

**SPAM - What happens next? Electronic Commerce Corner.
Opt-Out Is Not Final in the US. Spam will only get worse. And Spyware is Next.**

OECD. The Organization for Economic Co-operation and Development. This is not an organization one reads about every day in the newspaper. And yet it has an enormous impact on policy-making of governments around the world. In fact, what happens at the OECD in the next six to twelve months could well determine what happens to the Internet, and to e-mail marketing.

The OECD is essentially a research organization and "talking-shop" for policy-makers from the developed countries, basically Europe, the US, Japan, Korea, and a few others. Policies on every imaginable current economic and political issue are debated, research is commissioned, and government officials meet to discuss current problems and what can be done. Our State Department has a permanent representative stationed at the OECD in Paris and committee meetings bring representatives from Commerce, Treasury, the Federal Trade Commission, and other Federal agencies, depending on the subject.

It is enormously influential because the conclusions and guidelines and other pronouncements negotiated by its members represent a significant international consensus on important issues. For example, it is the place where the fundamental privacy principles now being implemented in US law were first negotiated and articulated on an international basis: notice of privacy policies, consent, opt-out, access to information, right to object, heightened security for record-keeping, use to which information can be put. Much of that thinking started in the US, of course, was articulated at the OECD, and then appeared in the EU's Data Protection Directive. Those ideas are now reappearing in things like FTC enforcement views on policies on website privacy, and Graham-Leach Bliley disclosure requirements.

Government officials from the entire developed world, and much of the developing world, often ask "What's the thinking at the OECD?" when confronted with a new policy issue, such as spam.

And if your CIO comes forward with new proposals on enhancing security of your IT network and creating a "culture of security" in-house, the thinking behind those proposals originated at an OECD committee on which the US Federal Trade Commission, and specifically Commissioner Orson Swindle, has taken a leadership role.

On Feb. 2 and 3, The Direct Marketing Association participated in a workshop at which the current state of the spam problem was examined and discussed by representatives of government, business, and consumers from the U.S., Europe, Canada, Korea, Japan, and other countries. The International Department has been part of an online dialogue on the issues of spam since October 2003 and this is the first of two workshops to be held on the subject.

We presented the DMA's views on the opt-out/opt-in debate, and our views on how government, consumers and business must work together to drive out the bad guys

and eliminate illegal traffic so business, suppliers and consumers can communicate without fear and without getting buried in spam. We also believe we need to get past the fruitless opt-in/opt-out discussion and solve the problem with technological tools, consumer education, and enforcement of existing law. We especially believe there must be increased international co-operation among investigation and enforcement authorities. Finally we need more unbiased research on the content of spam and the business model driving it.

We are both heartened and depressed by the workshop experience. We were heartened by the presentations of DMA members AOL and Brightmail, and from Messagelabs, a vendor to government of virus detection services and high security software. These highly sophisticated technical companies confirmed that our members are not the problem. Even with all the spam and viruses, the Internet is not about to crash or be overwhelmed. There are very bright, energetic people out there working to keep it running. Brightmail, for example, filters 15% of the Internet's e-mail. They observed that there is no agreed definition of "spam", but if it is unsolicited, butl, untargeted commercial offers, it looks like this:

90% have a call to action. Go buy something somewhere.

90% have a forged header.

75% are now in html or may only contain a url. Filters don't catch these yet.

10% "spoof" good brands.

Messagelabs and AOL confirmed we who honor opt-out are not the problem. However, it is sobering that there are a lot of very expert people out there who make as little as one-tenth of a cent per e-mail to broadcast stuff globally, filling our customers' inboxes to over-flowing, and it remains economic to the businesses who hire their services. According to AOL, "One sale, and they recover their costs." Many of them literally don't care about the law, if they know about it at all. And according to the FTC, many of them are kids in Dad's garage.

In short, the price of spamming has to rise. One way to raise the price is to enforce opt-out, or opt-in. Or to charge for sending e-mail, and no one wants that. Or provide for some sort of authentication of legitimate mailers, a solution most of the experts believed would be more effective than trying to charge for transmission. After all, these are guys who specialize in hoodwinking ISP's to send their stuff.

As for enforcement, law enforcement doesn't have the resources, except for big fraud cases. The problem is too dispersed and too common, and requires too much international co-operation. It will be up to the business community world-wide to enforce opt-out on its business partners, however they can do it, or every one will face opt-in laws, and possibly more aggressive enforcement. Agencies have to demand their clients do this. ISP's have to monitor their clients. E-mail service providers have to insist on their advertisers' doing this. Advertisers have to practice it. Otherwise even the DMA will have to give in to the drumbeat calling for opt-in.

This may be so even though opt-in won't work to empty the inboxes. This is so because there is too much of every other kind of spam e-mail, especially fraudulent and even criminal material, crowding the wires, and people with an ideological orientation, think it will solve the problem, the EC and consumer advocates. Unless we can figure out who spams, and why, and disrupt the business model some other way, the opt-in threat will haunt us, even though it won't work.

The complexity of the problem as presented by Brightmail and Messagelabs is disheartening. The percentage of "spam" in e-mail traffic has risen in some countries to 80%. Messagelabs estimates that spam is increasing in volume by 7% every two weeks.

And what's "spam"? There is no consensus, but it is much bigger than just "unsolicited offers". Most critically, it's loaded with pornography, viruses and fraud committed by people who are hard to find and who ignore the law. The newest and worst is "phishing" tricking people into going to a phony website that looks like a bank or ISP website. The sites look so authentic that good people are enticed into entering their social security numbers, credit card or bank account numbers and passwords or their computer passwords so financial information, and ultimately their money, can be stolen. And these people are hard to track down. David Jevans of Tumbleweed estimates it takes about 8 days to get a phony website based on a server in Eastern Europe shut down. There is simply no effective international crime control mechanism to do it faster.

On the disheartening side, the European Commission is fixated on one thing: consumer confidence in the Internet. Their presentation focused quite single-mindedly on how critical it was to make all countries have opt-in commercial e-mail marketing laws because "consumers are losing confidence in the Internet and this will prevent the growth of electronic commerce". Their presentation was based on the unscientific and thus "anecdotal" TransAtlantic Consumer Dialogue "study" referred to below. They did not acknowledge the two fundamental problems of the Internet: most "bad" commercial e-mail is either fraudulent (and clearly illegal) or just stupid. The latter problem can be solved by education of business, the former requires commitment of resources to law enforcement. Their presentation did not acknowledge the need to solve the difficult problem of enabling law enforcement authorities to work together legally, although Commissioner Liikanen's opening speech of welcome did so.

The Commission also blindly refuses to acknowledge a fundamental truth: e-commerce is growing nicely, very nicely indeed, spam or no-spam. U.S. consumers spent 23% more in November and December on purchases on the Internet than a year ago, USD 7.9 billion. E-commerce continues to grow in Europe, also. If e-commerce is growing slower in Europe it is for other reasons: size of multiple markets, maturity of development (especially in Scandinavia), lack of offerings, lack of credit card penetration, lack of household PC penetration, persistence of dial-up versus broadband, convenience of attractive retail experiences, even culture. (Spain, Greece and Italy have money, Internet service providers, commercial websites, etc., but e-commerce to consumers is quite under-developed. A real puzzle. Simply a factor of GDP per person? Culture? We'd love to hear theories.)

It must be acknowledged that Commissioner Liikanen's introduction, although fixated a bit on the "confidence" point, did recognize that enforcement and international co-operation were critical, and he underscored the need for continual development of technical solutions such as filters, closing open relays and filters.

The consumer advocacy groups were even less useful than the Commission, but one gets used to that. They had an opportunity to contribute plans for co-operation and even proactive involvement, but with a few exceptions and as usual, they did not fail to miss the chance to contribute positively.

They presented the results of a "study" conducted by the TransAtlantic Consumer Dialogue that "proved" consumers wanted opt-in and were "sick of" unsolicited commercial messages of every nature. They failed to highlight the fact that this "study" was really an on-line "opinion poll" survey conducted on a website that was designed to attract consumer advocates. It was a very carefully controlled respondent population, and thus unscientific. In any event, it told us what any good marketer knows already. Consumers hate messages that don't interest them. They get too many of them. Untargeted offers are unwelcome, and detrimental to your company's reputation. And given the choice between opt-in and opt-out as a solution to spam, consumers chose opt-in. Surprise.

The consumer organizations repeated their usual mantra we hear when any issue affects consumers. First, spam (or any other problem) is caused by business and they must fix it. Second, consumers must not be expected to take responsibility for themselves or go to any expense of time or money to learn anything. Third, whatever is decided, business must pay. Every other speaker, from the technical people, to government, and to associations underscored the obvious fact that consumers have to have tools they can use themselves, and they must understand how to protect themselves.

There were two exceptions to the dismal showing of the consumer advocates. The Swedish Consumer Protection Authority agreed with the US FTC (and the DMA) that the "problem spam" involves illegal and fraudulent offers and the problem won't be solved without international co-operation and more resources in law enforcement. There was a clear articulation of some of the problems of sovereignty that get in the way of that occurring.

The other enlightened exception was the National Consumers League of the US, which has often been a partner with the DMA in educational outreach to both business, on what is "the right thing to do" and to consumers on how to protect themselves. They proposed several excellent programs for the OECD to pursue that involve increasing public awareness through providing education toolkits, examples of good public education campaigns, and encouraging good business practices.

We were discouraged by the lack of clear data on the problem outside the technical experts, which means that law makers in Europe and the US have both acted without knowing the scope and nature of the problem. But that is par for the course.

We were heartened by some of the ideas that sprouted up in the closing session where the moderators presented their ideas for further work by the OECD and interested organizations:

- Agreement reached: this is an international technical, social, economic and political problem requiring coordinated responses by business and law enforcement globally.
- We have to learn who makes money with spam, and how. Follow the money.
- We have to figure out if opt-in or opt-out change the nature of unsolicited messages.
- We have to figure out what the categories of spam are, and whether they change with time.
- Law enforcement authorities have to learn "who to call" in other countries to conduct investigations, pass on complaints, and shut down "phishing" sites. (Shockingly, there is little formal interaction among enforcement authorities, and in some cases local laws and practices actually prevent them from sharing information and evidence they collect. Our own FTC is seeking legal authority to do this.)
- Consumers need to be educated on how to protect themselves.
- Technological tools must be perfected and distributed.

So there will be some action, and we hope progress in fighting spam. The DMA will continue to participate at discussions at the OECD and with our own government. U.S. DMA members need to assiduously comply with CAN-SPAM. We also urge members e-mailing abroad to learn which markets are "opt-in" and to observe the law in those markets.

And, finally, our own view of the "next big issue", confirmed by some of our technical friends": besides "phishing," it will be spyware, a close relative of pop-ups and pop-unders, a form of a "trojan virus." But you have lots of them on your PC. Go to sky-bot.com and download their program. You'll be shocked.