Japan gets tough on mobile spammers and scammers

By Alan Pedersen

MOBILE SPAM EN-MASSE has become the pariah of one of the world's most technologically innovative societies. Enraged consumers and disruptions to telecoms networks have now forced both the government and industry to tackle to problem head on.

In an attempt to curtail the rising number of complaints from mobile phone users, two new laws regulating the use of unsolicited commercial e-mail over mobile networks have been introduced.

With nearly 55 million mobile Internet subscribers across Japan, untargeted e-mails from a variety of porn peddlers, financial fraudsters and suspect scammers have become a pervasive problem for the Internet community. There are reportedly 950 million e-mails being sent each day over mobile networks and it is believed that around 85 per cent of them are spam.

Because consumers can be contacted everywhere they go and at any time of the day, the privacy invasion becomes much more intrusive. The problem is compounded by the fact that, unlike their European counterparts, Japanese mobile users pay to receive their messages. So, not only is spam a nuisance, but it is costing them money as well.

The two pieces of legislation were introduced at the beginning of July. They take the form of regulations from the Ministry of Public Management, Home Affairs, Post and Telecommunications (MPHPT), and a change to the Ministry of Economy, Trade and Industry's (METI) commerce law.

Unsolicited e-mailing has not actually been banned, but restrictions have been placed on companies which choose to follow such practices. What the laws require is for companies to clearly indicate when they are sending out unsolicited marketing messages. They are also obliged to reveal their identity (including name, address, contact number or e-mail address) and provide a means for consumers to opt-out from receiving further information. In addition, mass mailing via random telephone number generators will be banned.

> There are reportedly 950 million e-mails being sent each day over mobile networks... around 85 per cent of them are spam.

The MPHPT will also step up pressure on telecoms service providers to develop technological means of stopping untargeted messages from getting through to the public. Part of the problem is that the technological setup on some mobile networks makes it much easier for spammers to clutter up consumers inboxes with irrelevant and untargeted messages. They do not need e-mail addresses to send out mail because mobile subscribers' e-mail addresses are automatically matched to their telephone numbers. In order to target potentially hundreds of thousands of consumers, a spam merchant merely needs to harvest a list of random telephone numbers.

INDUSTRY EFFORTS

Leading operator NTT DoCoMo has already introduced anti-spam measures that allow its customers to block mail originating from specific Internet domains or addresses. And, in conjunction with the new laws, it has released a new anti-spam option that allows customers to block incoming messages that have been identified as being unsolicited.

The government will also back up its bark with bite, through the introduction of a range of penalties for non-compliance. MPHPT will be able to impose fines of up to 500,000 yen ($4,130) for a breach of its regulations. Those breaking METI's commerce law could face a three million yen ($24,836) fine or a two year prison sentence. For large corporations the stakes are somewhat higher, with fines of up to 300 million yen ($25,452).

DECEPTIVE PRACTICES

Unfortunately, Japan's cyber-scammers are extremely innovative and are still managing to stay one step ahead of efforts undertaken by the government and industry to keep them in check.

The latest scam to hit an unsuspecting public is "wan-giri" – the one-ring con. Duplicitous fraudsters make random calls to consumers' phones, hanging up after one ring. Curious recipients, keen to find out who has contacted them, call the number back and are connected up to recorded messages charging an extortionate rate.

This simple scam is causing havoc with telecoms networks and consternation among the public. Thousands of these untargeted calls can be made per minute and it is now becoming such a problem that DoCoMo has threatened to disconnect anyone who disrupts its network. Japan's telecoms regulations state that denial of service is illegal unless there are legitimate reasons. However, the MPHPT has recently endorsed DoCoMo's decision, deeming its disconnection policy to be perfectly legitimate.

The mobile service provider has also posted a warning to customers on its website. But, even scam-savvy customers who have wised up to the to the problem are still getting caught out as the virulent con trick mutates. Many of those who know to avoid 'one ring' calls still respond to fraudulent calls that ring two, three or maybe four times before hanging up. So far, the only realistic respite for harassed mobile users is to change their telephone number.

According to *Reuters* news agency, one person involved in the wan-giri scam has been arrested, although this was for an alternative pornography-related charge. However, the government is currently unable to prosecute these particular con artists.

i

Ministry of Public Management, Home Affairs, Post and Telecommunications (MPHPT): www.soumu.go.jp

Ministry of Economy, Trade and Industry's (METI): www.meti.go.jp

NTT DoCoMo: www.nttdocomo.com

Asia: Choking off access to the Internet

By Eugene Oscapella

Governments in three Asian countries have signalled their intentions to watch over the shoulders of Internet users and restrict access to websites. Serving as a window on the world, Internet cafes can also act as a vehicle for governments to monitor what their citizens are reading. Because computer ownership in many developing countries is limited, restricting access to websites through Internet cafes is a more effective monitoring and censorship device than it would be in the developed world.

Vietnam

The *Sydney Morning Herald* reported on August 6th that Vietnam has ordered tighter controls over Internet cafes to prevent "poisonous" materials being disseminated over the web. The Directorate General of Post and Telecommunications has asked authorities in all 61 provinces and cities to mete out severe punishment to those caught spreading dissent online.

The *Herald* reported that the department has also asked government ministries and agencies to compile a list of all banned Internet sites and services. Vietnam has only had access to the World Wide Web since 1997. Access to websites is blocked by firewalls. In addition, the newspaper reported that e-mail is regularly monitored.

Pakistan

In Pakistan, access to the Internet is also coming under fire. The *Nando Times* reported on August 5th that cybercafes will now be required to ask patrons for proof of identity and to keep records of users. Internet cafes also must start registering with the government. Until now, there was no such registration requirement.

Officials claim that keeping records at Internet cafes will help track down terrorists by making e-mails easier to trace. The *Times* quoted the chairman of the Pakistan Telecommunications Authority as saying: "If somebody cannot produce some form of identification, he can't use the Internet. It's in the interest of law and order, and stopping terrorism."

Still, the newspaper reported, regulators may have difficulty finding Internet cafes since many are small operations hidden away in towns and cities.

China

The Chinese government's efforts to monitor the Internet and restrict access also appear to be on the rise (see *PL&B Int*, Feb 2002, p.2). *Reuters* reported on August 6th that the Chinese government has sentenced a former policeman to jail for 11 years after he downloaded "anti-revolutionary" material from the Internet. According to the Hong Kong-based Information Centre for Human Rights & Democracy, he was the first person to be found guilty of subversion for downloading and printing material that Beijing officials deemed to be anti-revolutionary. [Incidentally, the domain name of the Centre's website is now listed as being for sale. This was one of the sites the convicted man was alleged to have visited.]

In July, according to online news service, *Yahoo.news* (Singapore), a group of 18 Chinese dissidents published a "declaration of Internet users' rights" in response to Chinese monitoring and censorship of the Internet. And in a measure that may help to suppress roving on the Internet, the Chinese government is reported to have forced over 3,000 Internet cafes to close permanently, and 11,000 to close temporarily. The stated purpose of the ban was to avoid a repeat of a recent fire in a Beijing cybercafe, in which 25 people died.