OECD Digital Economy Papers No. 202

Review of the 2006 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Against SPAM

OECD

https://dx.doi.org/10.1787/5k95tn9rmhq6-en

OECD

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

30-Mar-2012

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Cancels & replaces the same document of 17 February 2012

REVIEW OF THE 2006 OECD RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS AGAINST SPAM

23/10/2011

JT03318939

DSTI/CP/ICCP(2011)1/FINAL
For Official Use

English - Or. English

FOREWORD

In 2006 the OECD Council adopted a recommendation setting forth a framework for cross-border co-operation in the enforcement of laws against spam. This report provides information on the progress in implementation measures, mainly based on a questionnaire of OECD member's experiences. This report was presented to the Committee for Information, Computer and Communications Policy (ICCP Committee) and the Committee on Consumer Policy (CCP) in October 2011. Both Committees agreed that the report would be updated taking into account all the comments received through December 2011 and then declassified under the written procedure. It was prepared by Maria-Chiara Baldaccini from the OECD Secretariat under the supervision of Dimitri Ypsilanti, Head of the OECD Information, Communication and Consumer Policy Division.

TABLE OF CONTENTS

REVIEW OF THE 2006 OECD RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS AGAINST SPAM

SUMMARY

Background

In 2004, a horizontal *ad hoc* "Joint ICCP-CCP Task Force on Spam" was established to develop an OECD anti-spam policy framework. In this context, an OECD *Anti-Spam Toolkit*[1] was developed (hereinafter "the Toolkit"), and it was declassified by both Committees in 2006. The Toolkit includes a package of recommended policies and measures that address regulatory approaches, enforcement co-operation, industry driven activities, technical solutions, education and awareness initiatives, spam measures, and international co-operation and exchange.

In this context, an OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam (hereinafter "the Spam Recommendation" or "the Recommendation") was also developed, and it was adopted by the OECD Council on 13 April 2006. It is contained in Annex I to this document.

The Recommendation, *inter alia*, recognises the importance of international co-operation in tackling spam issues more effectively and reflects a commitment by OECD members to develop frameworks for improved co-operation among their spam enforcement authorities. The importance of encouraging participation by private sector and non-member economies in anti-spam efforts is also highlighted. These include international enforcement co-operation efforts, efforts to reduce the incidence of inaccurate information about holders of domain names, and efforts to make the Internet more secure.

The final provision of the Recommendation instructs the ICCP and the CCP to monitor progress made in cross-border enforcement co-operation within three years after its adoption and hereinafter as appropriate.

In this regard, the process for conducting a review of the Spam Recommendation was discussed at the October 2009 meetings of, respectively, the London Action Plan (LAP) and the CCP, where it was agreed that the review would be carried out by the CCP, in co-operation with the LAP, including input from the ICCP.

In support of the review, and as a first step thereof, a written questionnaire (contained in Annex II to this document) was developed in co-operation with the LAP. It was then circulated among OECD and LAP members in April 2010, for the purpose of gathering information on progress made in the implementation of the Spam Recommendation so far. Respondents included Australia, Belgium, Canada, Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, Japan, Korea, Mexico, Norway, Poland, Portugal, Slovak Republic, Sweden, Switzerland, Turkey, United Kingdom and United States.

Building on members' responses and reflecting member country implementation efforts, the present document was prepared by the OECD in co-operation with the LAP, with the aim to serve as a basis for discussions at a joint OECD-LAP session, which was held during the CCP's 82nd Session, on 24 October 2011.

Main points

Since the adoption of the OECD Recommendation, the spam landscape has undergone significant changes both at the national and the international levels. In line with the Recommendation, OECD members have undertaken efforts to:

- Strengthen their domestic frameworks.
- Provide anti-spam enforcement authority to relevant bodies.
- Strengthen anti-spam and -malware efforts, including a range of policies and measures aimed at enhancing stakeholder education and awareness, international co-operation, industry partnerships and technological solutions.
- Enact anti-spam provisions that cover spam sent through various media, focusing on a number of specific media or adopting a technology neutral approach.
- Provide their spam enforcement authorities with the technical training needed to investigate spam cases, also taking advantage of the cyber-forensic expertise and experience of spam investigators in partner LAP nations.
- Provide redress for financial injuries caused by spam, either under general liability rules and/or consumer protection provisions or under anti-spam laws.
- Develop a number of mechanisms to handle cross-border requests and cases, including memoranda of understanding (MoU) and other written agreements, and co-operation within existing networks.
- Enable their spam enforcement authorities to provide investigative assistance to their foreign counterparts relating to violations of their laws connected with spam.
- Designate national contact points for co-operation.
- Enhance co-operation with relevant private sector entities and other stakeholders in pursuing violations of laws connected with spam, taking into account that spam is a complex issue and that it may involve a large number of parties.

Thus, information provided by OECD members provides a positive feedback indicating that progress has been made in enhancing cross-border co-operation in the enforcement of laws against spam, and there appears to be a strong willingness to co-operate.

However some challenges still exist. They include:

- Challenges related to the existence of a plurality of agencies that often share responsibility for addressing spam issues at a national level, in terms of communication, co-ordination and data sharing;

- Limitations encountered by some authorities on the extent to which they are able to co-operate with foreign jurisdictions, due to statutory limitations (*e.g.*, confidentiality requirements, limitations to information disclosure).

- Differences in the levels of technical capability of investigators in various jurisdictions at national and local levels.

- Limitation of resources (including financial, technical and know-how resources) for combating spam.

- Challenges in identifying and solidifying contacts in key jurisdictions where spammers operate.

- Technical challenges, including the inability to identify and locate spammers who manipulate the Internet infrastructure to evade detection.

- Data protection concerns that can make it difficult for the private sector to share information with enforcement agencies.

Areas that require continued and/or enhanced efforts by member governments and their anti-spam enforcement authorities would include additional efforts to:

- Improve communication and co-ordination among relevant spam enforcement authorities at the national level, for more homogenous enforcement approaches and enhanced co-operation with foreign agencies.

- Ensure that agencies are provided with the necessary powers and resources, including financial, technical and know how resources, to properly exercise their tasks.

- Enhance efforts to ensure redress for spam victims.

- Enhance efforts to further improve stakeholder education and awareness on spam.

- Ensure maintenance of a national contact point, as called for in the Recommendation, and keep relevant related information updated.

- Enhance sharing of intelligence information among jurisdictions.

- Strengthen anti-spam international co-operation, among OECD and non OECD economies.

Governments' renewed efforts in this respect are key to tackling such challenges for a more effective anti-spam law enforcement co-operation across borders. Progress is still needed to equip authorities with the tools and resources that are needed to effectively address cross-border spam infringements.

Continued anti-spam international co-operation among and within international bodies and networks, including the OECD, the Contact Network of Spam Enforcement Authorities (CNSA), the EU-wide network of public authorities responsible for enforcing consumer laws in the member states (the "CPC Network"), the LAP and the Messaging Anti-Abuse Working Group (MAAWG), in this area, will remain a key element going forward, as will continued co-operation with other private sector entities and relevant stakeholders.

REVIEW OF THE 2006 OECD RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS AGAINST SPAM

Introduction

The Recommendation calls for governments to take steps to develop frameworks for closer, faster and more efficient co-operation among their spam enforcement authorities that includes, where appropriate: *a)* establishing a domestic framework; *b)* improving the ability to co-operate, *c)* improving procedures for co-operation; and *d)* co-operating with relevant private sector entities.

Establishing a domestic framework

As highlighted in the Recommendation, while cross-border enforcement co-operation is key to tackling the global issue of spam more effectively, adopting a comprehensive national approach is also critical in this respect.

Since the adoption of the Spam Recommendation, efforts to strengthen their domestic frameworks have been undertaken by a number of OECD members.

Introducing and maintaining effective anti-spam laws

Consistent with the Recommendation, Canada's Anti-Spam Legislation[2] ("CASL") received Royal Assent on 15 December 2010 and will enter into force following a Governor in Council order. CASL is intended, *inter alia*, to deter the most damaging and deceptive forms of spam[3] and other electronic threats, such as identity theft, phishing, false or misleading electronic representations, spyware, malware and botnets affecting Canada. CASL is a standalone piece of legislation that includes amendments to the Competition Act, the Personal Information Protection and Electronic Documents Act (PIPEDA), the Canadian Radio-television and Telecommunication Commission Act and the Telecommunications Act. CASL will be enforced by the Canadian Radio-television and Telecommunications Commission, the Privacy Commissioner of Canada and the Commissioner of Competition. Among other things, CASL creates new civil provisions, prohibiting:

- Sending of unsolicited commercial electronic messages (spam).
- False or misleading electronic representations (including sender or subject matter information, and locator).
- Using computer systems to collect electronic addresses without consent.
- Unauthorised altering of transmission data.
- Installing computer programs without consent; and
- Accessing a computer system in contravention of an Act of Parliament to collect personal information without consent.

In addition amendments to the Competition Act create parallel new criminal provisions where conduct is engaged knowingly or recklessly. CASL also allows for international co-operation between Canadian enforcement agencies and their counterparts abroad, involving the sharing of information after an agreement or arrangement in writing has been concluded.

In the Asia-Pacific region, Japan amended its Act on Regulation of the Transmission of Specified Electronic Mail[4] (hereinafter "Specified Electronic Mail Act") and the Act on Specified Commercial Transactions[5] (hereinafter "Specified Commercial Transactions Act") in 2008, in order to enhance its anti-spam framework by introducing an opt-in system and by promoting international co-operation. Korea, moreover, has undertaken work to renew its domestic legislation and technical methods.

In Europe, a number of governments have undertaken or carried out efforts to amend their national legislation and ensure correspondence to relevant EU provisions in this field. In particular, it should be noted that Directive 2009/136/EC[6] has extended the scope of the Consumer Protection Co-operation Regulation[7] to also cover art. 13 of the Privacy Directive,[8] that deals explicitly with unsolicited communications. This allows national authorities to enhance and improve information exchange and co-operation with their foreign counterparts in other member states when taking action against rogue traders, including spammers.

Switzerland, moreover, introduced a new anti-spam paragraph in its Federal Act against Unfair Commercial Practices, in April 2007. The paragraph prohibits the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of unsolicited direct marketing, without the user's prior authorisation. Other efforts include amendments to the Swiss telecommunication law that now foresees further anti-spam measures, as well as work undertaken to further amend the Swiss Act against Unfair Commercial Practices. This is intended to facilitate Switzerland's anti-spam law enforcement co-operation across borders through information exchange, including data and/or documents. The amendments of the Swiss Act against Unfair Commercial Practices will enter into force on 1 April 2012.

In the United States, agencies use several laws to address the harm caused by spam through the use of various media, including the CAN-SPAM Act, 15 U.S.C. § 7701 et seq., the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 41 et seq., the Telephone Consumer Protection Act, 47 U.S.C. § 227, and relevant criminal statutes, including 18 U.S.C. § 1037 (Fraud and Related Activity in Connection with Electronic Mail) and 18 U.S.C. § 1343 (Wire Fraud). Although the primary spam law in the United States, the CAN-SPAM Act,[9] has not been amended since 2006, through rulemaking, the FTC has clarified some of the language in the CAN-SPAM Act, including:

- adding a definition of the term "person";
- modifying the term "sender" in those instances where a single e-mail message contains advertisements for the products, services, or websites of multiple entities;
- clarifying that a sender may comply with the CAN-SPAM Act by including in a commercial email message a post office box or private mailbox established pursuant to United States Postal Service regulations; and
- clarifying that to submit a valid opt-out request, a recipient cannot be required to pay a fee, provide information other than his or her e-mail address and opt-out preferences, or take any steps other than sending a reply e-mail message or visiting a single page on an Internet website.

In addition to enforcing the CAN-SPAM Act, the FTC can bring spam cases involving deceptive or unfair practices under the Federal Trade Commission Act ("FTC Act"). The FTC's ability to co-operate with foreign consumer and law enforcement agencies on cross-border spam cases was enhanced by the Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers beyond Borders Act of 2006[10] ("US SAFE WEB Act"), which amended the FTC Act. The US SAFE WEB Act allows the FTC to co-operate with foreign law enforcement agencies through the sharing of compelled or confidential information from its spam investigations, which, prior to the passage of the US SAFE WEB Act, could not be shared with foreign agencies. In addition, the FTC can now use all of its investigative powers, including issuing administrative subpoenas to Internet Service Providers (ISPs), domain registrars and other third parties, to obtain information on behalf of foreign agencies. The US SAFE WEB Act also provides other mechanisms for strengthening the FTC's relationships with foreign agencies, including authorising mutual staff exchanges for up to six months and giving the FTC authority to negotiate binding international agreements with other countries.[11]

In regard to spam sent via fax, the US Federal Communications Commission (FCC) adopted Rule 13 in April 2006 to implement the Junk Fax Prevention Act. This law amended the Telephone Consumer Protection Act, and permits the sending of unsolicited fax advertisements to individuals and businesses with which the sender has an established business relationship, and provides a process by which any sender must stop sending such advertisements upon the request of the recipient. Among other things, Rule 13[12] also requires the sender of fax advertisements to provide notice and contact information on the fax that allows recipients to opt out of future fax transmissions from the sender and requires senders to honour opt out requests within the shortest reasonable period of time, not to exceed 30 days.

In Mexico some anti-spam provisions are contained in the Federal Consumer Protection Law.[13] In this context, with the aim to prevent unsolicited telemarketing calls, the Consumer Protection Federal Agency of Mexico (Profeco) launched the Public Registry of Consumers, in November 2007. Moreover, under the regulation of the Federal Police Law of May 2010, powers to assist competent authorities with the investigation and analysis of electronic mails related to the investigation and prevention of cybercrime are given to the General Directorate for the Prevention of Cyber Crimes, as are other monitoring and investigative powers with the aim of foreseeing criminal behaviour. The General Directorate can also implement policies and procedures in this area.

In Turkey, an opt-out scheme for several types of messages including fax, e-mail and SMS was established in November 2008[14] and further work on secondary regulation, focusing on text messages, has also been undertaken by the Information and Communication Technologies Authority. According to Turkish authorities, some amendments to the Turkish Penal Code would be beneficial to address spam cases more effectively.

Portugal and the United States have recently become party to the 2004 Council of Europe Convention on Cybercrime,[15] and Switzerland is considering its ratification.

As to the types of anti-spam sanctions enacted in the OECD area, it is noted that, while in some countries (including Australia, Belgium, the Czech Republic, Denmark, Norway and the Slovak Republic), violations of laws connected with spam are sanctioned through civil penalties or administrative provisions, in others criminal laws specifically designed to combat spam have been enacted.

For example, in Canada, amendments to the Competition Act include both civil and criminal provisions addressing false or misleading electronic representations. In Switzerland, criminal law contains different paragraphs prohibiting cybercrime and the Law on Unfair Competition[16] also includes a specific anti-spam paragraph, whose violation can be sanctioned with up to three years imprisonment. In the United

States, the CAN-SPAM Act also includes criminal penalties for certain spam-related activities, such as the use of falsified e-mail header information, the use of false information to register e-mail accounts or domain names utilized in connection with spamming, and the unauthorised use of a third-party's computer to transmit spam.

In other countries, including Germany and Mexico, under certain circumstances, spam may constitute a criminal offence under general criminal laws. These include computer-related forgery, computer-related fraud, and distribution of pornography, *inter alia*.

Enhancing anti-spam law enforcement

The Recommendation emphasises the need for OECD Members to take appropriate steps to provide their spam enforcement authorities with the necessary authority to investigate and take action, in a timely manner, against violations of laws connected with spam. Such violations include those that are committed from their territory or cause effects in their territory.

Consistent with the Recommendation, a number of Member countries, including Australia, Canada, Germany, Greece, Hungary, Korea and Japan, have provided anti-spam enforcement authority to relevant bodies.

The Australian Communications and Media Authority (ACMA) is responsible for the compliance and enforcement of the Spam Act. The Spam Act[17] applies to commercial electronic messages with an Australian link. An Australian link applies if:

- The message originates in Australia; or
- The individual or organisation who sent the message, or authorised the sending of the message, is:
  - An individual who is physically present in Australia when the message is sent; or
  - An organisation whose central management and control is in Australia when the message is sent; or
  - The computer, server or device that is used to access the message is located in Australia; or
  - The relevant electronic account-holder (message recipient) is an individual who is physically present in Australia when the message is accessed.

The ACMA is provided information-gathering powers under the Telecommunications Act 1997 to compel information from telecommunication carriers, service providers, and other persons, such as businesses or individuals. The ACMA can also apply to a magistrate for a search warrant where contraventions of the Spam Act are suspected.

In the United States, civil enforcement agencies can use all of their existing investigative powers, including the issuance of administrative subpoenas, to obtain evidence sufficient to investigate and take action against senders of spam. In the criminal realm, enforcement agencies can use subpoenas, search warrants, wire taps, and other techniques to investigate criminal wire fraud and CAN SPAM violations. In the United Kingdom, the Office of Fair Trading (OFT) has the power to obtain evidence under various pieces of legislation that it enforces. For example, the OFT can request information and has power of entry and investigation under the Enterprise Act[18] and the Consumer Protection from Unfair Trading Regulations

2008 (CPRs),[19] respectively.[20] It should be noted, however, that, although applicable, these powers come under general consumer protection legislation and are not specific to spam. This authority, moreover, could apply to spammers operating in the United Kingdom but targeting consumers in other EC member states only and it would not apply to non EC consumers.

In Germany, private action and the support thereto provided by consumer protection agencies are prioritised. In three specific cases, however, public authorities can take action against spammers:

- District Governments (police) have the authority to obtain evidence to investigate and take action against spammers within the limits of section 6 para.2 of the Telemedia Act.[21]

- The Federal Network Agency is responsible for combating practices where spam is used to abusively advertise telephone numbers (see section 67 of the Telecommunications Act)[22]. This also includes cases where spammers operate in Germany and abusively advertise German telephone numbers abroad. In cases where foreign numbers are used by spammers, the Agency informs the ITU (International Telecommunication Union).

- In case of a suspected criminal offence committed via spam, law enforcement authorities have the general authority to investigate the suspected person.

In all of these cases, German public authorities have the authority to obtain sufficient evidence to investigate and take action against spammers.

In Switzerland, the State Secretariat for Economic Affairs (SECO) can obtain specific information about spammers from ISPs and initiate civil or criminal proceedings against spammers. It does not, however, have the ability to investigate, and investigations are carried out by the examining magistrate, once a criminal action has been filed.

In Sweden, spam enforcement authorities have the authority to handle spam cases falling under the Marketing Act, as do authorities in Portugal, when spammers misuse personal data. In both countries, spam cases involving cybercrime are dealt with by law enforcement agencies (police).

In Portugal, officials note that, under Decree-Law 7/2004 transposing Directive 2000/31/EC on electronic commerce, the ICP-National Communications Authority (ICP-ANACOM)'s authority does not seem to be totally clear with respect to the competences that each sectoral authority has in relation to e-commerce, including unsolicited communications.

Similarly, in Norway the Consumer Ombudsman's (CO) authority to request information from ISPs and phone companies about spammers' identity is under discussion. According to the Norwegians, such authority needs to be clarified for the CO to be able to investigate and take action against spammers with concealed identity.

In other countries, a number of challenges appear to remain in the enforcement area. For example, according to the Czech authorities, under the Electronic Communications Act,[23] the Czech Office for Personal Data Protection (OPDP) does not seem to have the authority to request the necessary traffic and location data to obtain spam evidence. Further issues remain with respect to spam sent from outside Europe. In Turkey, while some anti-spam provisions are contained in the Electronic Communications Law, authorities indicate that obtaining sufficient evidence for spam investigation represents a challenge, due to the lack of specific legal arrangements in this field.

In other OECD countries spam enforcement authorities are deemed to have sufficient authority to investigate and take action against spammers, as far as mere unsolicited communications from identifiable spammers are concerned. Such is the case, for example, in Belgium. Significant challenges, however, seem to still exist with respect to spam cases involving cross-border computer-related fraud and other forms of cybercrime, as well as spammers with concealed identity.

In Poland, authorities are deemed to have adequate powers to investigate all violations of law, collect evidence, and take necessary action to identify and treat offenders. However, statistics indicate that such measures are not often taken. In this regard, according to the Polish Ministry of Infrastructure, a possible explanation could be that, under the Act on Providing Services by Electronic Means,[24] prosecution of spammers can only be victim-initiated and that spam victims may not be sufficiently aware of the remedies available to them.

Effectively addressing spam evolution

Spam has evolved from a nuisance to a vehicle for committing fraud and distributing malicious software (malware).[25]

According to the responses received, a number of countries indicate that an increase in spam is occurring. However, in some countries, data specifically regarding evolution of malware[26] delivered *via* spam do not appear to be easily available. This seems to be due to challenges related to the plurality of agencies that often share responsibility for spam matters, to lack of resources and to the diversity of the possible activities involving malware. In this respect, data and trends seem to differ in different countries: while for some OECD Members there seems to have been an increase of malware delivered *via* spam (*e.g.* Sweden), for others (*e.g.* Norway), based on feedback from ISPs, no indication exists in this regard, while in Greece no cases of spam involving malware have been reported to relevant authorities so far.

In a number of OECD countries, strengthened anti-spam and -malware efforts have been undertaken and include a range of policies and measures aimed at enhancing stakeholder education and awareness, international co-operation, industry partnerships and technological solutions.

The Australian Government endorses a five step approach[27] to fighting spam in Australia. This covers the enforcement of the Spam Act, education and awareness activities, international co-operation, industry partnerships and technological solutions to spam. This approach has not changed since the passing of the Spam Act, in 2003. However the approaches made to the five steps have been revised and developed significantly since that time. For example, the ACMA has developed the Australian Internet Security Initiative (AISI)[28] to help address the problem of "zombie" computers. These computers become compromised through the secret installation of malicious software, such as a "trojan", that enables the computer to be controlled remotely for illegal and harmful activities. The AISI collects data on computers that are operating as zombies, analyses this data, and provides daily reports to participating Australian ISPs on the zombie computers operating on their networks. The ISPs then inform their customers that their computer is compromised and provide advice on how they can fix it. The ACMA makes regular referrals to Australian law enforcement authorities in relation to botnet activities, which in Australia are a criminal activity.

For example, some OECD members (including Australia, Sweden and Switzerland) have taken steps on the education, awareness and empowerment front, helping users to protect themselves from malware and spam. Others (*e.g.* Mexico) have focused on efforts to strengthen the skills of their law enforcement authorities, taking into account that the spammers' *modus operandi* evolves in step with advancing technology and that being informed about changes is critical for enforcement officials. Mexico recently established a Scientific Division and created a Co-ordination for the Prevention of Cybercrimes of the

Federal Police, in order to improve its institutional anti-spam framework on the preventative and investigative fronts. A new Department for Cybernetic Security, whose tasks include the preparation of a national strategy for cybernetic security, was also recently established in the Czech Republic, as was a government CSIRT (Computer Security Incident Response Team), which is also dealing with spam issues.

In the United States, law enforcement agencies have adopted a number of approaches to attacking botnets,[29] whose frequent use, according to officials, represents the most significant change in the spam landscape. These approaches include prosecution of those responsible for developing and maintaining botnets, as well as actions targeting the infrastructure used to propagate them. In Turkey, the Information and Communication Technologies Authority has undertaken a pilot project related to malware prevention that includes malware delivered via spam and aims at tackling botnets. Further efforts include spam prevention and monitoring, user assistance, and raising user awareness about malware and identity theft.[30]

In Greece, although so far no cases involving malware distributed *via* spam have been reported to the Hellenic Data Protection Authority (HDPA), the significant increase in the number of spam-related complaints in recent years induced the HDPA to establish an internal Spam Case Handling Policy and to undertake work to draft two new directives in the area of unsolicited electronic communications. These focus on political communication with emphasis to electronic marketing and on obtaining user's consent through electronic means (in the context of Law 3471/2006, on data protection), respectively.

In the United Kingdom, the OFT is engaged in various fora and working groups aimed at reducing the spam problem. In particular, the OFT was instrumental in the establishment of LAP in 2004, participated in the Joint ICCP-CCP Task Force on Spam[31] with the UK Department for Business, Innovation & Skills' (BIS) representatives (then the Department of Trade and Industry) in the Joint ICCP-CCP Task Force on Spam[32] and held the co-ordinator role on the CNSA for a short period. Other agencies, however, are involved in enforcement and are currently taking principal responsibility in this regard. For instance, the Information Commissioner's Office (ICO), which plays a more junior role within LAP, has recently been tackling spam by SMS/text message which comes under the Privacy and Electronic Communications (EC Directive) Regulations 2003 and is arguably a bigger nuisance to consumers in the United Kingdom.

Addressing spam sent through various media

As regards spam enforcement authorities' investigative powers, a number of governments, including, Belgium, Denmark, Greece, Mexico, Hungary, Italy, Norway, Portugal, Sweden and Turkey have enacted anti-spam provisions that cover spam sent through various media. While such provisions tend to focus on a number of specific media, in some countries the approach appears to be technology neutral.

In Germany, private action against spam can be taken irrespective of the media used. As regards action taken by public authorities, it has to be distinguished between the three specific cases mentioned above, where public authorities investigate spam cases:

- Section 6 paragraph 2 of the Telemedia Act relates to e-mail spam only. Investigations by public authorities (*e.g.* police) are restricted to e-mail-spam accordingly.

- The Federal Network Agency can investigate spam sent through any media, as long as such spam is used to abusively advertise telephone numbers.

In case of investigations of criminal offences, there are no limitations with respect to the media used.

The Australian Spam Act covers commercial electronic messages sent by e-mail, SMS, MMS and instant messaging and the ACMA's approach to investigations of spam centres around these four delivery

methods. It should be noted that recent changes to the Australian legislation around telemarketing (Do Not Call Register Act 2006) have allowed fax numbers to be registered on the Do Not Call Register. Faxes sent to numbers registered on the Do Not Call Register may also be investigated by the ACMA. Similar registers and lists have also been introduced in other OECD members, including the United States. In Japan, the Specified Electronic Mail Act presently covers SMTP and SMS. In other countries, including Poland and Portugal, provisions cover unsolicited commercial information sent through electronic communications and the use of automated calling systems (*e.g.* SMS, fax and voice using automated calling systems) for direct marketing purposes, without the recipient's consent.

In Italy, the Competition Authority, responsible, among other things, for the enforcement of the provisions on unfair commercial practices,[33] has carried out a number of investigations concerning spam sent through e-mail or SMS. In this context, monetary sanctions were imposed on the content providers from which spam had originated, as were on the telecom operators who had retained an economic advantage from such spamming activities.[34]

The United States has domestic legislation that authorises relevant authorities to investigate spam sent through various media, including e-mail, mobile messages, and fax. The CAN-SPAM Act addresses both unsolicited commercial e-mail messages and unwanted "mobile service commercial messages."[35] Notably, the FCC issued a rule under the CAN-SPAM Act banning all unsolicited commercial e-mail messages sent directly to wireless devices without the user's express prior authorisation. To enforce this rule, the FCC created a wireless domain name list, requiring all wireless service providers to provide all Internet domain names used to transmit e-mail messages to wireless devices for inclusion on the list. Non-exempt senders of commercial e-mail messages are prohibited from sending the messages to any domain name on the list.

In addition, the Telephone Consumer Protection Act prohibits non-emergency autodialed and pre-recorded calls to numbers assigned to emergency telephone lines, health care facilities, wireless phones, and any other service for which the called party is charged without the called party's prior express consent. The courts and the FCC have interpreted this provision to prohibit text messages, such as phone-to-phone SMS, without the called party's prior express consent. The Telephone Consumer Protection Act also prohibits the sending of unsolicited advertisements to fax machines. Other United States agencies are also involved. The FTC, for example, exercises authority over harm caused through the use of these media.

On the technology neutral front, in the United Kingdom, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECRs) regulate the sending of spam[36] and covers communications defined as "any information exchanged or conveyed between a finite number of parties by means of a public electronic communications service". The PECRs are regulated by the Information Commissioner's Office (ICO). They have recently been modified to allow the ICO to serve a civil monetary penalty of up to GBP 500 000 for serious contraventions likely to cause significant damage or distress. The ICO also now has increased powers of investigation into likely breaches of the Regulations. Similarly, the Swiss Anti-Spam provisions cover every unsolicited message that has been sent by technical means. Canada's Bill C-28, which contains a special exclusion for voice communications, can also be mentioned in this context as technology neutral, as a regime governing deceptive telemarketing is already in place in Canada under the Competition Act. In the Czech Republic, although legislation covers spam sent through a range of different media, action is only taken against unsolicited commercial communications sent by e-mail, SMS, fax.

Training

A number of OECD governments provide their spam enforcement authorities with the technical training needed to investigate spam cases, also taking advantage of the cyber-forensic expertise and experience of spam investigators in partner LAP nations. These include Australia, Belgium, Canada, Germany, Hungary, Korea, Japan, Mexico, Poland, Sweden, Switzerland, Sweden, the United Kingdom

and the United States. In Turkey, where authorities do not deem to have sufficient technical training to investigate spam cases, the Computer Emergency Response Team (TR-CERT) provides technical training on information security matters, including spam for public officials. In addition, the Information and Communication Technologies Authority co-operates with ISPs, 3G providers and state research institutes.

However, in light of the responses received, room for improvement is still deemed to exist in this area in a number of OECD countries. The ability to address challenges is due, in some cases, to limited technical, financial and or know-how resources.

Another issue, highlighted and being addressed by the UK's OFT, is the varying degrees of capability and resources available for tackling online threats at a local level. In this context, according to the OFT, a minimum level of expertise and capacity for investigating Internet related threats needs to be achieved at a regional level across the country, with higher level expertise accessible at a national level. Further, it is highlighted, it could be beneficial to achieve this minimum level principle at European level as well, where similar challenges may also exist.

These efforts notwithstanding, it should be noted that authorities continue to encounter a number of technical challenges, including the inability to identify and locate rogue spammers, as the spammers often develop effective techniques to evade detection.

Ensuring redress for spam recipients

The Recommendation further calls for governments to consider ways to improve redress for financial injuries caused by spam. Such redress can be provided to spam recipients in a number of Member countries, either under general liability rules and/or consumer protection provisions (*e.g.*, in Belgium, Czech Republic, Denmark, Germany, Japan, and in the United Kingdom), or under anti-spam laws.

In Greece, for example, redress can be provided to consumers for financial injury caused by spam under Article 14 of Law 3471/2006.[37] The minimum redress for such injury amounts to EUR 10 000, unless otherwise claimed by the plaintiff. In Canada, CASL provides for a private right of action for consumers and businesses to seek damages.[38] In addition, the amendments[39] to the Competition Act provide for the possibility of restitution for the new civil false or misleading representations provision under that Act. In Australia, the Spam Act provides for ancillary orders where loss or damage has been suffered by an individual. However, no such claims have been made in relation to these provisions. No claims have been made in some countries (including Hungary, Norway and Sweden), in spite of availability of provisions and instruments. In the United States although the CAN-SPAM Act authorises civil and criminal penalties, it does not include provisions pertaining to redress for consumers. However, because a number of spam cases also involve fraud, spammers often face prosecution under both the CAN-SPAM Act and the FTC Act. The FTC Act authorises courts to award equitable remedies to consumers, including financial redress.

The possibility for providing redress to foreign consumers is foreseen in a number of countries, including Canada, Germany, Greece, Hungary, Norway, Portugal, and Switzerland. Moreover, the US SAFE WEB Act confirmed the availability of monetary restitution as a remedy for both domestic and foreign victims of FTC Act violations.

Improving anti-spam international co-operation

The Recommendation calls for governments to improve the ability of spam enforcement authorities to co-operate with their counterparts abroad, including implementing procedures for co-operation. In particular, it is recommended that spam enforcement authorities be: *(i)* provided with mechanisms to share relevant information with foreign authorities relating to violations of their laws connected with spam upon

request, in appropriate cases and subject to appropriate safeguards and *(ii)* enabled to provide investigative assistance to foreign authorities relating to violations of their laws connected with spam upon request, in appropriate cases and subject to appropriate safeguards. Under the Recommendation, OECD countries are also called for to designate a contact point for co-operation and to provide the OECD Secretariat with updated information regarding their laws connected with spam and their spam enforcement authorities. The OECD secretariat is called upon to record this information and make it available to interested parties.

Strengthening mechanisms for cross-border co-operation

Consistent with the Recommendation, OECD countries have developed a number of mechanisms to handle cross-border requests and cases, including memoranda of understanding (MoU) and other written agreements, and co-operation within existing networks.

For example, in Australia, a number of MoU have been established by the ACMA with New Zealand, Thailand, Chinese Taipei, Korea, China, Malaysia, Hong Kong, China, Philippines, Japan, the United States and the United Kingdom. In addition, the ACMA participates in the LAP. In Canada, cross-border information sharing efforts may be undertaken pursuant to written agreements or arrangements concluded by the Government of Canada or Canadian enforcement bodies and foreign counterparts.[40] The United States continues to pursue a multi-faceted approach to improve cross-border co-operation, including encouraging enforcement authorities in other jurisdictions to participate in informal networks and accede to the 2004 Council of Europe Convention on Cybercrime, developing more effective frameworks for co-operation with the private sector, facilitating training for enforcement agencies and advocating the implementation of technological tools that would make the Internet more secure.

Co-operation within networks such as the CPC Network, the European Contact Network of Spam Enforcement Authorities (CNSA), the International Consumer Protection and Enforcement Network (ICPEN), the LAP and the MAAWG, also plays a critical role, which is widely recognised in the OECD area. Such networks have helped provide contacts that may be used for informal referral of spam cases.

Such mechanisms do not seem, however, to be fully used. Some members of the networks mentioned above (including Sweden, for example), as yet, have not received any requests from other countries. In Japan, the mechanism contained in the Specified Electronic Mail Act, as amended in 2008, has not been used so far. It specifically allows[41] the Minister for Internal Affairs and Communications to provide any foreign enforcement authority with information that is deemed to contribute to the execution of their duties. Korea, as yet, has not handled any cross-border requests or cases. In Turkey where no legislative provision currently exists in this regard, it is expected that some mechanisms to handle cross-border requests will be established in the future.

Further challenges, it is noted, include limitations encountered by some authorities on the extent to which they are able to co-operate with foreign jurisdictions, due to statutory limitations (*e.g.* confidentiality requirements, limitations to information disclosure).

In civil spam matters, the United States follows internal agency procedures for handling the sharing of information with foreign agencies.[42] The procedures track the requirements of the US SAFE WEB Act, which generally authorises assistance when a foreign agency is investigating possible violations of foreign laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by laws the FTC administers. To facilitate the handling of requests, the FTC uses a request form that asks foreign agencies to provide, *inter alia*, the following information:

- a description of the agency, including the source of its authority to investigate or enforce the relevant law and the basis for its ability to keep the requested material confidential;

- a description of the conduct at issue, including the potential law violation, the type of enforcement proceeding, and the number of people harmed by the target's practices;

- a description of the specific information it would like the FTC to provide and how it intends to use those materials; and a description of any assistance the foreign agency has previously provided to the FTC, if applicable, and whether the foreign agency intends to use its best efforts to assist the FTC in the future.

For international criminal investigations, the US Department of Justice's Office of International Affairs handles incoming and outgoing requests for assistance.

Law enforcement authorities, moreover, mutually co-operate with each other in a number of countries. In this context, cross-border requests or cases can be handled under the framework of the International Criminal Police Organization (ICPO).

Providing appropriate investigative assistance to foreign counterparts

As mentioned above, the Recommendation highlights the importance for spam enforcement authorities to provide investigative assistance to their foreign counterparts relating to violations of their laws connected with spam upon request, in appropriate cases and subject to appropriate safeguards, in particular with regard to: *i)* obtaining information from persons; *ii)* obtaining documents or records; or *iii)* locating or identifying persons or things.

Consistent with the Recommendation, a number of members have enabled their spam enforcement authorities to do so.

In Europe, in case of an intra-community infringement of a national provision transposing art.13 of Directive 2002/58/EC, co-operation between the national competent enforcement authorities for consumer protection legislation is foreseen by the CPC Regulation, as amended by Directive 2009/136/EC.

In the United Kingdom, the OFT has the ability to provide investigative assistance to European Commission member countries under the European CPC legislation, through information and intelligence sharing. Part nine of the Enterprise Act 2002 also allows the OFT to provide information to an overseas public authority, but there are restrictions placed on the kind of information and when it may be disclosed. MoUs have also been established with several other overseas counterparts such as the US FTC and the Australian Competition and Consumer Commission (ACCC), whereby assistance is provided wherever practical and possible. The OFT, however, does not have the ability to specifically refer or receive spam cases other than set out above, within the confines of the consumer protection regime.

In Switzerland, under the Federal Act on International Mutual Assistance in Criminal Matters, law enforcement authorities have the ability to provide investigative assistance to other countries, which is especially useful in spam cases involving cybercrime. Otherwise, in spam cases not involving cybercrime, SECO co-operates informally with other spam enforcement authorities within the CNSA, LAP and ICPEN networks. In Japan, law enforcement authorities have the ability to provide assistance to co-operate with their foreign counterparts in spam cases (see Section on: *Ensuring redress for spam recipients*).

In Canada, CASL provides for co-ordination and consultation between and among the three enforcement agencies responsible for compliance, as well as for information sharing with, and providing investigative assistance to, international counterparts. It also provides for a broadly-defined Canadian jurisdictional link, which stipulates that CASL applies to electronic messages sent to, through or from

Canada. Disclosure of information from private sector organisations to the Canadian enforcement agencies is also provided by the legislation.

In the United States, the US SAFE WEB Act authorises the FTC to provide investigative assistance to foreign agencies. The principal type of investigative assistance the FTC may provide is the issuance of an administrative subpoena to compel documents or other evidence. The FTC has obtained information from several companies, including domain name registrars, email service providers, and telephone service providers, using this mechanism. In so doing, the FTC has provided subscriber information to foreign agencies that has helped them to confirm the identity of suspects operating foreign scams, as well as identify additional victims of those scams. The FTC has provided investigative assistance and or shared non-public information pursuant to the US SAFE WEB Act with several London Action Plan members, including the Australian Communications and Media Authority, the Canadian Radio-television and Telecommunications Commission, the Canadian Office of the Privacy Commissioner, the Dutch Independent Post and Telecommunications Authority, the New Zealand Department of Internal Affairs, and the UK Office of Fair Trading on a wide range of issues, including, in some cases, spam investigations. The US SAFE WEB Act also authorises the FTC to seek appointment[43] to conduct civil discovery on behalf of civil authorities or on behalf of criminal authorities when the request is referred by the US Attorney General. Further, the US Department of Justice, Office of International Affairs, serves as the focal point for international co-operation in criminal cases, including spam-related investigations, and handles thousands of requests a year for electronic evidence.

The United States has mutual legal assistance treaties with more than 75 countries, allowing co-operation on a wide range of criminal activity, including spam and other fraud. It also engages in mutual legal assistance *via* letters rogatory with countries for which there is no mutual legal assistance treaty. In addition, the 2004 Council of Europe Convention on Cybercrime can provide an independent legal basis for mutual legal assistance in international investigations that involve electronic evidence or substantive cybercrimes. The US Department of Justice and the Federal Bureau of Investigation also provide international co-operation in cybercrime investigations, and related training and capacity building, through prosecutors and special agents based in the United States and at US embassies abroad. In regard to the referral question, US agencies may refer cases and receive referrals from other foreign agencies.

Investigative co-operation of spam enforcement authorities with their foreign counterparts remains a challenge in some OECD member countries, due, in some instances, to a lack of resources.

Establishing national contact points

The Recommendation calls on member governments to designate national contact points for co-operation and to provide the OECD secretariat with updated information regarding their laws concerning spam and the spam enforcement authority designated as their contact point. Although a number of OECD members, including Australia, Canada, Czech Republic, Denmark, Germany, Greece, Korea, Japan, Norway, Portugal, Sweden, Switzerland and the United States, have identified such contact points and provided the OECD secretariat with relevant contact details, other countries have not.

Although there seems to be general support for the national contact points designated under the OECD Recommendation, one questionnaire respondent indicated that the primary method for identifying a contact is either through bilateral enforcement relationships or multilateral enforcement networks, such as the LAP.

Room for improvement in this area appears to exist. Improvements in this respect could be achieved, for example, by keeping the contact information list updated and by increasingly raising awareness of its

existence and availability among Member countries, as well as among and within existing enforcement networks**.**

In this respect, it should be noted, that, although the Recommendation calls on the OECD secretariat to keep record of the national contact points and make relevant information available to interested parties, as yet, dedicated resources have been unavailable to maintain web-sites or to ensure that updated contact point information is accessible. It should be also noted that the OECD has put forward proposals in the past to set up co-operative mechanisms for enforcement agencies (covering co-operation in the range of issues in the information and communication technology areas) but has not been successful in doing so.

Co-operating with business and other relevant stakeholders

The Recommendation calls on governments to co-operate with relevant private sector entities and other stakeholders in pursuing violations of laws connected with spam, taking into account that spam is a complex issue and that it may involve a large number of parties.[44] In particular, the Recommendation notes that spam enforcement authorities should co-operate with these groups on user education, promote their referral of relevant complaint data and encourage them to share with spam enforcement authorities investigation tools and techniques, analysis, data and trend information. Further, the Recommendation calls for countries to encourage co-operation between spam enforcement authorities and the private sector to facilitate the location and identification of spammers. Countries are also called on to encourage participation by private sector and non-member economies in international enforcement co-operation efforts, efforts to reduce the incidence of inaccurate information about holders of domain names and efforts to make the Internet more secure. Where appropriate, spam enforcement authorities and the private sector should continue to explore new ways to reduce spam.

Consistent with the Recommendation, many OECD members have taken steps to enhance co-operation in this respect. Initiatives include design and implementation of targeted business and consumer awareness and education campaigns (*e.g.* in Australia, Belgium,[45] Canada, Czech Republic, Greece and Portugal), including prevention talks on cybercrime at all levels of education (*e.g.* in Mexico), participation in industry events and consultation with relevant private sector entities (*e.g.* in Australia, Czech Republic, Denmark, Hungary, Poland), general co-operation (*e.g.* for information requests, in Korea and Switzerland), organisation of multi-stakeholder events, such as workshops and roundtables (*e.g.* in Portugal and Greece), as well as establishment of multi-stakeholder entities (*e.g.* in the LAP) and *ad hoc* working groups (*e.g.* in Poland).

In France, the multi-stakeholder body Signal-Spam, an anti-spam public-private partnership established in 2005, provides internet users with an online alert system which has proved to be quite successful. Signal-Spam is currently strengthening co-operation with other entities, including the French Commission nationale de l'informatique et des libertés (CNIL) and the Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (a partnership agreement with the latter was established in May 2011), and is working with a view towards building a similar system at the European level. Furthermore, on the mobile front, telecom operators, in co-ordination with web service publishers, hosts and the French Secrétariat d'Etat chargé de l'industrie et de la consommation have established another alert system, the "33 700", which allows spam victims to report unwanted or unsolicited SMS. Since June 2010, following a request from the French government, this alert system also covers voice spam. Other initiatives include the prevention of abusive telemarketing practices. Since April 2011 l'Association française de la relation client (AFRC), la Fédération du e commerce et de la vente à distance (FEVAD), la Fédération française des télécoms et la Fédération de la vente directe (FVD) have established the "liste PACITEL", a type of "Do not Call Register" which allows consumers to stop reception of unsolicited unauthorised telemarketing calls. The French government is considering to include "PACITEL" in its Projet de loi renforçant les droits, la protection et l'information des consommateurs.

The Association of the German Internet industry, eco e.V., set up a white list project called the "Certified Senders Alliance" (CSA)[46] together with the German Dialogue Marketing Association, (*Deutscher Dialogmarketing Verband* (DDV)). The aim of the project is to create a centrally managed white list of bulk mailers and to improve the quality of the average e-mail by ensuring that non-spam communications are not blocked by spam-filters. The service is free of charge for ISPs and Technology Partners and constitutes a self-regulatory approach to counter spam in Germany.

In Portugal, with the aim of making an analysis of actions taken by ISPs and providers of e-mail services to combat spam, ANACOM promoted an inquiry in May 2008 among all its registered ISPs. This was intended as a first step towards establishing a course of action combating spam, in co-operation with ISPs.

In Japan, the Anti-Spam Mail Promotion Council (ASPC)[47] was established in 2008. This multi-stakeholder initiative, involving ministries, telecommunication carriers, electronic mail senders, advertisement agencies, application service providers, security vendors, interested organisations, consumers and academic experts, was undertaken with the aim of promoting effective anti-spam measures. This would be achieved by ensuring close communication among relevant stakeholders, sharing the latest information, discussing measures to be taken and providing interested parties with relevant information about spam. The Council adopted a Declaration on Combating Spam in 2008, and released an *Anti Spam Handbook* and a *Sender Domain Authentication Manual* in 2011.

As part of its new internal Spam Case Handling Policy, the Hellenic Data Protection Agency (HDPA) recently prepared an information leaflet on legal e-mail marketing.[48] The leaflet is available on the HDPA's website and is enclosed in each warning concerning unsolicited communications sent to data controllers. Stakeholders, such as the Greek Internet Business Network and the Greek Advertising Companies, have also contacted the HDPA for information provision in this respect. In addition, the HDPA focused the Data Protection Day in 2010 on spam. Initiatives related thereto included distribution to citizens of an information leaflet on how to protect themselves from spam. Finally, the HDPA has been co-operating with industry on the creation of a self-regulatory code of conduct for ISPs. The HDPA is now examining the possibility of issuing a code of conduct as a set of guidelines for spam given difficulties in obtaining agreement from ISPs to adopt specific technical measures for the limitation of spam

In Norway, a "Stop online scams" forum was created in 2006. This comprises representatives from business and industry groups, as well as from law enforcement and other public authorities and focused on how consumers could protect themselves from fraudulent e-mails and other types of online fraud. The initiative has proven very useful in improving information sharing on online scams, including scams spread by e-mail; it has drawn significant public attention and media coverage. With respect to SMS spam, the Norwegian Consumer Ombudsman (CO) co-operates on a regular basis with mobile network operators. Such co-operation has been effective in terms of information gathering and preventative behaviour. Further, a working group to develop spam best practices for ISPs in Norway was established by the Norwegian Ministry of Transport and Communications and the Norwegian Post and Telecommunications Authority in 2007. The working group is chaired by ICT-Norway the Association for ICT Businesses and ISPs and includes representatives from Internet Service Providers (ISPs) and Email Service Providers. The best practice, which was subsequently developed, came into effect in January 2008.

In the United States, law enforcement authorities routinely work with Internet service providers, computer security companies and other private entities to understand how spam is affecting the marketplace and to develop targets for prosecution. For example, the FTC currently participates in an informal scams working group with email providers and technology companies aimed at improving intelligence gathering and co-operation with the private sector. The United States has also been actively encouraging the private sector to deploy domain-level email authentication as a tool for fighting spam. A

Spam Summit[49] bringing together industry and enforcement partners to discuss the evolution of spam and to develop new enforcement and technological solutions, and a multi-stakeholder roundtable on phishing education,[50] to discuss strategies for improving outreach to consumers about how to avoid spam messages phishing for personal information, were held by the United States, in 2007 and 2008, respectively.

As a LAP member, the United States has worked in co-operation with business and industry groups on developing more effective cross-border spam enforcement co-operation. In 2007, it led the co-ordination of a joint LAP conference with the MAAWG, which marked the beginning of an on-going dialogue between the LAP and the MAAWG on improving global co-operation between the public and private sectors. In 2008, it facilitated the co-ordination of a joint LAP conference with eco e.V., which furthered the dialogue with industry on improving public-private co-operation on spam issues. In addition, the US Department of Justice, the Federal Bureau of Investigation (FBI), and other federal law enforcement agencies participate in numerous outreach efforts with industry to combat spam, including the National Cyber Forensics and Training Alliance[51] and the FBI's InfraGard programme.[52]

The Internet technical community has also been active in this field, often working in close collaboration with governments and a wide range of stakeholders. The IETF, for instance, initiated work in this area. Some examples include: DomainKeys Identified Mail (DKIM) which provides a method for validating a domain name identity that is associated with a message through cryptographic authentication;[53] and Sender Policy Framework (SPF), an e-mail validation system designed to prevent email spam by verifying sender IP addresses.[54] The Internet Research Task Force has an open Anti-Spam Research Group, which investigates tools and techniques to mitigate the sending and effects of spam.[55]The IETF also liaises with the Messaging Anti-Abuse Working Group.[56]

NOTES

[1] Available at *www.oecd.org/dataoecd/63/28/36494147.pdf*

[2] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C., 2010, c. 23, available at: http://lois-laws.justice.gc.ca/eng/acts/E-1.6/index.html.

[3] For more information on such phenomena, see: OECD, (2009), *Online Identity Theft*, Paris, OECD

[4] Available at: *www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/Specified-E-mail-index.pdf*

[5] Available at: *www.japaneselawtranslation.go.jp/law/detail/?id=66&vm=04&re=01*

[6] Available at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:en:HTML*

[7] Available at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:364:0001:0011:EN:PDF*

[8] Available at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF*

[9] Available at: *www.ftc.gov/os/caselist/0723041/canspam.pdf*

[10] Available at: *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1608enr.txt.pdf*

[11] See FTC, The US SAFE WEB Act: The First Three Years, A Report to Congress (December 2009), available at: www.ftc.gov/os/2009/12/P035303safewebact2009.pdf

[12] See: 47 C.F.R. § 64.1200

[13] See, in particular, articles16-18. Available at: *www.profeco.gob.mx/juridico/pdf/l_lfpc_06062006_ingles.pdf*

[14] See: Turkish Electronic Communications Law No: 5809 of 5 November 2008, available at: *http://en.hukuki.net/index.php?topic=1296.0*

[15] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[16] See: art. 3 let. O, loi fédérale contre la concurrence déloyale 16, RS 241, LCD, available at: www.admin.ch/ch/f/rs/241/a3.html

[17] *www.comlaw.gov.au/Details/C2005C00309*

[18] Available at: *www.legislation.gov.uk/ukpga/2002/40/contents*

[19] Available at: *www.legislation.gov.uk/uksi/2008/1277/contents/made*

[20] See section 224 of the Enterprise Act, and section 21 of the Consumer Protection from Unfair Trading Regulations 2008 (CPRs)

[21] Available in German language at: *www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf*

[22] Available in German language at: *www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf*

[23] Available at: *www.mpo.cz/dokument75810.html*

[24] Available at: *www.giodo.gov.pl/data/filemanager_en/51.pdf*

[25] See: OECD, (2009), Computer Viruses and Other Malicious Software: A Threat to the Internet Economy, Paris, OECD.

[26] For more info on malware, see: OECD, (2009), *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, Paris

[27] See: *www.acma.gov.au/WEB/STANDARD/pc=PC_2861*

[28] See: *www.acma.gov.au/WEB/STANDARD/pc=PC_310317*

[29] See *supra*, note 27

[30] See *supra*, note 3

[31] Responsibility has now passed from BIS to Department of Culture, Media and Sport

[32] Responsibility has now passed from BIS to Department of Culture, Media and Sport

[33] See, Directive 2005/29/EC

[34] See, *inter alia*, decision n. of 9 October 2008, case *PS86 - SMS MESSAGGI IN SEGRETERIA-899 DA CONTATTARE*

[35] See 15 U.S.C. 7712

[36] Available at: *www.legislation.gov.uk/uksi/2003/2426/contents/made*

[37] Available at: *www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%203471-2006-EN.PDF*

[38] See sections 47-50 of CASL

[39] See section 80 of CASL

[40] As per sections 60 of CASL

[41] See article 30

[42] See 16 CFR § 4.11(j)

[43] As per 28 USC § 1782

[44] *www.oecd.org/dataoecd/29/12/35670414.pdf*

[45] See: *www.spamsquad.be/fr/home.html*

[46] More information available at: *www.certified-senders.eu/csa_html/en/266.htm*

[47] Available in Japanese language at: *www.dekyo.or.jp/soudan/anti_spam/index.html*

[48] Available in Greek language at: *www.dpa.gr/pls/portal/docs/PAGE/APDPX/SPAM/%CE%95%CE%9D%CE%97%CE%9C%CE%95%CE%A1%CE%A9%CE%A4%CE%99%CE%9A%CE%9F%20%CE%A6%CE%A5%CE%9B%CE%9B%CE%91%CE%94%CE%99%CE%9F%20SPAM.PDF*

[49] More information available at:*www.ftc.gov/bcp/workshops/spamsummit/index.shtml*

[50] More information available at:*www.ftc.gov/os/2008/07/080714phishingroundtable.pdf*

[51] More information available at:*www.ncfta.net/*

[52] More information available at:*www.infragard.net/*

[53] http://www.dkim.org/

[54] http://tools.ietf.org/html/rfc4408

[55] http://irtf.org/asrg

[56] http://www.maawg.org/

ANNEX I
OECD 2006 RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS AGAINST SPAM

(Adopted by the Council at its 1133rd Session on 13 April 2006)

THE COUNCIL,

Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14th December 1960, in particular Article 5 (b) thereof;

Recognising that spam undermines consumer confidence, which is a prerequisite for the information society and for the success of e-commerce;

Recognising that spam can facilitate the spread of viruses, serve as the vehicle for traditional fraud and deception as well as for other Internet-related threats such as phishing, and that its effects can negatively impact the growth of the digital economy, thus resulting in important economic and social costs for Member countries and non-member economies;

Recognising that spam poses unique challenges for law enforcement in that senders can easily hide their identity, forge the electronic path of their email messages, and send their messages from anywhere in the world to anyone in the world, thus making spam a uniquely international problem that can only be efficiently addressed through international co-operation;

Recognising the need for global co-operation to overcome a number of challenges to information gathering and sharing, for identifying enforcement priorities and for developing effective international enforcement frameworks;

Recognising that current measures, such as numerous bi- and multilateral criminal law enforcement co-operation instruments, provide a framework for enforcement co-operation on criminal conduct associated with spam, such as malware and phishing;

Having regard to the Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (hereinafter "Cross-border Fraud Guidelines"), which sets forth principles for international co-operation among consumer protection enforcement agencies in combating cross-border fraud and deception [C(2003)116];

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58] (hereinafter "Privacy Guidelines"), and the Ministerial Declaration on the Protection of Privacy on Global Networks [C(98)177];

Recognising that, in some instances, the Cross-border Fraud Guidelines and the Privacy Guidelines may apply directly to cross-border spam enforcement co-operation and that even where this is not the case, many of the principles expressed in these Guidelines can be usefully tailored to develop appropriate national frameworks and facilitate international co-operation to enforce laws against spam;

Recalling that, while cross-border enforcement co-operation is an important element in tackling the global problem of spam, it is necessary in this respect to adopt a comprehensive national approach which also addresses regulatory and policy issues, facilitates the development of appropriate technical solutions, improves education and awareness among all players and encourages industry-driven initiatives;

On the joint proposal of the Committee for Information, Computer and Communications Policy and the Committee on Consumer Policy:

AGREES that:

For the purposes of this Recommendation, and without prejudice to other existing co-operation instruments "Spam Enforcement Authorities" means any national public body, as determined by each Member country, that is responsible for enforcing Laws Connected with Spam and has powers to (a) co-ordinate or conduct investigations or (b) pursue enforcement proceedings, or (c) both.

For the purposes of this Recommendation, "Laws Connected with Spam" means (a) laws specifically targeting electronic communications; or (b) general laws, such as privacy laws, consumer protection laws or telecommunication laws that may apply to electronic communications.

This Recommendation is primarily aimed at national public bodies, with enforcement authority for Laws Connected with Spam. It is recognised that some Member countries have many competent bodies, some of which are regional or local, that can take or initiate action against spam. It is also recognised that, in some Member countries, private enforcement bodies may play a very important role in ensuring enforcement of Laws Connected with Spam, including in cross-border situations.

This Recommendation covers cross-border spam enforcement co-operation only in areas where the conduct prohibited by the Laws Connected with Spam of the Member country receiving a request for assistance is substantially similar to conduct prohibited by the Laws Connected with Spam of the Member country requesting assistance. Co-operation under this Recommendation does not affect the freedom of expression as protected in laws of Member countries.

Co-operation under this Recommendation focuses on those violations of Laws Connected with Spam that are most serious in nature, such as those that (a) cause or may cause injury (financial or otherwise) to a significant number of recipients, (b) affect particularly large numbers of recipients (c) cause substantial harm to recipients.

In all instances, the decision on whether to provide assistance under this Recommendation rests with the Spam Enforcement Authority receiving the request for assistance.

This Recommendation encourages Member countries to co-operate in this area under any other instruments, agreements, or arrangements.

RECOMMENDS that:

Member countries work to develop frameworks for closer, faster, and more efficient co-operation among their Spam Enforcement Authorities that includes, where appropriate:

a) Establishing a domestic framework.

Member countries should in this respect:

(i) Introduce and maintain an effective framework of laws, Spam Enforcement Authorities, and practices for the enforcement of Laws Connected with Spam.

(ii) Take steps to ensure that Spam Enforcement Authorities have the necessary authority to obtain evidence sufficient to investigate and take action in a timely manner against violations of Laws Connected with Spam that are committed from their territory or cause effects in their territory. Such authority should include the ability to obtain necessary information and relevant documents.

(iii) Improve the ability of Spam Enforcement Authorities to take appropriate action against (a) senders of electronic communications that violate Laws Connected with Spam and (b) individuals or companies that profit from the sending of such communications.

(iv) Review periodically their own domestic frameworks and take steps to ensure their effectiveness for cross-border co-operation in the enforcement of Laws Connected with Spam.

(v) Consider ways to improve redress for financial injury caused by spam.

b) Improving the ability to co-operate.

Member countries should improve the ability of their Spam Enforcement Authorities to cooperate with foreign Spam Enforcement Authorities.

Member countries should in this respect:

(i) Provide their Spam Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to violations of their Laws Connected with Spam upon request, in appropriate cases and subject to appropriate safeguards.

(ii) Enable their Spam Enforcement Authorities to provide investigative assistance to foreign authorities relating to violations of their Laws Connected with Spam upon request, in appropriate cases and subject to appropriate safeguards, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying persons or things.

(iii) Designate a contact point for co-operation under this Recommendation and provide the OECD Secretariat with updated information regarding their Laws Connected with Spam and the Spam Enforcement Authority designated as the contact point. The OECD Secretariat will keep record of this information and make it available to interested parties.

c) Improving procedures for co-operation.

Before making requests for assistance as foreseen in the previous paragraphs, Spam Enforcement Authorities should:

(i) Proceed to some preliminary investigative work to determine whether a request for assistance is warranted, and is consistent with the scope and priorities set forth by this Recommendation.

(ii) Attempt to prioritise requests for assistance and, to the extent possible, make use of common resources such as the OECD website on spam, informal channels, existing international networks and existing law enforcement co-operation instruments to implement this Recommendation.

d) Co-operating with relevant private sector entities.

Spam Enforcement Authorities, businesses, industry groups, and consumer groups should cooperate in pursuing violations of Laws Connected with Spam. In particular, Spam Enforcement Authorities should cooperate with these groups on user education, promote their referral of relevant complaint data, and encourage them to share with Spam Enforcement Authorities investigation tools and techniques, analysis, data and trend information.

Member countries should encourage co-operation between Spam Enforcement Authorities and the private sector to facilitate the location and identification of spammers.

Member countries should also encourage participation by private sector and non-member economies in international enforcement co-operation efforts; efforts to reduce the incidence of inaccurate information about holders of domain names; and efforts to make the Internet more secure.

Where appropriate, Spam Enforcement Authorities and the private sector should continue to explore new ways to reduce spam.

INVITES non-member economies to take due account of this Recommendation and collaborate with Member countries in its implementation.

INSTRUCTS the Committee for Information, Computer and Communications Policy and the Committee on Consumer Policy to monitor the progress in cross-border enforcement co-operation in the context of this Recommendation within three years of its adoption and thereafter as appropriate.

ANNEX II
SPAM QUESTIONNAIRE

The questionnaire covers issues related to the principles in the OECD Recommendation. It also requests information on new forms of cyber fraud perpetrated through the use of spam, on various platforms.

- What changes, if any, have been made to spam laws in your country since 2006? Have there been any changes in domestic legislation that have affected cross-border enforcement co-operation to address spam issues since 2006? Are any such changes needed? If so, what types of changes would you recommend in your laws?

- Has your country enacted criminal laws specifically designed to combat spam? If so, please provide a citation to, or text of, the relevant criminal law(s).

  - Do authorities in your country have the necessary authority to obtain evidence sufficient to investigate and take action against spammers, or individuals or companies profiting from the sending of spam? If no, please explain why. Would this authority include the ability to investigate and take action against spammers operating in your country by sending to recipients?

  - How has the evolution of spam affected authorities' enforcement efforts? Have enforcement actions involving malware delivered via spam increased?

  - Does the domestic legislation in your country authorise authorities to investigate spam sent through various media (including e-mail, SMS, fax)?

  - Do authorities have sufficient technical training to investigate spam cases that involve abuses of new technologies to deliver unsolicited messages? If no, please explain.

  - Does your domestic legislation permit redress to consumers for financial injury caused by spam? If so, does it also authorise redress to foreign consumers? Could you identify spam cases in which authorities were able to provide redress to consumers (domestic or foreign)?

  - How many spam-related actions have authorities in your country initiated since 2006 (*e.g.* court cases, investigations, administrative proceedings, assistance with foreign investigations)? How many of these cases involved cross-border co-operation? Were any of these cases brought with the assistance of the LAP members? Please provide a narrative description of the major spam-related actions identified in response to this question.

- Do authorities in your country have the ability to provide investigative assistance to foreign authorities? Do authorities in your country have the ability to refer spam cases to other countries or receive referrals from other countries? If no, please describe the obstacles.

- What mechanisms have been put in place or used to handle cross-border requests and cases?

- Are there national contact points created under the OECD Recommendation instituted in your country? If so, please provide the name and contact information. What role, if any, have the national contact points played in strengthening co-operation? How could their role be strengthened?

- Please provide examples of how authorities in your country have co-operated with businesses, industry groups, and consumer groups to address violations of spam laws.

- What technical challenges, legal problems, or other limitations have authorities encountered in strengthening cross-border co-operation? Do you believe that cross-border co-operation is currently sufficient? How could it be improved?