document, various jurisdictions in the more advanced OECD countries have already taken a legislative approach to Spam. Although this has been recent and therefore as pointed out long term effectiveness has yet to be measured, there has been widespread adoption of legal remedies. Most notable this has been in the EU, USA, Korea, Japan and Australia, with legislation also being considered or under implementation in Singapore, Malaysia, New Zealand, Taiwan and Thailand and the PRC. Any regulatory solutions should fully recognize that regulations will themselves only be a small part of the larger solution.

Since regulations may be enforceable only within the territorial borders of the state that enacts them, and since nearly all spam does or easily could originate from senders in other



sovereign states, no one should mistakenly believe that the problem of mass, unwanted or illegal spam will be effectively addressed through new regulations alone. This has been amply demonstrated in the many jurisdictions that have implemented new --and often very stringent-- regulations on spam or use.

In no case have any of these new regulations led to a significant decline in the volumes of spam and in all cases, despite new regulations, the volumes of unwanted and illegal spam have increased dramatically. Consequently, any new regulations or legislation should focus on ensuring that senders are truthful about their identity and that recipients have the training, technical tools and the legal right to stop receiving mail that they legitimately do not want. Thus making spamming an uneconomic proposition, with severe penalties for infringers that includes not only the originators but also the benefactors of the spam; the owners or distributors of products that are spammed. The rights to the public under the Privacy Ordinance also have to be protected.

As has been mentioned there is a criminal intent in some spam sent over the internet which has been increasing significantly, from child predation to outright fraud of the well known Nigerian 4-1-9 type. One form of illegal activity is generally described as 'phishing' and 'spoofing', the false representation of corporate email that seeks to redirect the recipient to a website that is not owned by the purported sender of the mail with the objective being to extract personal or financial information from the recipient with the intent to defraud. This has already occurred in Hong Kong. Some reports have linked such activities with organized crime and terrorist organisations. Such activities will make the public distrustful of legitimate business conducted online, including the governments e-gov initiatives, unless checked



Legislation already exists to combat the funding of organized crime and terrorism, in particular the Money Laundering Ordinance. Such legislation could be amended to take into account the above activities without significantly increasing compliance costs for legitimate businesses and organisations. In addition, as most unsolicited emails have the objective of extracting payment from the recipient, legislation to follow the money trail and seize assets can also be extended where there is fraud or a clear intent to commit fraud.

Attendees at a recent conference in the United Kingdom (October 12-14, 2004) appeared confident they can make an impact. It was expressed that similar legislation for offline "rogue traders" could be extended to their online counterparts, but that tracing spam originators remains the biggest challenge.

In the United States there has been successful prosecutions and the US Department of Justice has also just issued the first summons (October 14th 2004) specifically for unsolicited software downloads that alter the recipients PC device. The Korean Authorities have also noted a decrease in spam that the authorities attributed to an increase in enforcement activities. The US legislation has started to have an effect, stronger penalties may have more effect in containing the problem.

For any legislation to be effective, the ability of HK law enforcement agencies needs to be strengthened to be able to detect, investigate and prosecute cyber criminals, i.e. who use spam as their technique. This will involve training and certification for law enforcement agents, new facilities, new procedures for cooperation with the private sector in other words an integrated



government /industry/public partnership as all are stakeholders in combating the problem. In addition the relative legislation will have to be enacted to enable co operation with HK law enforcement agencies to be able to cooperate internationally

Therefore CompTIA would urge strong legislation to address the standards issue and also the criminal intent of spam that involves unsolicited downloads, spoofing of addresses and the creators of unofficial Websites (phishing) rather than broad legislation that would be onerous for private industry (and Government) to comply with. CompTIA would also urge wherever possible, the government's definition of illegal content be harmonized with those of other countries so that international co operation is facilitated to combat the problem.

One way to encourage bulk marketers to adopt e-mail best practices might be to provide a 'Safe Harbour' to the 'ADV'" labeling requirement for those companies who are members of a voluntary industry best practices group. It is likely that industry organizations will emerge that will compete on the basis of the e-mail practices they certify and the strength of their enforcement. Thus, legislation should identify basic components that industry guidelines should address, such as notice and 'opt in/out' obligations, but permit those in legitimate industries to take the lead in developing the specific guidelines within such parameters.

Identification considerations

Similar to unsolicited postal offers, there is also a requirement to be able to identify the sender so the recipient can request to be removed from the sender's bulk mailing list and also to provide a trace route to intercept and prevent fraud. Therefore each page of any unsolicited electronic message that is delivered in Hong Kong should bear a clear identification of the sender, being at minimum;



- The originators Business Registration Certificate number
- The originators name of their business or personal name if not registered
- The originators postal address
- The originators correct email, telephone and fax number
- For Hong Kong companies, the originators Business Registration Certificate number

If legislation is needed, it should be broad so as to cover future technology advances and therefore should be neutral as to delivery methods such as voice, video or email/fax/SMS, and address and concentrate on the core problems above.

Such legislation should provide both civil remedies and damages and in the case of fraud or an intent to defraud, appropriate criminal remedies should be available.

With the above in mind, we would like to ask OFTA the following:

1. Ref a 78, Technical Solutions. Given that software underlies many of the technology areas to address the above, will the Hong Kong Government through the various strategies such as Digital 21 and the Commission on Innovation and Technology, support R&D centres that develop commercial software products or applications that will enjoy copyright and/or patent or other appropriate Intellectual Property (IP), protections for the developers? It is CompTIA's hope that there is not any funding preference to favor open source software-based solutions (OSS) over proprietary or hybrid-based commercial solutions.
2. As the consultation document outlines that spam needs an international approach, (para's 86 to 93), and recommends working with government sponsored organisations such as OECD and APEC, and also supports WSIS principles.



Will industry associations, such and CompTIA for the IT related industries, be consulted at the appropriate time with respect to the collective input of association members on anti spam policy?

3. Going forward, we note that the bulk of the number of projects funded by the ITF, 190, have been IT related. Will the ITF continue to encourage and provide funding for commercial/proprietary software projects that will have potential to address the problems contained within the anti-spam consultation document?

CompTIA looks forward to working with the Government of the Hong Kong S.A.R. Government and OFTA in the adoption of a comprehensive anti-spam policy that will be technologically vendor and platform neutral and employs a technology, education and legal solution to this most pressing problem.

CompTIA Hong Kong Limited
18/F One International Finance Centre
1 Harbour View Street
Hong Kong SAR

www.comptia.org www.softwarechoice.org