

Spam: are anti-spam laws working?

It's six years since the EU required all member states to put in place laws to combat spam. And it's six years this month since the UK's law came into effect. Is it working? And what about the USA's Can Spam Act?

You've seen the note at the end of spam-mail: to unsubscribe click here. And if you do? Well, now the spammer knows your address works.

The EU law is at best weak: it specifically provides a loophole which allows the sending of spam to corporate e-mail addresses, provided there is an opt-out.

This allows services like fagms.net to provide bulk mailing - but to provide an opt-out in relation only to one specific client. fagms.net is so protective of its own privacy that the front page of its website is a blank page: the code for that page is simply:

fagms.net is registered through Network Solutions, one of very few registrars who do not release names of owners via third party searches.

It turns out that the company that runs this is based in Duesseldorf, Germany. United Mail Solutions GmbH is therefore subject to the German interpretation of the EU directive, even when sending mail to UK victims.

We have e-mailed the registered administrative contact, Henrik Basten (basten@unitedmailsolutions.com) registered with Network Solutions but, as at the time of writing no reply had been received.

United Mail Solutions is not the only company using the tactic of requiring victims to unsubscribe from individual campaigns.

US company vocus.com has built its own mailing list. Where the list was generated from is

uncertain but one user tells us he suspects that his information was obtained from the private records kept by a newswire service where his personal e-mail address was registered for administrative purposes but all releases are sent to a centralised clearing address. Vocus.com's mails are sent to the personal e-mail address not to the clearing address. Vocom have not replied to an e-mail requesting details as to where the address was obtained from and requiring its removal from their systems.

United Mail Solutions appears to use mailing lists provided by its clients rather than its own list. Vocus, on the other hand, sends unsolicited mail for a wide variety of clients on a wide variety of subjects. It does not appear to retain data in client-related silos.

And yet, both companies comply with the base requirements that turn their unsolicited junk into permissible mail by including the specified information for their client, not for themselves.

By exploiting basic protections for agents, they seek to avoid the intent of laws to reduce spam.

UK law makes it an offence to spam individuals in their private e-mail accounts unless they have formally opted to receive mail.

Easy.Com sends out mail even if there are specific instructions in the customer registration form not to do so. It relies on its standardised terms of business - and the process to be removed from their spam-list is tortuous.

The incidence of unsolicited mail has, since the laws were passed, increased exponentially.

The stealing of data to build databases is rampant. It is not illegal to use bots to take e-mail addresses from websites: the common view being that anything on the web is in the public domain. That argument fails to recognise the difference between publicly available information and public domain.

An e-mail address created for one specific purpose and given to a government department, hand-written on a single form, has found its way onto spam lists. An e-mail address given to a government department in a different country, and which someone in that department mistyped

(so proving an audit trail) is heavily spammed containing the mistyping; an e-mail address that was used in a single, hard copy, letter to the CEOs of ten banks in a single country now receives spam from all over the world.

Amusingly, a company in Singapore sends its spam out from the domain bestguru.info. They do include an unsubscribe link for those that want to confirm that the e-mail address used is valid; they are promoting a conference where their main website b2bgroup.com.sg is promoting a conference called "Best Practice Digital Marketing Bootcamp." The message is marked as "FW" - a common spamming practice to trap the unwary into thinking that a mail is from someone who knows them; what it does not have is the designation "<ADV>" which Singapore law requires all marketing messages to have. Yup, these are clearly people who one would want to teach all about best practice.

There are ways of dealing with this problem.

First, domain names are art and should be afforded the same intellectual property rights as any other form of art. There should be a presumption that mass mailings i.e. more than, say, a dozen copies of a substantially similar mail in any seven day period, should be illegal unless the recipient has expressly requested such mail. The inclusion of a "we can spam you" provision in standard terms of service should be prevented, and so should tick boxes that auto complete to say it's OK to send marketing mail.

Unsolicited e-mail is not a low-to-no cost marketing medium. It, uniquely, transfers the entire cost of the marketing, after the initial production of the spam message, to the recipient.

That, in any other world, would be regarded as tantamount to theft.

And governments need to take steps to protect the resources of the recipient, not protect those who would abuse them.

And laws as currently drafted aid the spammers, not their victims.