OECD WORKSHOP ON SPAM

2-3 February 2004 / Brussels, Belgium

Frameworks for Enforcement Co-operation in Related Areas

Giovanni Buttarelli, Data Protection Authority, Italy

TUESDAY, 3 FEBRUARY 2004

SESSION 6: INTERNATIONAL LAW ENFORCEMENT CO-OPERATION

FRAMEWORKS FOR ENFORCEMENT CO-OPERATION IN RELATED AREAS

Giovanni Buttarelli – Data Protection Authority, Italy

Several interesting ideas have already emerged from this Workshop.

Many proposals have been put forward, and we will attempt forging a synthesis this afternoon.

There is a red line connecting yesterday's and this morning's presentations – despite the many efforts made, the adoption of opt-in approaches in many countries, the harmonisation of rules in Europe, the enhanced role of codes of conduct, the implementation of technological solutions, in particular related to filtering, and the awareness-raising initiatives, spamming has not markedly decreased yet, indeed it is still on the rise in some countries.

A further consideration would appear to underlie several presentations, in my view. There is the need for a global approach worldwide, based on the interaction of many approaches and tools, rather than for solutions that are only based on suppression, self-regulation and/or educational initiatives.

Prior to making some general remarks, I would like to briefly refer to the recent experience in Italy – based on a very aggressive approach against spam, though ineffective in some specific cases.

In my country, we were among the first to follow the opt-in approach – ever since 1996 – to protect all kinds of recipient, whether natural or legal persons. In my country spamming is also a criminal offence, if it is carried out with a view to gain and/or with intent to cause harm to the recipient. These rules were supported twice by our national law-making body – in 1998 and in 2003.

I must confess that we do not have long-standing experience in daily co-operation on enforcement with other countries. There are several cases and excellent examples concerning the exchange of information and/or enforcement of our provisions, both within

Europe and in Australia, Canada and the USA (via the FTC), however they relate to sectors and issues other than spamming.

Our data protection authority has been working hard for the past 2-3 years. We have issued several provisions, also of a general nature, addressing the many issues related to consent and provision of information.

We have re-affirmed that it is prohibited to use software systematically harvesting all the data available on the Net (e.g. in forums and newsgroups), or else automatically generating e-mail addresses without checking the recipients and/or whether those addresses are active.

We have punished the commercial use of e-mail addresses that had been posted for specific purposes on the web sites of public administrative agencies and businesses.

We have dealt with disclosure of the lists of subscribers to service providers as well as with the lists of individuals registering domain names.

We have repeatedly supported the freedom of consent principle, whereby you cannot wring out consent from someone merely because you are providing him with some other service.

We have found that certain practices were unfair as they did not entail adequate, clear-cut information on the purposes for which third parties would be using the data, or else because the request for consent was used as an excuse for sending an initial advertising message – according to the opt-out pattern.

In 2002, we realised that we were not reaping a large crop and therefore we resolved to shift to a more repressive approach.

With the co-operation of a police force, we enforced twelve decisions simultaneously, i.e. on the same day, by blocking the unlawful activities carried out by some companies and preferring information on them to judicial authorities.

We put considerable emphasis on this initiative through the media, and the network people started exercising their rights of access, objection and cancellation on a massive scale directly with spammers – being also driven by the circumstance that they may not only claim damages before a court, but also be awarded by us, via an immediately enforceable provision, reimbursement of the costs related to the proceeding up to a total of 250 euro for each complaint lodged, increasing up to 500 euro in especially serious cases.

This led to many criminal investigations being started as well as to the lodging of many complaints with our Authority, which has to decide within 60 days; it should be noted that failure to comply with this decision gives rise to a separate offence.

Parliament empowered us by law to oblige providers to adopt filtering procedures as well as additional practicable measures with regard to spammers' e-mail co-ordinates.

The final results were encouraging both culturally and as regards the public opinion, however they placed a considerable burden on the operation of our organisation.

The investigations required to trace spammers are sometimes quite complex and energy-consuming; at other times they prove unsuccessful.

Spamming is not the most serious offence that may be committed by means of personal data, however it is already taking up at least 34% of our external audits as well as ¼ of the decisions concerning complaints lodged by citizens.

We were supposed to prefer information on thousands of individuals; therefore we were led to construe the criminal provision to the effect that spamming is only an offence if a systematic activity is carried out – rather than in the case of a single, unsolicited e-mail message.

However, we did not focus on suppression only. We also provided guidance on how to inform in a user-friendly manner and obtain consent fairly.

A special code of conduct is expected to be adopted shortly, which will have binding force and will be actually annexed to the original text of the Data Protection Act.

I realise that this framework is the outcome of a national approach. Indeed, spamming remains on the rise and law enforcement approaches are unable to cope with this problem by themselves – not even if one went as far as to apply the criminal law provisions in force in the place whence the e-mails originate.

Up to a few years ago, my e-mail address was also known abroad, though only to some friends and colleagues. Ever since I took part in a meeting on privacy in the USA and foolishly disclosed it to someone, I have been getting no less than 50 e-mails of all kinds – all of them from abroad – and the profile you could build up by reading those messages is all but flattering.

The safeguards laid down in Italian law are of little avail, as in principle they are not applicable to e-mail messages coming from abroad - in line with the establishment criterion followed in EC Directive 95/46.

I might refer to criminal law outside the scope of data protection legislation, for instance if there were attempted fraud and/or if my dignity or good repute were jeopardised. I might apply to the competent authority in the country where the spamming originated – and this solution was suggested to data subjects in one of our general decisions –, however this would take long and I cannot afford it.

Moreover, spam messages are often received during week-ends and it can be easily realised that many spammers are simply individuals carrying out their activities from their own houses without any specific organisation backing them and without falling necessarily under the scope of application of a data protection act – which, at least in Europe, usually excludes some processing operations of personal data for private and personal purposes. Therefore, responding to them to object to their spamming would result into confirming the validity of my address and making it all the more valuable for further messages.

There is an interesting case of co-operation among data protection authorities to quote here – and I am speaking out of personal experience.

As I was on the phone with some French colleagues, I got an unsolicited e-mail from France. I requested the sender in real time to stop e-mailing me and threatened that I would apply to the police, but I got an abusive message in the negative within a few seconds.

Then I asked my French colleague, again in real time, what I was supposed to do, and forwarded my e-mails to her. With commendable efficiency, the French authority traced the spammer, charged him with unauthorised trade practices, checked the source of the data, blocked the spamming activity, and sent two letters to me in a few days. I am really deeply thankful to Mr. Gentot, but then I wondered how we as data protection authorities could cope with these circumstances on a case-by-case basis.

Therefore, what short-period suggestions can we make?

My view is optimistic, however I am concerned by the increased economic costs of spamming as well as by the growing availability of paid anti-spamming e-mail services.

I agree with many of the proposals put forward here, and I am not going to dwell on them.

Let me make some final considerations in legal as well as technical terms.

From a legal standpoint, the traditional mechanisms followed by letters of request are not especially suited for these activities; indeed, I think that data protection can yield better results.

The European privacy directives, Strasbourg Convention no. 108/1981, and the Cybercrime Convention already envisage co-operation arrangements that have been implemented also via the Article 29 Working Party as well as through regular workshops on complaints handling, which are mentioned in the Communication by the European Commission.

I cannot see any obstacle to the exchange of information on cross-border complaints, the possible transfer of the complaint to the relevant authority (i.e. that of the country where the messages originate), and the harmonisation of practices adopted by all DPAs. As for this, it seems to me that there is no basic need for additional legislation.

This co-operation between DPAs can be anyhow enhanced at administrative level by setting up Intranets and/or exchanging data, and maybe a new legal framework for sectoral co-operation might be considered in order to further stimulate collaboration initiatives.

An example might be provided in this regard by Community Regulations 1/2003, which set out both horizontal – i.e. between competent authorities and judicial authorities in Member States as well as between Member States – and vertical networks – i.e. involving the Commission – with regard to competition law and envisaged additional bilateral and multilateral co-operation mechanisms with third countries.

Therefore, the difficulties to be coped with can perhaps be said to consist in the barriers to information exchange and co-operation with third countries.

Consideration should also be given to the legal feasibility of

- regarding the advertised entity as jointly liable whenever the e-mail sender cannot be identified,

- highlighting the liability of the providers of electronic communications services as well as the role played by regulatory authorities in this sector. In this way, serious, repeated non-compliance with data protection legislation, which is one of the basic regulatory requirements in the provision of such services, would lead either to issue of a warning or to suspension and/or withdrawal of the relevant licence pursuant to the provisions transposing Directives no. 19, 20 and 21 of 2002.

From a technical standpoint, the legislation concerning digital calling line identification raises the issue of whether a service allowing e-mails that are not included in a white list updated by the recipient to be rejected automatically and freely – without

charging the relevant costs to the recipient – could be set up also with regard to e-mail messages.

A non-negligible objection that can be raised with regard to these "whitelisting" services has to do with the fact that the "initial contact" between two users intending to communicate via e-mails would sometimes be required to occur via an out-of-band communication – i.e. by using tools other than electronic mail.

On the other hand, with a view to really effective measures applying to the Internet as well as to avoid impinging on the effectiveness of protocols and networks, it is advisable to await the initiatives currently being developed by technical fora such as the IETF (Internet Engineering Task Force) and the IAB (Internet Architecture Board), which can be expected to entail technical proposals to substantially modify the current e-mail protocols.

In this regard, it should be pointed out that the current SMTP (Simple Mail Transfer Protocol – RFC-821) protocol dates back to August 1982, when its first version was released.

Corrective measures based on the current protocol – though welcome as well as helpful in the current situation – would end up being palliation measures of a transient nature pending the re-definition of the relevant protocols, whilst the scope and impact of this re-definition exercise would not be smaller than those related to the introduction of the "new generation IP", i.e. the Ipv6 protocol. Therefore, let us leave this task to the technical experts.

Finally, I would like to refer to Mr. Mozelle Thompson's suggestion: he was right in suggesting the need to publicly clarify which judicial and administrative bodies – not only in the field of privacy and/or data protection – are competent and what they can do in terms of taking action.