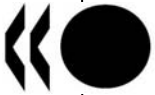


**Unclassified**

**DSTI/CP/ICCP/SPAM(2004)3/FINAL**



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

**13-May-2005**

**English - Or. English**

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

**Task Force on Spam**

**ANTI-SPAM LAW ENFORCEMENT REPORT**

**DSTI/CP/ICCP/SPAM(2004)3/FINAL  
Unclassified**

**English - Or. English**

**JT00184175**

Document complet disponible sur OLIS dans son format d'origine  
Complete document available on OLIS in its original format

## **FOREWORD**

The OECD Task force on Spam discussed this document during its meeting in March 2005, and recommended it for declassification to the CCP and ICCP Committees through a written procedure, which was completed on 23 April 2005.

The report was prepared by Jack Radisch, of the OECD Secretariat. It is published under the responsibility of the Secretary-General of the OECD.

**Copyright OECD, 2005.**

**Applications for permission to reproduce or translate all or part of this material should be made to:**

**Head of Publications Service, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.**

## TABLE OF CONTENTS

REPORT ON SPAM LAW ENFORCEMENT .....	4
Main Points .....	4
INTRODUCTION .....	6
I. The OECD Questionnaire on Cross Border Enforcement of Anti-Spam Laws .....	7
II. Types of public agencies with responsibility to enforce laws related to spam.....	8
III. National enforcement frameworks .....	13
IV. Challenges to effective cross-border enforcement .....	20
V. Current efforts to address the challenges of information sharing and gathering.....	25
VI. Conclusions .....	30
ANNEX A OECD QUESTIONNAIRE ON CROSS-BORDER ENFORCEMENT OF ANTI-SPAM LAWS .....	33
Instructions .....	33
COUNTRY: .....	34
Section I: Description of national enforcement framework .....	34
Section II: Cross-border aspects of anti-spam law enforcement.....	35
ANNEX B OECD TABLE OF CASES.....	36

## REPORT ON SPAM LAW ENFORCEMENT

### **Main points**

This report presents a snapshot synthesis of responses received from OECD member countries on the nature and extent of the powers possessed by public or publicly funded agencies with responsibility for enforcing laws used to take action against spammers. It aims to provide a basis for discussion on how to improve the capacity of enforcement agencies to respond to spam complaints and to co-operate with foreign counterparts.

### *Types of public agencies with responsibility to enforce laws related to spam*

Responses show that there is a diversity of enforcement agencies with responsibility over spam and that collaboration among the competent agencies is still in development. Both in countries that have a specific anti-spam law and those that do not, these agencies include consumer protection agencies, data protection agencies, communications regulators, and criminal authorities. For each type of agency, the report provides general information on their missions, and more detailed explanations on their powers. It also includes tables mentioning, for each country, the various agencies with responsibility over spam.

### *National enforcement frameworks*

Responses indicate that agencies with responsibility over spam have varied powers to investigate, initiate enforcement action, and obtain sanctions. This report provides information on the diverse enforcement procedures at the disposal of these agencies, and on their differing practices regarding: complaints handling, evidence gathering, priority setting, available fines, sanctions, and remedies. The processes for initiating actions fall generally into three categories: administrative, civil and criminal. Once a process has been initiated, available sanctions and remedies include: warning letters, injunctions, imprisonment, fines, monetary redress orders, and revocation of a business license.

### *Challenges to effective cross-border enforcement*

Building on the responses and independent research, the report outlines prominent issues confronting enforcement agencies when they wish to co-operate with foreign counterparts in taking action against spammers. It shows that the tools possessed by enforcement agencies may not always be adequate for effective co-operation, and provides a non-exhaustive list of challenges including:

- Restrictions on the scope of enforcement authority.
- Limitations on information gathering and sharing.
- The limited enforceability of outcomes across borders; and
- Varied enforcement priorities among the enforcement agencies.

The report also includes examples of types of spam complaints taking priority for cross-border enforcement.

### ***Current efforts to address the challenges of information sharing and gathering***

The report shows that a number of initiatives have been taken to address the cross-border spam enforcement challenges, and includes information on multi-lateral or bilateral Memorandum of Understanding (MOUs) specific to spam enforcement, on international agreements in related policy areas, on policy initiatives in other international organisations, and on efforts by the private sector. Agencies in several countries have entered into MOUs with foreign counterparts to improve co-operation. In Europe, the recent "cooperation procedure concerning the transmission of complaint information and intelligence" has been agreed upon by 16 anti-spam enforcement authorities in 13 member countries. On a more multilateral basis, some 27 agencies and 12 industry signatories have signed the London Action Plan (LAP) a "best efforts" initiative to promote international spam enforcement cooperation. Other relevant international initiatives in closely related areas such as the OECD's Cross-border Fraud Guidelines or the Council of Europe Cybercrime Convention are also mentioned. The report finally highlights that the private sector can also serve a key role in assisting the public bodies responsible for enforcing anti-spam laws, including by providing technical assistance and evidence needed to identify spammers.

### ***Conclusions***

While noting progress already made, the report concludes that significant steps are still required for national and cross-border anti-spam efforts to become effective. To serve as a basis for the discussion on further OECD work to facilitate co-operation on anti-spam law enforcement, the conclusions single out characteristics of the current situation that governments may want to consider and address.

## INTRODUCTION

The objective of this report is to analyse the nature and extent of the powers possessed by public or publicly funded agencies with responsibility for enforcing laws that are used to take action against spammers. The report is intended to provide a basis for the OECD Task Force on Spam to consider how to improve the capacity of enforcement agencies to respond to spam complaints and co-operate with foreign counterparts, and to present some examples of successful implementation of domestic and cross-border enforcement mechanisms (see Table of Cases, Annex B). The scope of the report does not encompass projects undertaken by law enforcement agencies to improve technical solutions to combat spam (such as securing servers or authenticating email). Information regarding the private sector's initiatives to combat spam through technical means and litigation are also beyond the scope of this report.

There is consensus among policy makers that spam constitutes an ill for the digital economy and that law enforcement plays an important role in the multi-faceted strategy to combat it. Nineteen OECD member countries have either enacted specific laws or amended existing laws to regulate and sanction spam, and legislation to this end is pending in three more member countries. In addition, five member countries use the rules and legal principles found in already existing law to combat the wide range of abuses conducted through electronic communication technologies such as e-mail, SMS (short message service), instant messaging, fax and VoIP (voice over Internet protocol). Taken together, these laws constitute the corpus of "anti-spam" law.

Successful enforcement of anti-spam law serves as an economic disincentive to spammers by imposing fines and penalties which undermine their profits, provides a state-sponsored mechanism for protection and redress to victims of spam-related consumer fraud, and vindicates the privacy rights of spam recipients. Ultimately, an increased enforcement presence may help restore trust in e-mail systems that has been eroded by spam.

Enforcement agencies, however, face significant obstacles in carrying out their duties, due to the difficulty and expense incurred to track down spammers, gather sufficient evidence to prosecute them and recovering monetary rewards for victims.

E-mail spammers may easily conceal their true identity and location by falsifying information in the message header, routing e-mail through open proxies and relays, exploiting a zombie drone or using an untraceable Internet connection. Even when a suspect can be identified, evidence is required to prove that he is responsible for the electronic communication being sent. A recent case in the Netherlands demonstrates that simple possession of the computers and software used to send spam e-mail is not sufficient in all jurisdictions to prove that one actually committed the illegal act of sending spam. In Australia, by way of contrast, a legal inference arises in cases where a person receives the financial benefit of spam that has been sent, whether he in fact sent it or sponsored it. Once a suspect has been identified and is proved to be the source of spam, there remains the challenge of recovering any money that victims of fraud have paid for goods or services. Even if such proceeds can be identified and located, enforcement agencies may not have the means to take possession of them if they are located in a foreign territory.

Spammers now send billions of electronic communications to e-mail addresses and mobile phones around the globe, without discerning market capacity or ability to understand the language of the message - much less showing concern for the impact of bulk messages upon network operators. In addition, most

OECD member countries receive more spam from foreign sources than domestic sources. Law enforcement investigations of spammers have revealed other international aspects of the spammer *modus operandi*. For example, businesses that market fraudulent goods through spam are frequently registered under the laws of a foreign jurisdiction, and their proceeds are often transferred to offshore accounts where their assets are held in trust and therefore protected from judgement collection. Spam is clearly an international problem, and only law enforcement policies which take account of its cross border aspects will provide the legal tools necessary to succeed at the international level.

The fact that spammers make the effort to conceal their identities and place assets abroad indicates that they know enforcement actions are difficult to execute across borders. There are multiple cross-border challenges facing enforcement agencies, including the non-extraterritorial application of domestic spam law, tracing the spammer's identity, gathering and sharing information from foreign enforcement agencies and making a successful claim on assets held in a foreign bank. Consequently, national enforcement agencies - in particular from countries that are not usually producers of spam - have an interest in co-operating at the international level if they wish to hold spammers accountable for their activities.

## **I. The OECD Questionnaire on Cross Border Enforcement of Anti-Spam Laws**

The Revised OECD Work Plan on Spam for 2004-2006 calls for investigating the improvement of cross-border co-operation in the enforcement of anti-spam laws. Specifically, the work plan seeks to build upon the study of anti-spam laws (conducted prior to the Brussels OECD Workshop on Spam in February 2004), which had focused on whether member countries had enacted anti-spam legislation and, if so, whether they had adopted the opt-in or opt-out approach. To this end, a questionnaire was distributed in July 2004 (see Annex A) to elicit information for the following purposes: to identify public agencies responsible for the enforcement of anti-spam laws, to analyse their powers and procedures to receive complaints, conduct investigations and take action against spammers, and to determine the key challenges to cross-border co-operation. Twenty-eight responses to the questionnaire have been received from the following OECD member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Korea, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States. In connection with a meeting which brought together enforcement agencies on 11 October 2004 in London, two non-member countries submitted responses to the questionnaire: Cyprus and Peru.

Specific anti-spam legislation in several countries expressly grants certain private parties the right to initiate a civil suit for damages against spammers. Indeed, the largest Internet service providers (ISPs) that operate e-mail account services have undertaken a co-ordinated strategy to bring civil law suits against the most prolific spammers. Private litigation has had a role in the overall effectiveness of anti-spam laws by rendering the business model for spammers less profitable. The focus of the work at OECD, however, is the activities of public, or publicly funded, enforcement agencies at the national level.

To gather information regarding each phase of an enforcement action, the questionnaire inquired about the powers and limits of any agency with an "enforcement role". An enforcement role here means any one of the following three functions: receiving complaints, conducting an investigation, or initiating proceedings in a court or tribunal. Although some agencies are not empowered to seek sanctions or remedies against spammers, they may nonetheless play an important role in international co-operation for the purpose of receiving complaints or gathering and sharing information. Respondents were encouraged to consult with the private sector and certain other non-governmental organisations that play a role in anti-spam enforcement, and asked to identify obstacles to sharing information for the purpose of an investigation.

The Report presents a synthesis of the powers and practices of enforcement agencies as revealed in responses to the questionnaire. Many respondents did not provide information regarding every agency with an enforcement role related to spam. Task Force members are invited to provide information to supplement the answers provided by their countries, which are posted on the OECD Spam EDG.

## II. Types of public agencies with responsibility to enforce laws related to spam

Responses to the questionnaire revealed the following principal types of public enforcement agencies with responsibility for enforcing anti-spam laws: (19) consumer protection authorities; (18) data protection authorities; (12) communications regulators; (9) police cyber-crime units or criminal prosecutors; and (4) various others (for a list of the different authorities in each country, see infra tables 1, 2 and 3). That is, the 29 countries responding to the Questionnaire identified 62 enforcement agencies. In every country without a specific anti-spam law, enforcement of the various laws applicable to conduct perpetrated through spam falls within the jurisdiction of several agencies. In Canada, for example, the Competition Bureau has the power to initiate proceedings against spammers if commercial representations contained in an e-mail are false or misleading, whereas the Privacy Commissioner may take action in cases where personal information, such as an e-mail address, is used without the consent of the data subject.

Several reasons account for the plurality of enforcement agencies with responsibility for spam. Jurisdiction may be divided territorially between regional offices of the same type (for example, regional offices of the *Fernmeldebüro* – a telecommunications authority in Austria). The principal reason, however, is that the variety of abuse committed through electronic communications may violate protections provided for under various laws, each attributing responsibility to a different agency. Spammers may violate:

- **Consumer protection law** by deceptively inducing recipients into paying for worthless wares or tricking recipients into various kind of scams and frauds (which could also result in breaches of criminal laws – see below).
- **Criminal law**, in case e-mails are used to send viruses or high volumes of electronic messages to the same e-mail account disabling or disrupting the recipient's ability to use it, or again in the case of fraudulent behaviour, when it is also a violation of criminal laws (such as the case of phishing).
- **Data protection law**, in case spammers are sending unsolicited commercial e-mail for the purpose of marketing without the recipient's prior consent, *i.e.* using personal information (the e-mail addresses) without the permission of the owner.
- **Telecommunication law and data protection law**, when e-mails contain false return addresses and misleading subject lines or fail to offer an opt-out service or to respect opt-out requests.

Even where a specific anti-spam law has been enacted, jurisdiction is divided between more than one enforcement agency in all but seven countries (Cyprus, Czech Republic, Denmark, Ireland, Peru, Spain and Sweden). However, although several agencies may be dealing with spam in the same countries, in several cases there is a specific authority which takes the lead, and puts more effort and resources in the fight against spammers. The leading agency plays an important role at both national and international levels, functioning as a point of contact and participating in international fora. This is the case, for example, of the FTC (a consumer protection agency), which has a larger role in the field than the FCC (a telecommunications authority), which deals principally with mobile spam, or of the French CNIL (data protection authority), which is very active in the sector, which is not the principal focus for the other authority involved, the consumer protection agency (DGCCRF).

In Australia, for example, the ACA (Australian Communication Authority) is responsible for enforcing the Spam Act, and has the power to investigate complaints about spamming. However, where spam messages carry content which is itself prohibited, the sender may also be subject to other criminal or civil laws. The ACA usually reports such spam to the relevant criminal or civil enforcement agency and co-operatively works on any investigation. In cases where the spam message contains misleading or deceptive content, the Australian Competition and Consumer Commission (ACCC) will intervene, applying the Trade Practices Act, a piece of legislation containing both civil and criminal provisions. Particularly serious infractions, for example messages containing child pornography, fraudulent content, or resulting in computer crimes, are directly under the responsibility of the Australian High-Tech Crime Centre (AHTCC), part of the Australian Federal Police, while cases with implications for financial markets are followed also by the Australian Security and Investments Commission (ASIC). As for the Web site referenced in the spam message, it is the Australian Broadcasting Authority (ABA) that has the power to require ISPs to take down Web sites that contain offensive/illegal content in spam (such as illegal pornographic material).

### *Consumer protection agencies*

Respondents to the questionnaire identified 19<sup>1</sup> consumer protection agencies with a role related to the enforcement of specific anti-spam laws or other laws that may be used against spammers (see Table 1). In general, consumer protection agency responsibilities include taking action against purveyors of deceptive or fraudulent marketing of goods and services. Consumer protection agencies typically bring action against spammers in cases where they send e-mail containing deceptive or fraudulent ads, or are linked to a Web site through which a commercial scam is conducted. From a policy perspective these activities are considered to be particularly odious, since they undermine the trust of users in online services.

The responses to the questionnaire indicate that nearly every consumer protection agency has the power to compel a party under investigation to provide evidence required for the carrying out of its duties. Consumer protection agencies possess a variety of enforcement powers, such as the ability to seek injunctions; levy administrative fines; bring suit against spammers in civil court, and refer spammers to criminal prosecutors (see Tables 4 and 5).

---

<sup>1</sup> In Germany, several private consumer organisations serve a role similar to the public consumer protection agencies mentioned in this section. The report counts these private (although publicly funded) organisations among public consumer protection agencies, due to the fact that they are empowered to bring legal suits against spammers under German law.

Table 1. **Consumer protection agencies with responsibility for enforcement of laws related to spam**

<b>Country</b>	<b>Consumer protection agencies</b>	<b>Link</b>
<b>Australia</b>	Australian Competition and Consumer Commission	<a href="http://www.accc.gov.au/content/index.phtml/itemId/54073">www.accc.gov.au/content/index.phtml/itemId/54073</a>
<b>Belgium</b>	Direction Générale du Contrôle et de la Médiation	<a href="http://www.mineco.fgov.be/redir_new.asp?loc=/protection_consumer/complaints/complaints_fr_001.htm">www.mineco.fgov.be/redir_new.asp?loc=/protection_consumer/complaints/complaints_fr_001.htm</a>
<b>Canada</b>	Competition Bureau Canada	<a href="http://competition.ic.gc.ca/epic/internet/incb-bc.nsf/en/Home">http://competition.ic.gc.ca/epic/internet/incb-bc.nsf/en/Home</a>
<b>Denmark</b>	Danish Consumer Ombudsman	<a href="http://www.consumerombudsman.dk">www.consumerombudsman.dk</a>
<b>Finland</b>	Finnish Consumer Ombudsman and Agency	<a href="http://www.kuluttajansuoja.fi">www.kuluttajansuoja.fi</a>
<b>France</b>	Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes	<a href="http://www.finances.gouv.fr/DGCCRF/">www.finances.gouv.fr/DGCCRF/</a>
<b>Germany</b>	Federation of German Consumer Organisations (vzbv)	<a href="http://www.vzbv.de/go/english/index.html">http://www.vzbv.de/go/english/index.html</a>
<b>Hungary</b>	General Inspectorate for Consumer Protection	<a href="http://www.fvf.hu/">www.fvf.hu/</a>
<b>Italy</b>	Antitrust Authority Consumer protection council (Ministero delle Attività Produttive)	<a href="http://www.agcm.it/">http://www.agcm.it/</a> <a href="http://www.minindustria.it/organigramma/index.php?sezione=organigramma&amp;tema_dir=tema2&amp;nodo=63">http://www.minindustria.it/organigramma/index.php?sezione=organigramma&amp;tema_dir=tema2&amp;nodo=63</a>
<b>Japan</b>	Japanese Fair Trade Commission Ministry of Economy Trade and Industry	<a href="http://www.jftc.go.jp/">www.jftc.go.jp/</a> <a href="http://www.meti.gov.jp">www.meti.gov.jp</a>
<b>Korea</b>	Korea Fair Trade Commission Korea Consumer Protection Board	<a href="http://www.ftc.go.kr/eng/">www.ftc.go.kr/eng/</a> <a href="http://www.cpb.or.kr">www.cpb.or.kr</a>
<b>Mexico</b>	Profeco	<a href="http://www.profeco.gob.mx/html/inicio/inicio.htm">www.profeco.gob.mx/html/inicio/inicio.htm</a>
<b>Norway</b>	Norwegian Consumer Ombudsman	<a href="http://www.forbrukerombudet.no/index.db2?id=490">www.forbrukerombudet.no/index.db2?id=490</a>
<b>Poland</b>	Office for Competition and Consumer Protection	<a href="http://www.uokik.gov.pl">www.uokik.gov.pl</a>
<b>Slovak Republic</b>	Slovak Trade Inspection	<a href="http://www.soi.sk">www.soi.sk</a>
<b>Sweden</b>	Swedish Consumer Agency/ Consumer Ombudsman	<a href="http://www.konsumentverket.se/mallar/en/startsidan.asp?lngCategoryId=646">www.konsumentverket.se/mallar/en/startsidan.asp?lngCategoryId=646</a>
<b>United Kingdom</b>	Office of Fair Trading	<a href="http://www.oft.gov.uk/default.htm">www.oft.gov.uk/default.htm</a>
<b>United States</b>	Federal Trade Commission	<a href="http://www.ftc.gov/">www.ftc.gov/</a>
<b>Peru</b>	INDECOPI	<a href="http://www.indecopi.gob.pe/">www.indecopi.gob.pe/</a>

### *Data protection authorities*

Respondents identified 18 data protection authorities as having a role related to the enforcement of anti-spam laws (See Table 2). The Korean Information Security Agency, while not a data protection

agency as such, is responsible for enforcing provisions of legislation that are similar to data protection laws. In many OECD countries, data protection authorities are responsible for enforcing legislation that restricts the collection and use of personal information. Member States of the European Union (EU) in particular consider e-mail addresses which identify an individual to be personal information. The Directive on Electronic Communication and Privacy (2002/58 EC), implemented into national legislation by all EU Member States, prohibits sending unsolicited commercial e-mail for the purpose of marketing without the data subject's prior consent. In addition, data protection law typically grants the data subject control over information to which he is the referent and provides for the right to correct information. Consistent with this principle, the Directive requires that the e-mail sender provide a valid address for opt-out requests and forbids the sender from concealing his identity. Outside the European Union, the Privacy Commissioners in Canada, New Zealand, Switzerland and Cyprus have responsibility for enforcing laws related to spam.

The responses to the questionnaire indicate the primary investigative power possessed by data protection authorities (DPAs) is the authority to request that information be provided voluntarily; failing voluntary compliance some DPAs have the power to compel production of documentary evidence. Data protection authorities typically initiate action by writing warning letters to request spammers to change their business practices. In case compliance with their directions is not forthcoming, most of the governmental authorities are empowered to levy administrative fines against spammers, others may seek fines in civil court, while some of them may only seek fines in criminal court (see Table 4).

An example of a data protection authority with new powers is the *Commission Nationale de l'Informatique et des Libertés* (CNIL) in France. Following new legislation, the CNIL has not only the possibility to make enquiries and investigate before deciding if it will be necessary to refer offenders to the public prosecutor who can start a criminal action, but also to apply one of the administrative sanctions within its powers, as for example to issue a warning which can be publicly diffused or ask the offender to stop sending the allegedly illegal e-mails. If these admonitions have no effect, the CNIL can apply an administrative fine – up to EUR 150 000 or to EUR 300 000 for repeat offenders – or use an injunction against the sender to stop his or her activity.

In particular, warning letters and referring spam cases to criminal authorities seems to be DPAs' most commonly used method of taking action against spammers. The Korean Information and Security Agency (KISA) has been extremely active in this regard; it reports having sent 15 462 warning letters to businesses and referred 1 463 cases to public prosecutors, however the criminal authorities have not yet brought any formal charges in response.

Table 2. **Data protection authorities with responsibility for enforcement of laws related to spam**

<b>Data protection authority</b>		
<b>Belgium</b>	Privacy Protection Commission	<a href="http://www.privacy.fgov.be/">www.privacy.fgov.be/</a>
<b>Canada</b>	Office of the Privacy Commissioner	<a href="http://www.privcom.gc.ca/">www.privcom.gc.ca/</a>
<b>Czech Republic</b>	Personal Data Protection Office	<a href="http://www.uoou.cz/">www.uoou.cz/</a>
<b>Finland</b>	Data Protection Ombudsman	<a href="http://www.tietosuojafi.fi">www.tietosuojafi.fi</a>
<b>France</b>	Commission Nationale de l'Informatique et des Libertés	<a href="http://www.cnil.fr/">www.cnil.fr/</a>
<b>Ireland</b>	Data Protection Commissioner	<a href="http://www.dataprivacy.ie/">www.dataprivacy.ie/</a>
<b>Italy</b>	Italian Data Protection Authority	<a href="http://www2.garanteprivacy.it/">http://www2.garanteprivacy.it/</a>
<b>Korea (Rep.)</b>	Korea Information Security Agency	<a href="http://www.kisa.or.kr/english/">www.kisa.or.kr/english/</a>
<b>Netherlands</b>	Dutch Data Protection Agency	<a href="http://www.cbppweb.nl/en/index.htm">www.cbppweb.nl/en/index.htm</a>
<b>New Zealand</b>	Office of the Privacy Commissioner	<a href="http://www.privacy.org.nz/top.html">www.privacy.org.nz/top.html</a>
<b>Norway</b>	The Data Inspectorate	<a href="http://www.datatilsynet.no/">www.datatilsynet.no/</a>
<b>Poland</b>	Inspector General for the Protection of Personal Data	<a href="http://www.giodo.gov.pl/168/i/en/">www.giodo.gov.pl/168/i/en/</a>
<b>Portugal</b>	Data Protection Commission	<a href="http://www.cnpd.pt/">www.cnpd.pt/</a>
<b>Spain</b>	Spanish Data Protection Agency	<a href="http://www.aepd.es">www.aepd.es</a>
<b>Sweden</b>	Data Inspection Board	<a href="http://www.datainspektionen.se/in_english/start.shtml">www.datainspektionen.se/in_english/start.shtml</a>
<b>Switzerland</b>	Federal Data Protection Commissioner	<a href="http://www.edsb.ch/e/aktuell/index.htm">www.edsb.ch/e/aktuell/index.htm</a>
<b>United Kingdom</b>	Office of the Information Commissioner	<a href="http://www.informationcommissioner.gov.uk/">www.informationcommissioner.gov.uk/</a>
<b>Cyprus</b>	Commissioner for Personnel Data Protection	<a href="http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument">www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument</a>

### *Communications regulators*

Communications regulators are generally responsible for regulating domestic and international communications by radio, television, wire, satellite and cable. To carry out these duties they are typically charged with processing applications for licenses, analysing consumer complaints, conducting investigations and developing and implementing regulatory programmes. In several countries spam is considered a problem to be tackled also by communication regulators, which in certain cases have a primary enforcement role to play in the field, in view of the fact that unsolicited commercial e-mails are today flooding communication networks, hampering e-mail delivery and the functioning of the Internet as a whole (see Table 3). Respondents reported a variety of enforcement powers, including: the ability to make spot inspections at a place of business, write letters of inquiry and, in the case of civil litigation, subpoena witnesses and documents. Eight communication regulators may levy administrative fines against spammers, and one may bring suit against spammers in civil court.

Table 3. Communications regulators with responsibility for enforcement of laws related to spam

<b>Communications regulator</b>		
<b>Australia</b>	Australian Communications Authority	<a href="http://www.aca.gov.au/consumer_info/spam/consumerinformation.htm">www.aca.gov.au/consumer_info/spam/consumerinformation.htm</a>
	Australian Broadcasting Authority	<a href="http://www.aba.gov.au/">www.aba.gov.au/</a>
<b>Austria</b>	Telecommunications Authority (especially office for Vienna, Burgenland and Lower Austria)	
<b>Finland</b>	Finnish Communications Regulatory Authority	<a href="http://www.ficora.fi">www.ficora.fi</a>
<b>Hungary</b>	National Communications Authority	<a href="http://www.hif.hu/english/index1.html">www.hif.hu/english/index1.html</a>
<b>Italy</b>	Authority for communications safeguards	<a href="http://www.comunicazioni.it/">www.comunicazioni.it/</a>
<b>Japan</b>	Ministry of Internal Affairs and Communications (MIC)	<a href="http://www.soumu.go.jp/joho_tsusin/eng/index.html">http://www.soumu.go.jp/joho_tsusin/eng/index.html</a>
<b>Mexico</b>	COFETEL	<a href="http://www.cft.gob.mx/">www.cft.gob.mx/</a>
<b>Netherlands</b>	OPTA	<a href="http://www.opta.nl/">www.opta.nl/</a>
<b>Portugal</b>	National Authority for Communications	<a href="http://www.anacom.pt">www.anacom.pt</a>
<b>Slovak Republic</b>	Telecommunications Office	<a href="http://www.teleoff.gov.sk">www.teleoff.gov.sk</a>
<b>Turkey</b>	Telecommunication Authority	<a href="http://www.tgm.gov.tr/">www.tgm.gov.tr/</a>
<b>United States</b>	Federal Communications Commission	<a href="http://www.fcc.gov/">www.fcc.gov/</a>

### III. National enforcement frameworks

Responses to the questionnaire indicated a wide variety of powers, processes and sanctions at the disposal of the various types of enforcement agencies described above. This section aims to extract some key elements to consider how to improve the capacity of enforcement agencies to respond to complaints, gather sufficient evidence, take effective action against spammers and enhance co-ordination.

#### A. Investigatory powers

##### *Notifying enforcement agencies*

The first phase of law enforcement involves receiving complaints about spam, which requires communication with and outreach to the recipients of spam and the operators of networks through which it is sent. Every respondent to the questionnaire indicated that the agencies with responsibility for enforcing a spam-related law provide at least one means for recipients to notify the authority concerned, *e.g.* via e-mail, filling out a form on the agency Web site, telephone, fax or post. Only in a few cases does the enforcement agency provide an online complaint form, although this is indeed an efficient means to collect complaints and evidence. Commonly users have to send their complaint in writing, either through the post, or by e-mail, in this last case the supposedly illegitimate e-mail message is directly attached to the complaint, allowing the authority to determine whether it violates the law.

In the United States, the Federal Trade Commission (FTC) (consumer protection agency) makes significant efforts to reach out to recipients of spam by managing or interacting with several complaint resources. Consumers can file a complaint with the FTC on-line against a company or organisation that they believe defrauded them by contacting the FTC Consumer Response Center or use an e-mail address created to specifically gather spam complaints. This spam mailbox was created in 1998 to encourage consumers to send their spam message with the purpose of future law enforcement action and data mining. The mailbox has received over 140 million spam messages and helps FTC identify trends in spam and consider which spammers to pursue. The FTC also receives complaints from Consumer Sentinel, a database of complaints accessible by law enforcement agencies that enter into a prior agreement with the FTC to keep the complaints confidential. This database collects complaints that consumers have filed through e-consumer.gov (see Section V), an initiative sponsored by the International Consumer Protection and Enforcement Network (ICPEN).

The idea of operating a spam box has also been developed in France, where the CNIL lead the project “*Boite a spam*” (“spambox”). The electronic mailbox was used to receive forwarded spam messages for the purpose of studying the problem. The messages were not treated as complaints, but simply as a source of information, allowing the CNIL to better understand the problem. Complaints to the CNIL can be currently sent by post.

The requirement to investigate every complaint which states a *prima facie* case of a legal violation is not an uncommon policy. Only six respondents answered that their enforcement agency had discretion to investigate a complaint or not, whereas twelve answered that every complaint, if it states a *prima facie* violation of law, must be investigated. This responsibility would be impossible to fulfil if an enforcement agency received millions of forwarded e-mails, each constituting a complaint. In Italy, the *Garante per la protezione dei dati personali* (data protection authority) distinguishes between reports from recipients of spam, and formal complaints that violate a data subject’s rights. Since May 2002, 1 754 formal complaints regarding spam have been lodged with the *Garante*. Formal complaints must be investigated, but the data subject is required to lodge his complaint by registered mail or by e-mail with an approved electronic signature.

Responses indicate that data protection authorities are more often required to investigate complaints than the other enforcement agencies, and sometimes require a more formal procedure, such as a written letter. Canada, for example, does not have a law specific to the regulation of spam, but spam may violate certain provisions of its Personal Information and Electronic Communications Law. Complaints to the Privacy Commissioner must be made in writing and include the e-mail which is the object of complaint. As in Italy, *formal* complaints must be investigated. On the other hand, the Canadian Competition Bureau is not obligated to investigate all complaints regarding spam-related fraud, and can therefore act in accordance with its enforcement priorities.

### *Handling complaints*

As mentioned above, enforcement agencies do not always have discretion whether to investigate complaints. Resources, however, are limited, therefore agencies use different approaches to handling complaints depending on the type of illegal activity at hand. Certain law enforcement agencies distinguish spammers they will pursue with their full powers from spammers for whom a warning letter is sufficient. It is usually not difficult to distinguish between professional spammers and legitimate businesses that have overlooked the law, since the latter do not attempt to conceal their true identity, nor do they typically send out huge volumes of e-mail.

The above-mentioned twofold approach to spammers, aims to foster compliance with the law, without having to carry out resource intensive administrative or court proceedings against parties who are simply unaware that they are not following the law. Australia indicated that the Australian Communications Authority (ACA) has sent 150 warning letters to businesses since the Spam Act was enacted in April 2004, but its policy is to reserve fines for professional spammers (typically those who send hundreds of thousands of e-mails marketing fraudulent goods and services) and businesses that repeatedly violate the Spam Act. France reported that the CNIL systematically sends a reminder letter to companies which are the subject of complaint if they are situated in France or in the European Union, with the purpose building awareness and educating citizens and businesses – in particular small businesses – explaining the requirements imposed by the law. A different approach has been undertaken by Austria, which has fined some 100 businesses, most of whom did not know they were breaking the law, and only sent out several hundred e-mails to a targeted market. This initial policy is meant to send a strong message to the public that spam is an abuse of electronic communications and will not be tolerated; however Austrian administrative law provides a mechanism for warning letters that the communications regulators may use in the future. These contrasting policies may indicate that engendering compliance requires different methods in different societies.

These different approaches are calibrated and applied taking into consideration the different kind of spam messages received by users every day. Different methods are adapted to different offenders. In particular, several small and medium-sized enterprises are not fully aware of the legal requirements to make use of personal data – such as e-mail addresses – or to send commercial messages. In this case an education-based approach is also required as a complementary measure. Education and outreach may help in preventing violations. For this reason national authorities, who are signatories of the London Action Plan, are developing several activities to improve their skills internally, increase interagency co-operation, and raise awareness among users and businesses of the problem of spam. During a joint LAP/ICPEN sweep on spam scams which took place in 2004, members took a snapshot of the spam problem in their jurisdictions. The spam identified as illegal will be investigated and followed up with enforcement action in partnership with the industry as appropriate over the following months.

#### *Powers to gather evidence*

As mentioned above, identifying the source of spam and gathering evidence to link a specific person to the act of sending spam are among the greatest challenges facing enforcement agencies. For this reason, enforcement agencies require the tools necessary to obtain sufficient evidence for investigations to proceed to the sanctioning phase of enforcement.

Respondents indicated 16 enforcement agencies may issue requests for voluntary provision of information such as business records containing information relevant to the investigation and witness statements. These informal methods of gathering evidence may be useful in collecting information about the identity of spammers from such third parties as ISPs and domain name registries, without alerting the spammer about an investigation. Spammers who unwittingly break the law may comply with such requests, but spammers engaged in fraudulent activity are unlikely to respond for fear of prosecution.

For this reason, enforcement agencies require compulsory means of obtaining information, *e.g.* via subpoena or a court-ordered warrant. Respondents provided information for about half of the enforcement agencies identified. On the basis of this information the majority of the agencies possess the power to compel production of documentary evidence and witness testimony, and to conduct on-site inspections at businesses. Enforcement agencies appear to be adequately empowered to collect the evidence necessary to prove wrong doing. For example, in the Netherlands, OPTA (*Onafhankelijke Post en Telecommunicatie Autoriteit*) (communications regulator) may issue a subpoena for information to which the recipient is

legally obliged to respond, by meeting the relatively easy legal standard that the order to produce information is reasonable in the context of an investigation.

In contrast, Switzerland, which is in a transition period as regards anti-spam legislation, does not currently provide the Data Protection Commissioner with compulsory power to obtain information. In Mexico, COFETEL (*Comisión Federal de Telecomunicaciones*) (communications regulator) does not have power to compel production of information from ISPs, unless their actions breach telecommunications laws and regulations. Profeco (*Procuraduría Federal del Consumidor*) (consumer protection authority), however can serve compulsory process to gather information for investigations relating to consumer fraud. Likewise in the United Kingdom, the Office of the Information Commissioner (data protection authority) may not compel third parties to provide information, but the Office of Fair Trade (consumer protection authority) may issue information request notices, which are enforceable by court order.

#### *Co-operation with other enforcement agencies at the national level*

The power to gather evidence is only a starting point in effective enforcement policy. Since, depending on the nature of the Spam in question, enforcement responsibilities are often split among several agencies, successful action against spammers may require referring complaints and sharing information between agencies both at the national level and with counterparts in other countries. If there seem to be restrictions on sharing information between enforcement agencies from the same country, co-ordinating effectively among several agencies is a challenge that a number of countries have started to address. (Note: Restrictions that apply to sharing information with foreign counterparts are addressed in the section on cross-border enforcement co-operation).

The questionnaire specifically asked whether each country has any protocols or arrangements in place to refer complaints about spam or share information between agencies. Only five respondents indicated that protocols at the national level are in place or in development for these purposes. Twelve respondents indicated that informal intra-agency co-operation effectively occurs without any agreed-upon protocol. This is the case for example of Austria or Belgium, where co-operation among different authorities is informal. Referring complaints outside the scope of their jurisdiction to other enforcement agencies poses no particular difficulty. In many countries referrals are made as the result of an administrative legal requirement, regardless of whether the complaint pertains to spam or any other matter.

Australia has addressed the challenges that might otherwise result from the lack of a single enforcement agency by seconding personnel from the Australian Communications Authority to work in the Australian High Tech Crime Centre, which ensures effective communication between the two agencies. In addition, it has agreements with three agencies to co-operate on enforcement of the Spam Act, and regularly refers spam e-mails with offensive/illegal content to the appropriate authority. In Mexico, a bilateral agreement between COFETEL (the communications regulator) and Profeco (consumer protection authority) provides for joint assistance in cases involving deceptive and fraudulent advertisement practices, which may be applicable to cases involving spam. The OFT has led a national co-ordination strategy of national regulators with an interest in spam. The OFT had chaired two meetings where representatives from bodies such as the Information Commissioner's Office, Advertising Standards Authority, DTI, Office of Telecommunications, ICSTIS (Premium Rate Numbers Regulator), Local Authorities, Home Office and criminal authorities agreed a matrix mapping out respective responsibilities as well as a workable referral system.

The example of co-operation between enforcement agencies at the national level most frequently cited is between enforcement agencies which receive complaints and police or criminal prosecutors who process them. In Japan and Korea, co-operation with criminal prosecutors is the normal enforcement procedure if

spammers do not comply with administrative requests to cease their activity, as the enforcement agencies possess no sanctioning power of their own. In contrast, the *Forbrug* of Denmark and CNIL of France (consumer protection and data protection authorities respectively) may levy administrative fines against spammers, but have also transmitted spam cases to prosecutors to take action under criminal law; they also may appear as a witness in the criminal proceeding against the spammer. Complaints received by the Canadian Competition Bureau that appear to be fraudulent are referred, pursuant to informal understandings, to the police or organisations such as Phonebusters – a central (clearing house) agency that collects information on fraudulent marketing practices. The Competition Bureau has been transferring about 250 fraudulent spam-related complaints per month to Phonebusters. In the United States, the FTC has no criminal law enforcement authority, but it can refer cases to the criminal authorities when appropriate. When the FTC decides to pursue a CAN-SPAM case seeking only civil penalties (*i.e.* equitable remedies are not sought because no fraud is alleged), it refers the case to the Department of Justice (DOJ) for litigation.

Moreover, to facilitate effective enforcement and communication among agencies responsible for spam enforcement, the FTC has organised a spam task force comprised of 136 members representing 36 states, several units within the DOJ, and the FTC. The FTC has conducted two training sessions on investigative techniques for its task force and conducts monthly conference calls to share information on spam trends, technologies, investigative techniques, targets and cases. The benefits of these co-ordinated efforts in the United States are evidenced by over 60 civil law suits brought by enforcement agencies against spammers; far more than any other country. This also reflects the fact that much spam has its origin in the United States.

Notwithstanding the efforts to co-ordinate activities at least at the national level, it is still difficult to identify a single point of contact in each country. As mentioned, spam is a cross-cutting issue, and several aspects linked to spam activities can be already covered by existing instruments, such as anti-fraud or data protection laws. For this reason co-operation at the national level would be particularly important to avoid duplication of activities, and allow the optimization of resources and the exploitation of synergies between the different players. Often it is easier to pursue a spammer for fraud, or misuse of personal data, rather than for sending the spam message in itself. For example in France, the CNIL has a fundamental role in the process, providing the basic elements to the public prosecutor. The same is true in Belgium where the *Direction Générale du Contrôle et de la Médiation* carries out the necessary investigations and participates in the process as a witness. Co-ordination will allow the information gathered to be used more effectively while saving essential resources.

Several authorities agree that while informal co-operation is indeed a first step, more clearly established channels of communications would simplify the process, increase transparency and increase the efficiency of the system. Spammers are today organized internationally;<sup>2</sup> it would be unrealistic to expect to be able to face this phenomenon without a clear framework at national and international levels.

### ***B. Processes used to initiate enforcement action***

Once a complaint about spam has been filed with or, if necessary forwarded to, the appropriate enforcement agency, the next phase of enforcement is to initiate some action. This section of the report

---

2. For example, spammers are using offshore computer servers to host their Web site, therefore avoiding having them taken down in case of a pursuit. These services, also called “bullet-proof Web host services” are available on the Web. On the subject, see the “Law barring junk email allows a flood instead”, NYT, 01/02/2005, at <http://www.nytimes.com/2005/02/01/technology/01spam.html?ex=1108270800&en=fad6b058565b5287&ei=5070>.

provides information on the processes used to initiate enforcement proceedings or actions against spammers. The description of the processes used should be distinguished from the remedies or sanctions sought, which are treated in the next section. Respondents identified three general types of procedures that enforcement agencies may use:

- Administrative action.
- Civil proceedings, and
- Criminal proceedings.

A few respondents identified specialised courts or administrations through which action is processed, such as the Market Court in Sweden and Advertising Standards Authority in the United Kingdom.

Collectively, the responses indicated that 34 of the 62 enforcement agencies identified may initiate their own administrative procedure leading to a sanction against a spammer. Taking administrative action such as issuing warning letters, orders to comply with the law and fines are most frequently available to data protection authorities, followed by consumer protection authorities and communication regulators. Criminal courts are the second most frequently available forum in which enforcement agencies may initiate action against spammers: twelve consumer protection authorities, nine data protection authorities and four communication regulators may refer complaints directly to public prosecutors or transmit cases to them when the spammer fails to comply with an administrative order. Complaints are also referred directly to the public prosecutor when the content of spam is criminal (such as pornography or, in some cases, fraud). Finally, 13 enforcement agencies may bring proceedings against spammers in civil court: 9 consumer protection authorities, 3 data protection authorities and 1 communication regulator have this recourse available to them. In some countries, for example Austria, only private citizens can sue a spammer in a civil court, while in the United States Internet Service Providers can bring suits against spammers under the CAN-SPAM Act in addition to enforcement authorities (such as the FTC the DOJ).

There appears to be several advantages to acting through administrative procedures. An enforcement agency which acts on its own initiative does not have to rely on the discretion of a separate body to bring concrete action against spammers. In addition, proceeding through a criminal or civil court may be time consuming leaving consumers and users of electronic communications technologies open to fraud or misuse of personal data in the meantime. Further, criminal procedures may require a higher burden of proof, making it more difficult to obtain the remedy or sanction sought. However, the range of remedies and sanctions available to enforcement agencies are broader when they enlist the aid of courts. In certain countries, an injunction may only be available to the enforcement agency if granted by a judge, as well as civil redress, or sanctions implying imprisonment.

Negotiated settlements may provide an inexpensive and prompt alternative means of ensuring compliance compared to one of the three processes mentioned above. Nine respondents indicated that enforcement agencies in their country have initiated actions against spammers which resulted in a settlement before the necessity of a contested hearing. For example, the Australian Communications Authority (ACA) (communications regulator) provides the possibility to enter into an “enforceable undertaking” with a spammer. In Belgium, the *Direction Générale du contrôle et de la Médiation* can propose to the offender a transactional settlement, with the payment of a certain amount of money. Typically, such agreements require spammers to cease their activity and, if harm has been done, oblige restitution to consumers and/or the disgorgement of ill-gotten gains. If the spammer does not conform to the terms of the agreement, the ACA may apply to a federal court for it to make a finding of non-compliance, and the Belgian authority may similarly refer the case to the public prosecutor. Two countries, however, specified that a hearing in court is a fundamental procedural guarantee in every suit.

### *C. Sanctions and remedies*

Whereas the previous section outlined the processes by which enforcement agencies may take action against spammers, this section addresses the concrete remedies and sanctions with which they may discipline spammers. The tools available to enforcement agencies in the fight against spam range from the soft coercion of warning letters to the deprivation of liberty through imprisonment.

Responses to the questionnaire indicate the following non-monetary sanctions available to enforcement agencies: warning letters, injunctions, imprisonment through criminal process, revocation of business license, ban on Internet service, closure of the business premises, confiscation of material used to send spam and destruction of data files. The two most widely available non-monetary remedies are warning letters and injunctions. A clear contrast appears in this respect between the powers of data protection authorities and consumer protection agencies: 9 of the 18 data protection authorities identified in responses have the ability to warn spammers that their actions are illegal and request that they stop sending spam in violation of data protection laws; whereas 12 of the 19 consumer protection authorities identified are empowered to seek injunctions ordering the spammer to cease the illegal activity or face penalties for contempt where spam is the vehicle for fraud. Communications regulators are split almost evenly between these two non-monetary sanctions.

Table 4. **Non-monetary remedies and sanctions**

<b>Remedy/sanction</b>	<b>Data protection authority (18)</b>	<b>Consumer protection agencies (19)</b>	<b>Communication regulator (12)</b>
Warning letter	9	3	4
Injunction	2	12	3
Imprisonment (through criminal process)	9	8	2
Revocation of business license	4	-	3
Ban Internet access	2	1	1
Closure of business premises	1	1	1
Confiscate material	2	1	1
Destruction of data	3	-	-

Responses to the Questionnaire identified the following monetary remedies available to enforcement agencies: administrative fines, civil fines, criminal fines, consumer redress, disgorgement of ill-gotten gains and asset freezes. Fines are a monetary sanction the proceeds of which are typically kept by the government. Consumer redress aims to put the consumer back in the position he had been in prior to falling victim to fraud, thus unlike a fine, the money collected from the spammer is returned to the consumer. Disgorgement of ill-gotten gains results in identifiable proceeds from illegal activity being confiscated and sent to the treasury. An asset freeze is a preliminary measure, typically a court order, in which a third party such as a bank is ordered to sequester the assets of the spammer to prevent him from moving the assets to another jurisdiction where they may be unreachable. This protective enforcement tool, where permitted, improves the likelihood of enforcement agencies to collect on any money judgement that is ultimately issued. In order to be effective, however, the asset-freeze needs to be brought or enforced in the country in which assets are located.

Data protection authorities and communication regulators are empowered to seek monetary remedies against spammers primarily through administrative fines. Consumer protection agencies appear to be able

to seek fines also through civil courts and criminal courts almost nearly as often as through an administrative process. This might be explained as a matter of judicial economy, since many consumer protection agencies must already seek their non-monetary sanctions through civil courts. The power to seek consumer redress and disgorgement of ill-gotten gains are comparatively rare and asset freezes were only mentioned once.

Table 5. **Monetary remedies and sanctions**

<b>Remedy/sanction</b>	<b>Data protection authority</b>	<b>Consumer protection agencies</b>	<b>Communication regulator</b>
Administrative fine	10	11	8
Civil fine and/or damages	3	9	1
Criminal fine	5	9	3
Consumer redress	-	2	2
Disgorgement of ill-gotten gains	-	3	1
Asset freeze	-	1	-

#### **IV. Challenges to effective cross-border enforcement**

The aim of the following sections is to outline the prominent issues confronting enforcement agencies that wish to co-operate with foreign counterparts in taking action against spammers. The issues raised and examples cited of challenges facing enforcement agencies and the efforts to address these challenges are drawn from the responses to the Questionnaire and independent research. However, they are not intended as an exhaustive list of either the problems or the possible responses.

##### ***Restrictions on scope of enforcement authority***

When a spammer and message recipient are located in different countries, enforcement agencies are confronted with numerous challenges, both practical and legal, in their efforts to take action against the spammer. As stated above, anti-spam law is largely enforced by public authorities who base their powers on public law. In some cases, the laws invoked to combat spam are not applicable to messages which originate from a foreign source, which may impede enforcement agencies in the country where a message is received from even requesting a foreign counterpart to take action under its own law. The other side to this issue arises when the message in question is illegal where it was received, but not illegal where it was dispatched; a situation which makes it impossible for the foreign counterpart to bring an action under its own law. Finally, even where enforcement agencies are enabled by law to seek foreign assistance and their counterparts are willing to help, there may be conditions and/or restrictions to sharing and gathering information.

To assess the current legal capacity (as distinct from practical ability) of enforcement agencies to engage in cross-border actions against spammers, the Questionnaire asked whether the law applies to foreign spammers targeting domestic e-mail users. If the law applies to such cases, some enforcement agencies may take action against a domestic presence or activity related to the spammer (*e.g.* by confiscating inventory or prohibiting the transit of goods). Further, enforcement agencies may seek assistance from a foreign counterpart in the country where the spammer is located. Fifteen respondents answered that enforcement action could in theory be pursued against spammers regardless of where the

electronic message in question originated, as long as the message has a national link, such as being sent to an electronic address accessed in the national territory.<sup>3</sup>

Certain nuances in the responses should be taken into account. The Netherlands implemented Directive 2002/58 EC by amending its Telecommunications Act, and does not provide for taking enforcement action against foreign-source spam on that basis. However, sending unsolicited commercial e-mail might entail the automated processing of personal data, and potentially violate Dutch data protection laws. The situation is similar in other EU countries, where enforcement action could be pursued against foreign spammers as long as the spammer is situated outside the European Union, while spammers situated inside the European Union should be dealt with according to the domestic law in the message's country of origin. In Belgium, the Consumer Protection Authority can only take action against foreign-based spammers if they are situated outside the EU, while in Finland the Communications Regulator may not take action against foreign-based spammers, but the Consumer Protection and Data Protection Authorities are empowered to do so. Thus, even if the specific anti-spam law does not apply to foreign-source spam, there may be other legal grounds upon which to take action against the spammer or to seek the assistance of a foreign counterpart.

Thirteen respondents answered that enforcement actions either cannot be brought against foreign-based spammers or are not brought against them in practice, due to the difficulty of investigating in a foreign country and the problems linked to the execution of an eventual condemnation. In some countries the law expressly limits the application of its provisions to spamming activity based within the country's territory. In other countries, the resources required to identify and locate a spammer cannot be justified for the purpose of responding to a foreign complaint. Foreign-based spammers therefore might seem to risk no action being taken against them by the enforcement agencies in these countries. However, nearly every respondent to the Questionnaire answered that it is possible to notify foreign counterparts about spam emanating from within the counterpart's country.

Although spam is often accessed outside the country where it was dispatched, it is likely that addressees where the spammer is located have also received his or her spam, and that the local enforcement agency may take action based on evidence thereof. A legal obstacle to international co-operation may arise where the spammer is careful to send spam only to addressees located outside the country in which he/she is located. Six respondents (three Consumer Protection Agencies and three Telecommunications Regulators) indicated that they may not take action against spammers who target foreign email users, without some other national link. For these enforcement agencies sending spam from within their territory does not constitute a sufficient legal basis for taking action; spam must be received by an email user in their jurisdiction.

### ***Information gathering and sharing between enforcement agencies***

Enforcement agencies that wish to take action against spammers located in a foreign country are limited by the fact that they cannot exercise their full enforcement powers beyond national borders. However, enforcement agencies may be able to locate and identify spammers, and collect evidence against them, which might then be of use to foreign counterparts. Certain distinctions regarding information gathering and sharing should be made clear in the cross-border enforcement context. First, an enforcement agency may seek to gather information from individuals and businesses in its own jurisdiction, such as ISPs, through the exercise of compulsory process or voluntary co-operation. When investigations reveal that a spammer is located in a foreign jurisdiction, the enforcement agency may, as mentioned above, seek to enlist the aid of a foreign counterpart in the country where the spammer is located. However, the country

---

3. The Spam Act in Australia, for example, specifically foresees its applicability to all spam messages sent or received in the country or that have a link with the country.

requesting assistance may be restricted by its own domestic law with regard to the type of information it may share with the foreign counterpart that it has contacted. Second, the foreign counterpart may be limited in its power to take action and/or gather information in response to the request of a foreign agency without the spammer having already violated its own domestic law.

Only two respondents to the Questionnaire indicated that gathering and sharing information for and with a foreign enforcement agency are not permitted, yet in those countries where information sharing is possible the qualifications are numerous. Information provided in response to the Questionnaire was not specific enough to provide a cross country comparison of where information sharing and gathering is possible. As Table 6 indicates, most responses focused on the conditions and restrictions to sharing information with a foreign enforcement agency. Such a comparative matrix would be of great value to determine with specificity the existing gaps in the ability of enforcement agencies to gather and share information for and with foreign counterparts. However, a synthesis of the information contained in the responses to the Questionnaire does provide the Task Force with an overview of the types of conditions and restrictions that enforcement agencies face when seeking to share information in the context of cross-border co-operation.

The most frequent condition mentioned in answers to the Questionnaire was the need for information to be shared through some form of international arrangement. Among these responses six countries did not specify any existing international co-operation arrangement, implying that sharing information about spam cases is in theory possible, but that an international agreement of some sort is still required. Several respondents also distinguished information gathered informally from information obtained through the exercise of a compulsory process. The former could be shared with foreign enforcement agencies, subject to the condition of disclosure to and permission from the original source of information, whereas the latter could not be shared with foreign enforcement agencies.

Six responses, however, did specify existing arrangements for sharing information, especially between consumer protection agencies. In Europe, the Contact Network of Spam Authorities (CNSA) was mentioned by several respondents. The network has been created to improve information sharing and best practices among European authorities dealing with spam. Following this line, a “Co-operation procedure concerning the transmission of complaint information and intelligence relevant to the enforcement of article 13 of the privacy and electronic communication directive” was prepared.<sup>4</sup> The procedure has been agreed upon, so far, by 16 anti-spam enforcement authorities in 13 European countries. The nature of the agreement is such that more agencies can adhere to it over time. The agreement – originally developed by OPTA in co-operation with CNIL - establishes a common procedure to share information and handling cross-border complaints, so as to make it easier to identify and prosecute spammers anywhere in Europe.<sup>5</sup>

---

4. Council conclusions, available at <http://register.consilium.eu.int/pdf/en/04/st15/st15481-re01.en04.pdf>].

5 See the press release at:  
<http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/146&format=HTML&aged=0&language=EN&guiLanguage=en>.

Table 6. **Conditions for and restrictions on sharing information with foreign enforcement agencies**

Condition or restriction	No. of responses
Must take place through some form of international agreement	12
Must comply with privacy/data protection laws	5
Must be done in pursuance of the agency's own functions	4
The information must not be confidential	4
The information shared must not have been gathered pursuant to the agency's exercise of compulsory process	2
The agency sharing the information may request a promise of confidentiality from the agency receiving the information	1
If the requesting State wishes to know about complaints with regard to a particular spammer, the foreign authority sharing information must request the consent of the party who originally complained to it	1
Law of criminal procedure does not permit sharing information about a defendant once a criminal investigation is initiated	1

### *The enforceability of outcomes across borders*

No OECD member country has concluded a specific agreement providing for the recognition and enforceability of judgements obtained by foreign enforcement agencies against spammers. Nine respondents indicated that their country is signatory to a multilateral or bilateral agreement providing for the recognition and enforcement of judgements in civil and commercial matters which may apply in some cases to judgements against spammers. Where the civil court judgement creditor is a public enforcement agency, however, some foreign courts may consider these judgements to be penal or administrative in character, and thus not subject to the agreement. This reasoning could be used to exclude Europe's tri-part series of conventions on the recognition and enforcement of foreign judgements in civil and commercial matters: the Council Regulation (EC) No 44/2001<sup>6</sup> the 1988 Lugano Convention<sup>7</sup> and the 1968 Brussels Convention,<sup>8</sup> which apply to judgements on civil and commercial matters, therefore excluding administrative sanctions. If no particular agreement on jurisdiction and enforcement has been concluded between countries, national rules of private international law governing the recognition and enforcement of foreign judgements could apply; that is recognition and enforcement might be accorded as a matter of comity between nations on such conditions as, for example, judicial reciprocity and compliance with adequate rules of procedure.

The United States and Australia Free Trade Agreement contains a provision that addresses judgements obtained by the FTC, the Securities and Exchange Commission, the Commodities Futures Trading Commission, the Australian Competition and Consumer Commission, and the Australian Securities and Investment Commission. The Agreement provides that courts in the United States and

6. Council Regulation (EC) 44/2001 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters, 22 December 2000. Official Journal L 12 of 16.01.2001, available online at <http://europa.eu.int/scadplus/leg/en/lvb/l33054.htm>.

7. Convention on jurisdiction and the enforcement of judgements in civil and commercial matters, online at [http://www.curia.eu.int/common/recdoc/convention/en/c-textes/\\_lug-textes.htm](http://www.curia.eu.int/common/recdoc/convention/en/c-textes/_lug-textes.htm).

8. Convention on jurisdiction and the enforcement of judgements in civil and commercial matters, Brussels 1968, online at <http://www.curia.eu.int/common/recdoc/convention/en/c-textes/brux-idx.htm>.

Australia should not refuse to enforce monetary redress judgements obtained by these agencies in fraud cases simply because such judgements are penal in nature. This provision could apply to a judgement obtained in a spam case involving deceptive marketing or fraud. Although the provision does not require courts to enforce such judgements, it makes clear that enforcement of such judgements should be considered under private international law rules for enforcement of judgements.

The Hague Conference on Private International Law is preparing a Convention on Jurisdiction and Foreign Judgements<sup>9</sup> in which each ratifying country would agree to enforce each others judgements, regardless of where the actual cause of action takes place. According to Article 2(5) of the Convention's current draft, "Proceedings are not excluded from the scope of the Convention by the mere fact that a government, a governmental agency or any person acting for a State is a party thereto." The work on this convention, however, was put on hold when it became apparent that it would be difficult to obtain agreement. The text was therefore revised, and the current version of the preliminary draft Convention, officially known as the Draft on Exclusive Choice of Court Agreements,<sup>10</sup> applies in international cases to exclusive choice of court agreements concluded in civil or commercial matters. The Convention aims to secure an international legal regime that ensures the effectiveness of exclusive choice of court agreements by parties to commercial transactions giving effect to foreign judgements in civil and commercial matters following litigation pursuant to a choice of forum clause. It is therefore highly unlikely that cases brought against spammers by enforcement agencies would fit within its scope.

Notwithstanding the efforts made at the European level to harmonise legislations, enforcement in practice differs from country to country, and cross-border co-operation is still difficult due to legal and jurisdictional limitations. At the international level the situation is even more dramatic: although enforcement authorities are trying to work together, there is not a mechanism automatically operating when a case is opened against a spammer based in another country. Considering the rapidity of action of these subjects, the reaction must be immediate, and not the result of case-by-case agreements.

### ***Establishing priorities for international co-operation***

The Questionnaire asked respondents to identify the type of complaints that would take the highest priority or be most appropriate for cross-border enforcement co-operation. The purpose of this question was to discern whether there is any agreement across countries concerning which types of spam should be the focus of cross-border enforcement actions. Seven responses indicated that no priority was assigned to complaints about any specific type of spam; among these seven, five stated that all unsolicited commercial e-mail receives the same priority, and two stated that no priorities were in place. Twenty one respondents indicated at least one type of spam that would take priority for the purpose of cross-border enforcement. Table 7 lists the types of spam complaints which receive priority from enforcement agencies for cross-border enforcement.

Although respondents cited many possible grounds for granting priority to a spam complaint, the most commonly cited criteria are based on some type of damage that the message may cause, *e.g.* risk to the financial or health interests of consumers, user privacy and damage to networks and property. The type of spam most commonly identified as being an appropriate priority for cross-border co-operation is e-mail containing false or deceptive claims causing damage to the recipient. This data reveals a preference for protecting the interests of online consumers above those of ISPs, businesses, individual data subjects and other parties whose interests are damaged by spam. ISPs and businesses clearly suffer economic damage from spam through lost network capacity and worker productivity, but their welfare is not an object of

---

9 The text of the 1999 draft is available on the Web site of the Hague Conference on Private International Law at [http://www.hcch.net/upload/wop/jdgm\\_drafte.pdf](http://www.hcch.net/upload/wop/jdgm_drafte.pdf).

10 Latest draft (april 2004) online at [http://www.hcch.net/upload/wop/jdgm\\_wd110\\_e.pdf](http://www.hcch.net/upload/wop/jdgm_wd110_e.pdf).

public interest as such, *i.e.* a public institution cannot prioritise their complaints over those of a competitor without being accused of distorting free competition. The same reasoning cannot be invoked to explain why protection of data protection rights does not rank as high an enforcement priority as protection against fraud in cross-border cases.

Since responsibility for enforcing anti-spam law is most often divided among several types of enforcement agencies, one might expect different priorities for different types of agencies. However, of the 22 countries with multiple enforcement agencies only 4 respondents indicated that enforcement priority changes as a function of each agency's mission. This fact implies that even where responsibility is divided there is generally agreement at the national level regarding what type of spam should take priority for cross-border enforcement co-operation.

Table 7. **Types of spam complaints taking priority for cross-border enforcement**

	Consumer Protection Agencies	Data Protection Authorities	Telecommunications Regulators	Criminal Authorities
Criteria for priority				
Message contains false or deceptive claims (e.g. Phishing, scams, claims about health performance)	8	7	4	1
Message contains a virus	3	3	2	3
Unsolicited Commercial E-mail	3	1	-	-
Message contains offensive or criminal content (e.g. child pornography)	1	1	2	1
Degree of damage suffered (no specific example of damage provided)	1	1	-	-
Volume of messages sent	-	1	-	-
Repeat offender	-	-	1	-
Mobile phone spam	-	-	1	-
Message originates from outside EU	-	1	-	-

## V. Current efforts to address the challenges of information sharing and gathering

### *Multi-lateral or bilateral MoU specific to spam law enforcement*

Currently, four OECD member countries (Australia, Korea, the United Kingdom and the United States) have entered into various memorandums of understanding on spam to improve co-operation between enforcement agencies on cross-border cases. Australia (ACA and ACCC), the United States (FTC) and the United Kingdom (OFT and ICO) entered into a multilateral MoU on spam in July 2004, which provides that enforcement agencies responsible for anti-spam will co-operate in: detecting and investigating spam violations, tracking spammers, exchanging evidence and coordinating law enforcement against cross-border spam violators. In October 2003, Australia (ACA) and Korea (KISA) signed a

bilateral MoU on spam, which provides for the exchange of intelligence relating to spam originating in one or the other country and gathered as a result of a law enforcement investigation. The Australia/Korea MoU also provides for exchanging information concerning efforts to establish and enforce anti-spam regulatory frameworks and their effective use. Australia is also Party to a Joint Statement with Thailand on co-operation in the fields of telecommunications and information technology at a Ministerial level which involves, among other provisions, exchanging information about anti-spam policies and strategies.

The International Consumer Protection Enforcement Network (ICPEN) co-operates in combating cross-border Internet fraud through operating a multilingual Web site, [econsumer.gov](http://econsumer.gov), which provides information about consumer protection in its member countries, contact information about consumer protection agencies in those countries and an online complaint form to gather and share cross-border e-commerce complaints. In the first six months of 2004, 3 502 complaints were reported to [econsumer.gov](http://econsumer.gov), 54% of which pertained to offers communicated through e-mail. At a meeting in October 2004, the United Kingdom Office of Fair Trade and the United States Federal Trade Commission unveiled the London Action Plan on Spam (LAP); a non-binding agreement open to signature by enforcement agencies with responsibility for anti-spam laws, and certain private sector actors with an interest in combating spam.

In substance the London Action Plan provides that participating government and public agencies use their best efforts to develop better international spam enforcement co-operation by: designating a national point of contact for communication on spam cases with foreign enforcement agencies; encouraging national co-ordination among the different agencies that have spam enforcement responsibilities; prioritising cases based on harm to victims when requesting international assistance; encouraging and supporting the involvement of less developed countries in spam enforcement co-operation; taking part in periodic conference calls to discuss cases, legislative and law enforcement developments; exchanging effective investigative techniques and enforcement strategies. A Web site will be created to allow members to discuss and exchange information/best practices in a secure manner on line. Ongoing projects include the spam sweep as well as an educational project on zombie drone computers. The London Action Plan members include 27 agencies from 19 jurisdictions and 12 key industry signatories (including 5 ISP associations). Membership is varied both geographically as well as in terms of remit (CPA, DPAs, Telecommunication regulators).

### ***International agreements in related policy areas***

In June 2003 the OECD governments agreed on *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (2003). The scope of these Guidelines would cover spam when it is used as a vehicle for fraudulent and deceptive commercial practices. The framework created by the Guidelines addresses domestic systems and principles for international co-operation; notification, information sharing, investigative assistance, confidentiality, and jurisdiction to protect consumers; as well as section on monetary remedies and Private sector co-operation. The Guidelines are available at [www.oecd.org/sti/crossborderfraud](http://www.oecd.org/sti/crossborderfraud).

Denmark, Norway, Finland and Sweden have established a cross-border working relationship in the area of consumer protection through the Co-operation agreement between the Nordic consumer ombudsmen. The Agreement provides that Parties may conduct lawsuits on behalf of each other and exchange information about marketing practices across national borders (subject to national rules on secrecy and a request to treat the information in confidence). The agreement could apply to cases of deceptive or fraudulent activity conducted through spam that has been dispatched from the territory of a Contracting Party and received in that of another Contracting Party. The Agreement also includes provisions that require consultation with the businesses affected, the payment of expenses and translation.

In the area of criminal law, the Council of Europe Convention on Cybercrime, which entered into force on 1 July 2004, requires States that have ratified it to implement criminal legislation related to, *inter alia*, computer-related fraud and violations of network security. These provisions could be used to take action against spammers who use electronic messages as a tool to commit fraud (such as 419 scams) and/or spread viruses. The Convention acts as a catalyst to take action against spammers in countries where capacity is currently lacking, by reinforcing the investigative powers of competent authorities, and providing them the tools necessary to obtain evidence of wrongdoing (*e.g.* production orders, search and seizure of stored computer data, real time collection of traffic data and interception of content data) [Articles 18-21]. With regard to international co-operation, the Convention is of particular interest to the Task Force's consideration of cross-border enforcement as it provides guidelines for extradition [Article 24] and a detailed regime of mutual assistance in gathering and sharing information between the Parties [Articles 25-34]. To date eight countries have ratified the Convention, of which one, Hungary, is an OECD member country.

Recently, the European Union Council of Ministers approved Regulation EC NO 2006/2004<sup>11</sup> on Consumer Protection Co-operation. The aim of the Regulation is to link up national enforcement authorities and enable them to take co-ordinated action against rogue traders who abuse the freedom of the Internal Market in order to deceive consumers. It removes existing barriers to information exchange and co-operation and empowers enforcement authorities to seek and obtain action from counterparts in other Member States. The new EU-wide enforcement network will start work in 2006.

In the European Union, Directive 98/27 EC (the Injunctions Directive)<sup>12</sup> is an innovative effort to address the cross-border challenges of consumer protection enforcement. It specifically aims at addressing how to control traders that undertake activities in one Member State, which harm the collective interests of consumers in another Member State. The Injunctions Directive sets out a common procedure whereby an action for an injunction can be brought by a 'qualified entity' before a designated court or administrative authority for infringements of national provisions transposing the EU directives listed in its Annex. Where the subject matter of a commercial electronic message contains misleading terms for example, qualified entities (such as public enforcement agencies, consumer organisations or trade associations) may apply in the proper forum for a "stop now order". The objective of the Directive is to ensure that collective actions to protect consumers can be brought where the business is located and therefore where the remedy is most likely to be effective.

### ***Policy initiatives in other international organisations***

Several other international organisations such as the European Commission (EC), International Telecommunications Union and APEC have undertaken policy oriented projects dedicated to finding solutions to spam, including work related to law enforcement activities.

Within the EC, the Directorate General Information-Society (DGIS) has assembled a Contact Network of Spam Authorities to improve co-operation and discuss co-ordinated approaches to enforcement (see also *supra* page 21). The two enforcement agencies heading this group CNIL (France's data protection authority) and OPTA (the Netherlands' communications regulator) have circulated a questionnaire to other

---

11 OJ L 364, 11 p. Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation). Online at: [http://europa.eu.int/comm/consumers/prot\\_rules/admin\\_coop/index\\_en.htm](http://europa.eu.int/comm/consumers/prot_rules/admin_coop/index_en.htm).

12 Directive 98/27/EC of the European parliament and of the council of 19 May 1998 on injunctions for the protection of consumers' interests. Online at: [http://europa.eu.int/comm/consumers/policy/developments/acce\\_just/acce\\_just09\\_en.pdf](http://europa.eu.int/comm/consumers/policy/developments/acce_just/acce_just09_en.pdf).

enforcement agencies in the EC, asking how Article 13 of Directive 2002/58/EC has been implemented, whether it applies to natural or legal persons, who the relevant national authority is and what the available sanctions are for each country's national legislation. For its part, DGIS has researched the above questions and has also gathered information regarding: whether European enforcement agencies possess sufficient resources to investigate and enforce the laws implementing Directive 2002/58; the monitoring of dedicated e-mail boxes (spam boxes); co-operation between ministries and avoiding overlap and duplication between the various authorities with enforcement responsibilities; cross-border complaints and co-operation on enforcement inside the EU and co-operation with third countries.

The International Telecommunications Union (ITU) has conducted a series of activities on countering spam to foster the creation of harmonised policy frameworks, the promotion of international co-operation and to provide support to developing countries in the field of spam.<sup>13</sup> ITU co-operated with OECD to gather content for its database on anti-spam laws worldwide and to compile a list of the competent enforcement authorities and their contact details.<sup>14</sup> In addition, ITU has hosted virtual conferences in which representatives from enforcement agencies responsible for countering spam discussed the primary difficulties facing international co-operation and possible frameworks to address them. ITU maintains pages on its Web site which provide up-to-date information on non-confidential matters pertaining to spam policy, including international co-operation and law enforcement.

The Asia-Pacific Economic Co-operation (APEC) E-Commerce Steering Group<sup>15</sup> has undertaken to report on several issues related to law enforcement in its Work Program on Spam. First, it has set out to identify means available for cross-border co-operation to combat fraudulent and deceptive spam, further implementing the APEC Consumer Protection Guidelines. The work in this regard aims to develop points of contact, encourage information sharing between consumer protection and other law enforcement representatives, develop investigatory skills, and encourage appropriate complaint/case referrals between APEC economies. Second, the Work Program on Spam sets out to evaluate the effectiveness of measures to combat spam through use of quantifiable metrics.

### *Private sector assistance*

The private sector has been extremely active in bringing lawsuits against spammers and developing best practices and technical recommendations for Internet and e-mail service providers; especially the Anti-Spam Technical Alliance which brings together Yahoo, Earthlink, Microsoft and AOL. In addition, ISPs, domain name registries, cell phone operators, and industry associations have cultivated partnerships with law enforcement agencies in the fight against spam. The most common example of private sector assistance to enforcement agencies cited in responses to the Questionnaire was the provision of information to use as evidence of a spammer's illegal activity or to identify spammers. Another common form of private sector assistance is testimony at legal proceedings against spammers. Ten respondents indicated that private sector actors assist spam investigations by providing information voluntarily, *i.e.* in absence of a binding obligation to do so. Since Internet Service Providers and e-mail service providers are adversely affected by the volume of messages that spam creates for their networks to handle, assisting enforcement agencies with investigations is aligned to their own interests. Private sector actors have also assisted enforcement agencies by shutting down servers which are set up for the sole purpose of sending spam. As is the case for enforcement agencies which would share information with foreign counterparts, private sector actors also face conditions and limits to sharing information with enforcement agencies.

---

13 See ITU Web pages dedicated to countering spam initiatives, online at [www.itu.int/spam](http://www.itu.int/spam).

14 See Anti-spam Laws and Authorities Web page at <http://www.itu.int/osg/spu/spam/law.html>.

15 Asia-Pacific Economic Cooperation, Electronic Commerce Steering Group (APEC-ECSG), online at: [http://www.apecsec.org.sg/content/apec/apec\\_groups/som\\_special\\_task\\_groups/electronic\\_commerce.html](http://www.apecsec.org.sg/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html).

Private sector actors face limits on information sharing of both a practical and legal nature. For example, in Belgium ISPs claim that they cannot provide some of the information requested by enforcement agencies, because they do not maintain traffic logs for more than two weeks. Likewise, free email service providers claim that they do not have useful information, because they do not control the identity or geographical location of users. With regard to legal limitations on private sector information sharing, the limits and restrictions vary from country to country. Most respondents from the European Union indicated that data protection law restricts voluntarily sharing information regarding the identity of subscribers, and telecommunications law requires treating the content of electronic messages as secret; however these legal restrictions will not prevent a court order from taking effect or an enforcement agency from carrying out its powers of compulsory process. In Portugal, for example, the refusal of an ISP to provide information related to an official investigation could lead to a fine or imprisonment. In the United States, the Electronic Communications Privacy Act restricts the ability of ISPs to voluntarily disclose information contained in e-mails from their subscribers to enforcement agencies. By way of exception, ISPs may disclose information pursuant to a search warrant or court order, or with the consent of the subscriber. However, information sharing in response to civil subpoenas issued in connection with enforcement agency litigation is limited to subscriber information; email content is not available under such circumstances. On the other side of information sharing, nearly every respondent indicated that the employees of enforcement agencies owe a duty of confidentiality in regards to information received in connection with an investigation, whether the source be a private sector actor or not. This duty may restrict how information may be used and with whom it may be shared. In general, responses indicated that agencies may only share information such as trade secrets or personal information, obtained in connection with an investigation, in furtherance of carrying out their official functions.

Many enforcement agencies have set-up permanent or temporary spam boxes to which recipients of spam may forward messages for the purposes of collection, research, analysis and eventually taking action. Due to the sheer volume of spam forwarded to the spam boxes it is impractical to manually read and categorise each message. Consequently, the potential evidence contained therein has to a large extent not been utilised for the purpose of taking legal action. In Australia, the private sector developed a useful tool to confront this challenge for use by the Australian Communications Authority (ACA). The subscribers of Pacific Internet, an Australian ISP, may now use a plug-in developed by Spammatters to report any spam received to the ACA's forensic database with just one mouse click. The database reduces the need for manual spam investigations by automatically extracting information from the messages, including the header and message body, and allows them to be used as evidence in an Australian court.

In a teleconference organised within the context of co-operation under the London Action Plan, Microsoft's legal counsel provided valuable mentoring to representatives from participating enforcement agencies by explaining specific investigation techniques to identify spammers. Microsoft has successfully brought private lawsuits against spammers in North America and Europe that it identified by following information contained in email messages and tracing back possible links through the chain of services that a spammer needs to set up his operation: *e.g.* email service provider, domain name registrar, website hosting company, internet service provider, email list sellers, payment processors, etc. It is estimated that 80% of email spam is now sent by hijacked computers, therefore some of the sources named above are not helpful to identify the spammer as distinct from the technical source of the message.

In addition to providing assistance to investigations, the private sector has taken an active role in combating spam on several fronts not related to enforcement. Industry associations have been particularly active in consultations to prepare anti-spam legislation, and developing guidelines for self regulation on marketing practices which recommend that members not use spam. The Anti-Phishing Working Group is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account

usernames and passwords, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them. Finally, private organisations such as Spamsquad in Belgium and The Friendly Internet Forum in Hungary have been active in consumer education regarding how to protect against spam and how to complain to enforcement agencies.

Public/private partnerships in combating spam work in both directions, not only to the benefit of public enforcement agencies or the public interest. Respondents indicated examples of policies to provide the private sector with incentives to share information with enforcement agencies. In Australia ISPs and carriers that provide information pursuant to the ACA's exercise of compulsory process are not liable for damages which result from complying with the request for information. Enforcement agencies also provide direct assistance to private actors with their private suits against spammers. In France, the CNIL (data protection authority) has provided companies bringing private suits against spammers with complaints from users to bolster their case against the same spammer, and even testified in private legal proceedings. The personal information contained in messages that users had forwarded to the CNIL was deleted before being given to the private plaintiffs.

## **VI. Conclusions**

The results of the questionnaire show that while policy makers have identified spam as a critical and global issue that requires co-ordinated international action, significant steps are still required for national and cross-border enforcement to reach effectiveness. The following is an attempt to single out characteristics of the current situation that governments may want to consider when they further work together to facilitate anti-spam law enforcement across borders.

### ***Spamming remains a profitable activity***

Recent figures highlight that the overall volume of unsolicited commercial e-mail continues to remain significant. Moreover, spam is taking on new and more harmful forms, becoming the vehicle for the diffusion of fraud, *e.g.* phishing attacks, and viruses. The reasons for this situation may be diverse, but likely include challenges to national and cross-border enforcement of anti-spam laws, in a broad sense. Initiating more actions against spammers and obtaining higher fines and penalties for the most egregious violations will help render spamming less profitable. However, addressing the impediments to national and cross border enforcement of anti-spam laws is instrumental to achieving the broader goal of reducing spam.

### ***Growth of anti-spam enforcement activities***

Most OECD countries have been active in fighting spam, and policy makers recognise enforcement as a priority. The number of anti-spam laws has increased and enforcement agencies in a number of countries have initiated actions. Initiatives have already been undertaken to improve enforcement co-operation and involve different players. For example, an informal network of authorities, the London Action Plan, has been created, the European Union has created an enforcement protocol, and a number of countries have entered into MOUs. Through these efforts, information and best practices are already being exchanged. Enforcement efforts appear however fragmented, and further co-ordinated efforts are needed to combat a phenomenon which is increasing and taking more dangerous forms.

### ***Jurisdictional gaps in conjunction with diverse domestic frameworks are a problem***

There is not a single set of rules against spam but a patchwork including elements of consumer protection law, criminal law, data protection law, and telecommunication law. With respect to complaint handling mechanisms, only a small number of enforcement agencies permit spam to be forwarded

electronically or provide an online complaint form. Although the information provided through the e-mails sent to spam boxes usefully orientate the action of anti-spam authorities and help investigations against spammers, resources for creating and maintaining them may be insufficient. Current sanctions and remedies are not always sufficient to act as a disincentive to spammers domestically and internationally. Finally, the criteria for jurisdiction vary from country to country and enforcement agencies face limitations to hold spammers accountable for their illegal activities: for example when the spammer is physically located within their territory but the spam is sent abroad; or conversely when the damage is caused to individuals, businesses, or ISPs within their territory but the spammer is located abroad.

***National co-ordination should be first priority***

Multiple authorities have responsibility over investigation and/or enforcement of the various laws that can be violated by spammers and do not, in most cases, co-ordinate to fully exploit synergies, means and resources. Some countries already have a co-ordination mechanism in place. For example, in Australia four agencies have an agreement to cooperate on spam-related matters. The United States has a central contact point to facilitate communication among agencies responsible for spam at federal and state level. Other countries also need to further efforts to strengthen domestic inter-agency co-operation and to designate one agency as a contact point for foreign authorities would facilitate cross border co-operation.

***Cross-border enforcement against spam requires a global strategy to reach effectiveness***

If national co-ordination is a prerequisite for international co-operation, enforcement action across borders would still benefit from a global strategy to overcome a number of challenges to information gathering and sharing, to identify enforcement priorities, and to develop an effective international enforcement framework.

Adequate mechanisms for information gathering and sharing are needed for enforcement agencies to be able to investigate, preserve and obtain information and evidence and share that information with foreign counterparts in appropriate circumstances. It may be that cross border co-operation would have its greatest potential for success when authorities in the country of origin respond to the request of an authority in the recipient country because authorities in the country where a spammer is located are generally in a better position to identify the person behind an account from which spam was sent. If so, enforcement agencies in countries where spam is received should endeavour to locate the spammers and provide evidence enabling the authority in the country where the spam originates to exercise its powers, and, for example, compel production of information.

As no country can be expected to investigate and take action in response to every request from a foreign authority, it may be appropriate to establish priorities regarding what types of complaints are most appropriate for cross border co-operation. Despite the differing approaches to legislating against spam, and in particular the “opt-in” vs. “opt-out”, it appears that a considerable volume of spam would be illegal under most of the current legal frameworks. The real challenge is to move towards a common approach to prioritising which cases are worthy of the considerable effort required to bring actions in cross-border cases.

Finally, further consideration of how best to develop effective frameworks and arrangements for international co-operation would be important. The range of options is wide: further informal frameworks such as bilateral MOUs, multilateral or model MOUs, networks such as the London Action Plan, formal frameworks such as the OECD Guidelines on Cross-border Fraud, or binding legal instruments such as the Council of Europe Cybercrime Convention. While informal frameworks do indeed improve communication and working-level collaboration, a formal framework may be more appropriate in the future to create a common stable and effective mechanism at global level. Such a framework would not

need to be all inclusive, but could constitute the basis for further/enlarged arrangements among interested players, and be a platform for the various initiatives currently planned or developed.

***Global outreach should be the objective***

One of the major risks to effective enforcement of anti-spam laws is the ease with which spammers may set-up their operations and move to jurisdictions where there is no anti-spam law, where the enforcement capacity is weak and international co-operation is laden with conditions. Such jurisdictions may be the weakest link. To avoid the creation of spam havens, efforts to strengthen capacity to take action against spammers should reach out to the broadest possible coalition of enforcement agencies worldwide.

## ANNEX A

## OECD QUESTIONNAIRE ON CROSS-BORDER ENFORCEMENT OF ANTI-SPAM LAWS

Improving cross-border enforcement co-operation is a key element of the OECD work plan on spam [DSTI/CP/ICCP/SPAM(2004)1]. In particular, the work plan calls for conducting a survey on enforcement issues, building on the existing Survey of Spam Legislation in OECD Countries. This questionnaire is an important step in the process of understanding the current framework for enforcement of anti-spam laws in member countries and addressing the key challenges for more effective cross-border co-operation.

The OECD Survey of Spam Legislation, which was included in the background paper for the OECD Workshop on Spam, revealed a lack of uniformity in legal approaches to spam. Some countries have adopted specific anti-spam legislation to address the problem, while others use existing laws (*e.g.* consumer protection, data protection, and criminal law) to regulate activities that incidentally employ spam to accomplish unlawful purposes.

In countries where specific anti-spam legislation has been enacted, the general approach to enforcement has been to designate a public agency as primarily responsible for ensuring compliance with the law. On the other hand, in countries where several laws regulate activities that are carried out through spam, various agencies may be involved. In either case, different agencies may be in charge of receiving complaints from recipients of spam, investigating these complaints, and of either forwarding the dossier to a prosecutor or initiating proceedings.

The complex web of legal frameworks and agencies involved in the investigation and enforcement of spam related laws poses particular challenges for cross-border enforcement. The questionnaire below addresses this issue by requesting information that will help identify opportunities and limitations to effective cross-border enforcement. The purpose of the questionnaire is to:

- Identify aspects of domestic legal frameworks most relevant to international enforcement co-operation.
- Identify national contact points for anti-spam international co-operation.
- Elicit information concerning the powers and limits of enforcement agencies responsible for spam-related laws to investigate complaints and bring enforcement action, both domestically and across borders.

**Instructions**

In the questions below, the word “enforcement agency” refers both to public agencies or authorities and to publicly funded organisations that have an anti-spam enforcement role at the national level. An enforcement role could include any one of the following three functions: receiving complaints, conducting an investigation, or initiating proceedings in a court or tribunal. If there is more than one such agency, please answer separately on behalf of each. Respondents may provide additional information in an annex where they believe it will be helpful (*e.g.* providing information on the content of complaints). Although the focus of the questionnaire is on enforcement agencies, consultation with the private sector, or other non-governmental organisations that play a role in anti-spam enforcement, should be sought where appropriate.

The information contained in your responses will be analysed and form the basis of a report to be presented at OECD meetings in October. The answers themselves will not be made available to the public. A note will be sent to permanent delegations and delegates to the ICCP, CCP, WPISP and TISP when the questionnaire is posted to assist member countries in co-ordinating their responses to the questionnaire. We would appreciate responses by **20 August 2004**. Please send your responses to: [anne.carblanc@oecd.org](mailto:anne.carblanc@oecd.org) and [michael.donohue@oecd.org](mailto:michael.donohue@oecd.org).

**COUNTRY:**

**Section I: Description of national enforcement framework**

**A. Authority**

Do you have a specific anti-spam law in your country? (If yes, please provide the URL.)

If so, what enforcement agencies are responsible for its enforcement? (Please provide the URL.)

If not, which enforcement agencies have initiated proceedings against spammers under other laws, or have the power to do so? (*e.g.* enforcement agencies responsible for consumer protection, data protection or telecommunication laws).

Please indicate whether each enforcement agency listed in responses to Questions 2 and 3 possesses civil, criminal or administrative powers or some combination of these powers.

How do enforcement agencies receive complaints from spam recipients? (*e.g.* e-mail? online form? telephone?) Are enforcement agencies required to investigate every complaint they receive, and prosecute every case brought to their attention?

If more than one agency possesses enforcement powers, are there established protocols or arrangements for referring complaints between the agencies?

What are the primary investigative powers possessed by each enforcement agency? (*e.g.* can it request that evidence be provided voluntarily? issue compulsory process itself? request a court to obtain a warrant or issue a subpoena?)

How does each enforcement agency initiate proceedings against a spammer? (*e.g.* can it bring its own action directly in a civil or criminal court? initiate administrative proceedings? refer cases to a public prosecutor?)

**B. Sanctions, remedies and outcomes**

What legal remedies or sanctions are available to each enforcement agency? (*e.g.* injunctions or other conduct prohibitions? civil penalties? criminal fines? imprisonment? disgorgement of ill-gotten gains? monetary redress to spam recipients?)

How many spam-related proceedings have been initiated by each enforcement agency? (If possible, indicate the number of administrative, civil and penal cases.) Please provide any readily accessible information about the outcomes of the proceedings that have already been concluded.

Have any of these proceedings been settled without a hearing? If so, please indicate how many.

If the sanction or remedy that is obtained is not complied with by the spammer, what further steps are available to the enforcement agency?

**C. Private sector assistance**

How does the private sector provide assistance to enforcement agencies responsible for anti-spam laws? (*e.g.* assist in gathering evidence, testifying in court, providing affidavits?)

What legal or practical restrictions are there on the ability of ISPs and others in the private sector regarding the provision of evidence about spam to enforcement agencies? Are there laws or policies in place to act as incentives for the private sector to share information (*e.g.* providing indemnity to ISPs?)

Under what circumstances is information that the private sector shares with the enforcement agency treated as confidential? If there is any such confidential treatment, how is it affected by the kind of information or material that the private sector has shared?

## **Section II: Cross-border aspects of anti-spam law enforcement**

### **D. Cross-border challenges**

Can each enforcement agency take action against foreign spammers targeting domestic e-mail users? If yes, under what circumstances?

Can each enforcement agency take action against a domestic spammer that is targeting foreign e-mail users? If yes, under what circumstances?

Can each enforcement agency notify authorities in other countries about spam-related investigations that affect those countries?

Can each enforcement agency share information with, or otherwise provide investigation assistance to a foreign enforcement agency? If yes, under what circumstances? (*e.g.* does the e-mail have to be illegal in both countries as a condition to sharing information?)

What do you consider, or have you experienced, as being an obstacle to effective cross-border enforcement of laws related to spam?

### **E. Existing arrangements for international co-operation**

Does your country or its enforcement agencies have any bilateral or multilateral arrangements with other countries or agencies to co-operate in enforcing laws used against spammers? If so, please provide copies of any relevant arrangements. (*e.g.* laws, rules or policies)

Does your country have any arrangements in place that could facilitate the recognition and enforcement of judgements obtained in spam cases in foreign courts? If so, please provide copies of any relevant arrangements.

### **F. National contact point for anti-spam enforcement**

Is there an enforcement agency in your country that could be designated as a primary point of contact to facilitate anti-spam enforcement co-operation with foreign enforcement agencies? If so, please provide the agency's name and contact information.

### **G. Cross-border policy**

What kinds of spam complaints would take highest priority or be most appropriate for cross-border enforcement co-operation? (*e.g.* deceptive, fraudulent or virus carrying spam, or unsolicited commercial e-mail?)

Is there an agency primarily responsible for spam policy issues? Please provide the agency's name and contact information.

## ANNEX B

## OECD TABLE OF CASES

## I: CASES BROUGHT UNDER A SPECIFIC ANTI-SPAM LAW

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<b>Denmark</b>	Danish National Consumer Agency vs. Fonn Denmark <a href="http://www.siliconvalley.com/mlcd/siliconvalley/5762085.htm">www.siliconvalley.com/mlcd/siliconvalley/5762085.htm</a>	After receiving 50 complaints, the Consumer Protection Ombudsman brought suit against a Danish software company that had sent 156 unsolicited commercial e-mails.	Law on marketing practices	The Copenhagen Maritime and Commercial Court in Copenhagen fined Fonn DKK 13 000 (approx. USD 2 200)	Unknown	
<b>Japan</b>	MIC v. (not public) <a href="http://www.soumu.go.jp/oho_tsusin/eng/Relations/Telecommunications/news031113_1.htm">www.soumu.go.jp/oho_tsusin/eng/Relations/Telecommunications/news031113_1.htm</a> <a href="http://www.soumu.go.jp/s-news/2003/031113_2.htm">http://www.soumu.go.jp/s-news/2003/031113_2.htm</a>	MIC (Telecommunications Authority) issued an order of compliance against a company providing dating services based in Nakano-ku, Tokyo. The company had sent spam to mobile phones. The order requires the company to alert recipients that the electronic message is unsolicited and to provide sender's information.	Law on Regulation of Transmission of Specified Electronic Mail	Administrative order issued		None

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<b>Japan</b>	MIC v. SIS World <a href="http://www.soumu.go.jp/foho_tsusin/eng/Relations/Telecommunications/news040416_3.html">www.soumu.go.jp/foho_tsusin/eng/Relations/Telecommunications/news040416_3.html</a> <a href="http://www.soumu.go.jp/s-news/2004/040416_2.html">www.soumu.go.jp/s-news/2004/040416_2.html</a>	MIC issued an order of compliance against a company providing dating services based in Shinjuku-ku, Tokyo, which had sent mobile spam. The order requires the company to alert recipients that the electronic message is unsolicited and to provide sender's information.	Law on Regulation of Transmission of Specified Electronic Mail	Administrative order issued		None
<b>United States</b>	FTC vs. Creaghan <a href="http://www.ftc.gov/os/caselist/0423085/0423085.htm">www.ftc.gov/os/caselist/0423085/0423085.htm</a> FTC vs. Phoenix Avatar LLC <a href="http://www.ftc.gov/os/caselist/0423084/040429phoenixavatarmemo.pdf">www.ftc.gov/os/caselist/0423084/040429phoenixavatarmemo.pdf</a> <a href="http://www.usdoj.gov/opa/pr/2004/April/04_crim_281.htm">www.usdoj.gov/opa/pr/2004/April/04_crim_281.htm</a>	Federal Trade Commission received 40 000 consumer complaints about spam linked to the defendant and his Web sites that sell bogus anti-ageing products. Defendant operated the Web sites through aliases and foreign addresses, and disguised the source of the e-mails by forging return addresses in the "from" fields and sending them through open proxies. Consumers forwarded over 490 000 e-mails to the FTC regarding the defendant's fraudulent weight loss patches and penis enlargement pills. The e-mails used forged "from" addresses, and failed to provide clear and conspicuous opportunity to opt-out from receiving future messages or a valid physical address.	CAN-SPAM Act and Section 5, FTC Act CAN-SPAM Act	A federal judge issued a temporary restraining order prohibiting spamming, false product claims, and freezing the defendant's assets. The merits of the case have not yet been litigated. A federal judge initially issued a temporary restraining order prohibiting spamming, false product claims, and freezing the defendant's assets. Criminal charges are pending.	Defendant resides in Florida, and identifies his business as being located in Canada, Sweden and Switzerland. The products are sold on Web sites with domain names registered to individuals in China. Proceeds from sales are wired to Latvian bank. Unknown	Unknown The Department of Justice, which is bringing a separate criminal complaint against the defendants, ISPs and the US Postal Service provided investigation assistance by following the paper trail left in registering for Web sites through which the products were sold.

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<b>United States</b>	<p>FTC vs. Bryant and Bryant</p> <p><a href="http://www.ftc.gov/os/caselist/0423125/041005dbacmp.pdf">www.ftc.gov/os/caselist/0423125/041005dbacmp.pdf</a></p>	<p>Defendants sent deceptive spam by claiming in their message that recipients could make substantial income through business opportunity with a false "money back guarantee", which required stuffing envelopes at home. The defendants charged a \$25 registration fee and \$25 for a kit which did not contain letters to stuff, but two pages of instructions and a CD ROM which explained how to perpetuate the same scam. The e-mails contained spoofed header information, and false return information</p>	<p>CAN-SPAM Act, 5 FTC Act and 45(a) of the Telemarketing Sales Rule.</p>	<p>A federal judge issued an asset freeze and temporary restraining order prohibiting further sales and shipment of the products. Proceedings in civil court seeking a permanent injunction and consumer redress are pending.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>FTC vs. Global Web Productions</p> <p><a href="http://www.ftc.gov/os/caselist/0423086/040428globalwebmemosupporting.pdf">www.ftc.gov/os/caselist/0423086/040428globalwebmemosupporting.pdf</a></p>	<p>Consumers forwarded nearly 400 000 e-mails to the FTC regarding the defendant's fraudulent weight loss patch and anti-aging spray.</p>	<p>CAN-SPAM Act</p>	<p>A federal judge issued a temporary restraining order prohibiting further sales and shipment of the products.</p>	<p>The defendants reside in Australia and New Zealand, and Global Web is based in Australia. The Web sites through which sales are conducted routinely change registry between Japan, Malaysia, Hong Kong, China and Singapore.</p>	<p>The case was brought with the assistance of the Australian Competition and Consumer Commission and the New Zealand Commerce Commission.</p>

	<b>Case</b>	<b>Summary</b>	<b>Laws under which action was brought</b>	<b>Outcome / Status</b>	<b>Cross-border elements</b>	<b>Co-operation obtained</b>
<b>United States</b>	<p>United States of American vs. Nicholas Tombros  <a href="http://www.securityfocus.com/news/9606">www.securityfocus.com/news/9606</a></p>	<p>Defendant drove around a suburb with a laptop and a wi-fi antenna sniffing out unsecured residential access points, which he then used to send thousands of messages advertising pornography sites. Tombros was charged with a provision under the CANSPAM Act which prohibits breaking into someone else's computer to send spam.</p>	<p>CAN-SPAM Act</p>	<p>Defendant entered a plea agreement and will be sentenced in December 2004. A first-time violator faces up to one year in federal stir for a small-time operation-- three years if he or she meets one of several minimum standards of bad behaviour, like leading a spam gang of at least three people, sending over 2 500 messages in one day, or using 10 or more falsely-registered domain names.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>United States of American vs. Smathers and Dunaway  <a href="http://newpaper.asia1.com.sg/top/story/0,4136,66784-1096646340,00.htm">http://newpaper.asia1.com.sg/top/story/0,4136,66784-1096646340,00.htm</a></p>	<p>The Defendants are charged with conspiracy to steal data of 30 million AOL customers, and some 92 million e-mail addresses. Dunaway purchased the list e-mail addresses from Smathers, an AOL employee, and sold it for USD 52 000 to spammers. Dunaway later bought an updated version of the list for USD 100 000, and resold it again.</p>	<p>CAN-SPAM Act</p>	<p>The defendants each face a maximum sentence of five years in prison and a fine of USD250 000, or twice the gain or loss from the offence.</p>	<p>Unknown</p>	<p>Unknown</p>

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	<b>Case</b>	<b>Summary</b>	<b>Laws under which action was brought</b>	<b>Outcome / Status</b>	<b>Cross-border elements</b>	<b>Co-operation obtained</b>
<p align="center"><b>United States</b></p>	<p>United States vs. Chung, Sadek, Lin and Lin (Phoenix Avatar LLC) <a href="http://www.usdoj.gov/opa/pr/2004/April/04_cr_m_281.htm">www.usdoj.gov/opa/pr/2004/April/04_cr_m_281.htm</a></p>	<p>Four men were charged (two of whom were arrested) for sending hundreds of thousands of commercial electronic mail messages advertising diet patches and other devices, while using false and fraudulent headers to hide their identities. The defendants are allegedly responsible for sending hundreds of thousands of messages advertising medicine and other products. The complaint also alleges that the defendants were responsible for devising a scheme to defraud others by selling these medical devices via the U.S. Mail by means of false and fraudulent representations.</p>	<p>CAN-SPAM Act and Mail Fraud Statute</p>	<p>Pending. The CAN-SPAM Act carries a penalty of up to three or five years' imprisonment. Violations of the mail fraud statute carry a penalty of up to 20 years' imprisonment.</p>	<p>Unknown</p>	<p>The Federal Trade Commission, which is bringing a separate civil suit against the defendants, ISPs and the U.S. Postal Service provided investigation assistance by following the paper trail left in registering for Web sites through which the products were sold.</p>

## II: CASES BROUGHT UNDER GENERAL LAW

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<b>Australia</b>	ASIC vs. Hourmouzis <a href="http://www.internetnews.com/bus-news/article.php/499241">www.internetnews.com/bus-news/article.php/499241</a>	The Australian Securities and Investments Commission charged the defendant with interruption of the lawful use of file server computers, and making a statement that was false or misleading and likely to induce the purchase of securities. The defendant sent more than 4 million e-mails to discussion boards, claiming certain stock would rise to USD3 or more. Subsequently the price doubled on a trading volume that was more than 10 times the previous month's average, and the defendant sold his shares on the first trading day after the transmissions, making a profit of USD 17,000.	Securities regulations	Defendant pleaded guilty and was sentenced to two years' imprisonment. The U.S. Securities and Exchange Commission instituted its own proceedings against the man and obtained a judgement ordering that he disgorge ill-gotten profits of USD 15 000	The Australian resident sent e-mails to addresses in the United States, Australia and other parts of the world, after purchasing 65 000 shares in Rentech through a stock broking firm in Canada.	Unknown
	People vs. Marinellis <a href="http://www.news.com.au/comm/story_page/0,4057,7726290%255E15306,00.html">www.news.com.au/comm/story_page/0,4057,7726290%255E15306,00.html</a>	The defendant operated a "419" advance fee scam, sending e-mail with messages to convince people into believing they could claim millions of dollars through lottery winnings, an inheritance or a business opportunity if they first sent off money for "expenses". The defendant collected a total of USD 5 million from victims worldwide.	17 charges including five criminal counts of conspiring with others to cheat and defraud.	Pending	The defendant claims to be the Australian contact for an organisation with 220 operatives acting globally.	Unknown
<b>Canada</b>	Case name unknown <a href="http://p2pnet.net/story/1546">http://p2pnet.net/story/1546</a>	A juvenile suspected of hacking into thousands of computers was charged with mischief and fraudulent use of a computer by infecting computers with a "Trojan" virus that forces them to send thousands of e-mails at once with the aim to make the recipient system crash.	Criminal law	Pending	Unknown.	Unknown

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<b>China</b>	People vs. Jianquan and Wenqui <a href="http://lateline.news.com/ll/english/1311289.shtml">http://lateline.news.com/ll/english/1311289.shtml</a>	The defendants used phone text messages to swindle money from subscribers by telling them that they had won lottery prizes. The recipients were told they could claim their prize by sending lottery tax payments to designated bank accounts. More than 50 similar cases resulted in the conviction of 65 people last year.	Criminal law	A court in the province of Fujian sentenced one man to eight years imprisonment for obtaining USD 16,000. The second man was sentenced to four years for illegal earnings of USD 6,000.	Unknown.	Unknown
<b>France</b>	Prosecutor of the Republic (TGI du Mans) vs. L <a href="http://www.legalis.net/inet/decisions/diffamation/tqi_mans_071103.pdf">www.legalis.net/inet/decisions/diffamation/tqi_mans_071103.pdf</a>	A former employee of a pharmaceutical company spoofed the sender address in 700 000 unsolicited e-mails he sent to harass his former employer. The resulting saturation of the message inbox constituted a trespass upon the company's information system.	Criminal law [Penal Code 462-2 and 3].	The <i>Tribunal de Grande Instance</i> of Le Mans sentenced the defendant to a 10 month suspended jail sentence and two years probation.	Unknown	Unknown
	Prosecutor of the Republic (TGI de Paris) vs. M.R. G.V. <a href="http://www.juriscor.net/jpt/visu.php?ID=533">www.juriscor.net/jpt/visu.php?ID=533</a>	The defendant acquired a CD-ROM of 50 000 e-mail addresses and used them to send spam containing a link to a pornographic site. One recipient filed a complaint with the prosecutor.	Criminal law [Penal Code Article 226-16].	Defendant found guilty of automatic processing of personal information without prior notification to the proper authority (the CNIL), and ordered payment of a EUR 3 000 fine. However, the court acquitted the defendant of the charge that he had unlawfully collected personal information, citing the fact that mere possession of a CD-ROM containing personal data does not constitute collection.	Unknown	Unknown
	TGI (Draguignian) vs. Dinant No Web link available	A man was convicted of blocking the functioning of an automated information system, and the unfair collection of personal information by using a program designed to capture e-mail addresses from a service provider. The defendant disrupted the servers of Wanadoo by making 23 million individual attacks to copy e-mail addresses.	Penal Code 25-78-17, 226-18-1 and 226-31		Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
France	<p>CNIL vs. Alliance Bureaucratic Service</p> <p><a href="http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-075a.pdf">www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-075a.pdf</a></p>	<p>The CNIL received 650 notices from e-mail users referring to unsolicited commercial email that they had received from Alliance Bureaucratic Services. ABS is accused of having used "robot mail" to collect e-mail addresses of the recipients, a tool which it sells. Such tools are illegal under French data protection law. Further, some of the recipients complained that there was no opt-out option in the e-mails that they received. Finally, the company should have notified the CNIL in advance that it would use the e-mail addresses for the purpose of direct marketing.</p>	<p>Criminal law [Penal Code Article 226-16, 18].</p>	<p>Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to initiate criminal proceedings.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>CNIL vs. Suniles</p> <p><a href="http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-078a.pdf">www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-078a.pdf</a></p>	<p>The CNIL received 170 notices from e-mail users referring to unsolicited commercial e-mail that they had received from SUNILES. SUNILES is accused of having used "robot mail" to collect e-mail addresses of the recipients, and not providing an option to opt-out of receiving future emails. Further SINALES did not notify the CNIL in advance that it would send e-mail for the purpose of direct marketing</p>	<p>Criminal law [Penal Code Article 226-16, 18].</p>	<p>Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to initiate criminal proceedings</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>CNIL vs. (John Doe-company sending the emails "Le Top 50 du X")</p> <p><a href="http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-079a.pdf">www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-079a.pdf</a></p>	<p>The CNIL received 1 000 notices from e-mail users referring to unsolicited e-mails that they had received from an unidentifiable source promoting pornographic websites. The internet users claimed to have never had previous contact with the Web sites in question. The unidentified source is accused of having used "robot mail" to collect e-mail addresses of the recipients, and not providing an option to opt-out of receiving future e-mails. Further the company did not notify the CNIL in advance that it would send e-mail for the purpose of direct marketing.</p>	<p>Criminal law [Penal Code Article 226-16, 18].</p>	<p>Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to initiate criminal proceedings.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>CNIL vs. BV Communication</p> <p><a href="http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-076a.pdf">http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-076a.pdf</a></p>	<p>The CNIL received 260 notices from e-mail users referring to unsolicited commercial e-mails that they had received from BV Communications. The Internet users claimed to have never had previous contact with the company in question. BV Communication is accused of having used "robot mail" to collect e-mail addresses of the recipients, and not providing an option to opt-out of receiving future emails. Further the company did not notify the CNIL in advance that it would send e-mail for the purpose of direct marketing.</p>	<p>Criminal law [Penal Code Article 226-16, 18].</p>	<p>Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to file criminal charges.</p>	<p>Unknown</p>	<p>Unknown</p>

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<b>France</b>	CNIL vs. GreatMeds.com <a href="http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-077a.pdf">www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-077a.pdf</a>	The CNIL received around 500 notices from e-mail users referring to unsolicited commercial emails that they had received from GreatMeds.com. The emails received by users contained various text and links permitting recipients to navigate to the company's Web site through which it sells various medications on-line. The Internet users claimed to have never had previous contact with the company in question. GreatMeds.com is accused of having used "robot mail" to collect e-mail addresses of the recipients, and not providing an option to opt-out of receiving future e-mails.	Criminal law [Penal Code Article 226-18]:	Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to file criminal charges.	GreatMeds.com is apparently a company located in the United States	Unknown
<b>Italy</b>	Garante vs. unknown company <a href="http://www.legalday.co.uk/enxex/evershed03/November/e80281103.htm">www.legalday.co.uk/enxex/evershed03/November/e80281103.htm</a>	The Italian Data Protection Authority ( <i>Garante</i> ) reported to the Italian criminal court a graphic arts business, which continued to send spam even after the <i>Garante</i> issued a "data processing block". In addition the company failed to comply with an order requesting information regarding the origin of the personal data used in the spam, and the name of the person responsible for its processing treatment. Some recipients of the spam had complained to the <i>Garante</i> , claiming that the company had sent them advertising and promotional communications without having the necessary "informed" consent from them.	The new Data Protection Code enacted in June 2003 provides for criminal sanctions if personal data is processed without complying with the obligation to inform consumers and obtain their consent.	The representative of the company was fined EUR 15 000 Euro for failure to comply with the DPA request. Criminal proceedings are pending and could potentially lead to up to 3 years' imprisonment.	Unknown	Unknown
<b>Japan</b>	METI v. Access Control <a href="http://www.meti.go.jp/policy/consumer/release/remain.pdf">www.meti.go.jp/policy/consumer/release/remain.pdf</a>	The Ministry of Economy, Trade and Industry ordered Access Control to cease violations resulting from its failure to identify itself in unsolicited e-mail and not providing an email address for the purpose of opting out from future unsolicited email.	Specified Commercial Transactions Law	No further action taken. Continued violation would be referred to criminal authorities	None	None
<b>Korea</b>	Case name unknown <a href="http://times.hankooki.com/league/biz/200402/kt2004020919282811860.htm">times.hankooki.com/league/biz/200402/kt2004020919282811860.htm</a> <a href="#">III</a>	The Fair Trade Commission responded to 212 complaints of spam by ordering 25 spammers to correct their unlawful online advertising practices and issuing fines. The company receiving the heaviest fine arbitrarily sent spam even after consumers had opted-out. The FTC director general in charge of the consumer protection bureau announced that they were reviewing business suspension and heavier fines as possible future measures.	E-Commerce Consumer Protection Law	Fines ranged from KRW 1 to 7 million (USD 5,800), and two adult phone services were fined KRW 5 million each for sending SMS spam.	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<b>Netherlands</b>	Case name unknown <a href="http://www.dmeurope.com/default.asp?ArticleID=2428">www.dmeurope.com/default.asp?ArticleID=2428</a>	The Dutch Ministry of Justice brought charges of a "Nigerian 419 scam" e-mail fraud in response to a complaint filed by a Dutch cable operator and ISP.	Criminal	The Amsterdam district court acquitted six of the thirteen alleged e-mail scammers, due to lack of sufficient evidence; ruling that the discovery of the suspects at locations from where spam was being distributed was insufficient grounds for a conviction. The Dutch public prosecutor is appealing the decision. The prosecution had collected evidence at the time and place of arrest including: illegal Internet-connections, spamming software, mobile handsets, Nigerian scam letter-templates and even piles of names and addresses. However, the prosecution failed to prove convincingly that the suspects used the confiscated equipment to commit the alleged crimes at the locations in question.	Victims of the e-mail scam resided in Japan and the US. The defendants did not appear at the first trial and are thought to have fled the country, raising the question of the practical value of an appeal. The Dutch police confirmed ties between the defendants and drug smugglers in the Dutch Antilles.	Unknown
<b>Russia</b>	Case name unknown <a href="http://english.pravda.ru/main/18/90/361/13170_spam.html">http://english.pravda.ru/main/18/90/361/13170_spam.html</a>	Cell phone operator "Uralsky GSM" complained to the police that more than 15 000 cell phone owners were receiving unsolicited SMS. Upon investigation police confiscated the computer containing software for sending the SMS-messages, which the defendant had created himself. He was charged with creating software to perform denial of service attacks, and copying personal information.	Unknown	The defendant pleaded guilty, was put on probation for one year and required to pay fine of RUB 3 000 (USD 100).	Unknown	Unknown
<b>Switzerland</b>	Case name unknown <a href="http://www.edsb.ch/d/doku/empfehlungen/spam_neu.pdf">www.edsb.ch/d/doku/empfehlungen/spam_neu.pdf</a>	Upon complaints from recipients of unsolicited commercial e-mail, the Federal Data Protection Commissioner (SDPC) sent notice to a man sending spam to businesses and private individuals to provide information in his possession about the recipients and to delete it. The SDPC gave him 30 days to comply with the request, or the matter would be referred to a prosecutor	Art. 29-3 of the Federal Data Protection Act	Pending	Unknown	Unknown

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United Kingdom	Case name unknown <a href="http://software.silicon.com/secure/v0.39024655.39122143.00.htm">software.silicon.com/secure/v0.39024655.39122143.00.htm</a>	A man who had been fired for failing to complete his time-sheet retaliated by launching a denial of service attack against his former employer (UK insurers Domestic & General). The five-million mail attack brought down the corporate website and cost an estimated GBP 18 000 in lost business. The defendant admitted using a spam tool which he downloaded from the Internet.	Criminal	He faces six months in prison or a fine of up to £5,000.	Unknown	Scotland Yard's computer crime unit identified him and had him arrested.
	ICSTIS vs. BW Telecom <a href="http://www.icstis.org.uk/icstis2002/default.asp?node=74&amp;month=2">www.icstis.org.uk/icstis2002/default.asp?node=74&amp;month=2</a>	The Independent Committee for the Supervision of Standards of Telephone Information Services ("ICSTIS"), the industry-funded regulatory body for all premium rate charged telecommunications services, fined BW Telecom GBP 75 000 for sending unsolicited e-mails that indirectly promoted a premium rate adult Internet site to random e-mail addresses with no apparent attempt made to prevent them from being sent to children. The email contained peak-rate dialler software which disconnected users from their ISP before reconnecting them to a service that charged them GBP 1.50 a minute for Net access.	ICSTIS Code of Practice	ICSTIS barred access to service for a period of 12 months and instructed BW Telecom to offer redress to all 240 complainants	US company based in New York	Unknown
6 separate cases	ICSTIS vs. Vertical Media Ltd, Fast Way Holdings Ltd, Litmus Ltd, Indiano Communications, Greenbay Ltd and Quartel Ltd <a href="http://www.theregister.co.uk/2004/05/24/text_fine_icstis/">http://www.theregister.co.uk/2004/05/24/text_fine_icstis/</a>	Responding to thousands of complaints, ICSTIS- the premium rate watchdog, levied fines on six companies for sending text spam, making unsolicited phone calls and using automated calling equipment to leave "missed calls" on mobile phones, tempting punters to phone back on premium-rate phone numbers costing up to GBP 1.50 a minute. The regulator found that these companies deliberately tried to con people into calling premium-rate numbers to claim prizes that didn't exist or didn't match what was promised.	ICSTIS Code of Practice	Vertical Media Ltd, Fast Way Holdings Ltd, Litmus Ltd, Indiano Communications, Greenbay Ltd and Quartel Ltd were ordered to pay fines of GBP 75,000 each, and redress to those affected, and barred from operating in the UK.	The six companies are based overseas and had been operating through the same UK-based agent, Smile Telecom of Bury	The Department of Trade and Industry, communications regulator Ofcom and the police have also been called in to investigate the links between those involved
	ICSTIS vs. ACME Marketing <a href="http://www.icstis.org.uk/icstis2002/default.asp?node=74&amp;id=2">http://www.icstis.org.uk/icstis2002/default.asp?node=74&amp;id=2</a>	ICSTIS acted on complaints from the public about receiving SMS spam that informed recipients that they could claim either a holiday or GBP 5 000 and invited them to call a premium rate number to find out how. The text message failed to state call costs and company identity/contact details, while none of the recipients had consented to receiving it. Monitoring showed that callers could only actually claim the holiday and would be entered into a draw to win a GBP 5 000 prize	ICSTIS Code of Practice	ACME Marketing was fined GBP 3 000 and access to the service was barred for a period of six months. They were also instructed to offer redress to all complainants	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<b>United Kingdom</b>	Advertising Standards Authority vs. C Fry <a href="http://www.asa.org.uk/adjudications/show_adjudication.asp?adjudication_id=37209&amp;from_index=by_media&amp;date_s_of_adjudications_id=546">http://www.asa.org.uk/adjudications/show_adjudication.asp?adjudication_id=37209&amp;from_index=by_media&amp;date_s_of_adjudications_id=546</a>	ASA upheld several complaints concerning unsolicited commercial e-mails selling a prank CD-ROM and telephone call service. The e-mails contained misleading headers, were sent without the explicit consent of recipients, and claimed that they had been sent as opt-in promotions from partner companies.	Advertising Code	The ASA instructed the advertiser to ensure that in future promotional e-mails were sent only to consumers who had consented to receive them and that consumers who had given consent were given an opportunity to opt-out on each occasion. The sender claimed that he had not sent the messages, but the ASA noted that the e-mails appeared to have been sent either by or on behalf of the individual, and had ignored requests to show that recipients had consented to receiving the messages.	Unknown	Unknown
<b>United States</b>	FTC vs. Westby and Bevelander <a href="http://www.ftc.gov/opa/2003/09/fy0357.htm">http://www.ftc.gov/opa/2003/09/fy0357.htm</a>	The FTC alleged that the defendants sent e-mails containing false or misleading header information, spoofed e-mail addresses and provided opt-out links that didn't function.	Consumer Protection §5(a) of the FTC Act	Settlement bars the defendants from spoofing, using deceptive subject lines, false header information, or making false claims that they will remove consumers from e-mail lists. In addition, the defendants must give up USD 112 500 in ill-gotten gains made from the alleged illegal activities [USD 87 500 from Westby and USD 25 000 from Bevelander]. The settlement also contains record-keeping provisions to allow the FTC to monitor compliance.	The defendants, Westby and Bevelander, reside in Missouri and the Netherlands respectively. The businesses through which they operated, Maps Holding B.V. and PB Planning & Services B.V. have their principal places of business also in the Netherlands and are incorporated there.	Unknown.
	FTC vs. Zachary Keith Hill ; United States vs. Keith Hill <a href="http://www.ftc.gov/os/caselis/0323102/040322cmdp0323102.pdf">www.ftc.gov/os/caselis/0323102/040322cmdp0323102.pdf</a> <a href="http://www.ftc.gov/os/caselis/0323102/040322pleaagree0323102.pdf">www.ftc.gov/os/caselis/0323102/040322pleaagree0323102.pdf</a>	Defendant hijacked corporate logos and used deceptive spam to induce consumers into providing 473 credit card numbers and other personal financial information and then illegally purchased USD 47 000 in merchandise.	Consumer Protection: §5(a) of the FTC Act and Section 521 of the Gramm-Leach-Bliley (GLB) Act, Criminal: 18 US Code, 1029 (a)(5)	Defendant settled FTC charges that his scam violated federal laws, however he was later convicted in a separate criminal proceeding initiated by the US Department of Justice and sentenced to 46 months in prison.	Unknown	Assistance from the FBI Washington Field Office, and US Attorney for the Eastern District of Virginia's Computer Hacking and Intellectual Property Squad.

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<p><b>United States</b></p>	<p>FTC vs. a minor  <a href="http://www.ftc.gov/os/2004/06/040518stipaminorbyhisparents.pdf">www.ftc.gov/os/2004/06/040518stipaminorbyhisparents.pdf</a></p>	<p>The minor defendant copied corporate logos and deceptive spam to conduct a classic phishing attack, conning consumers out of credit card numbers and other financial data.</p>	<p>§5(a) of the FTC Act and Section 521 of the Gramm-Leach-Bliley (GLB) Act</p>	<p>Defendant settled FTC charges that his scam violated federal laws. If approved by the court, the defendant, a minor, will be barred for life from sending spam and would give up USD 3 500 in ill-gotten gains.</p>	<p>Unknown.</p>	<p>Assistance from the FBI Washington Field Office, and U.S. Attorney for the Eastern District of Virginia's Computer Hacking and Intellectual Property Squad.</p>
	<p>FTC vs. GM Funding  <a href="http://www.ftc.gov/os/caselist/doisweep/030505gmtundstip.pdf">http://www.ftc.gov/os/caselist/doisweep/030505gmtundstip.pdf</a>  <a href="http://www.ftc.gov/os/caselist/doisweep/030505universaltstip.pdf">http://www.ftc.gov/os/caselist/doisweep/030505universaltstip.pdf</a></p>	<p>Defendant conducted phishing attacks with forged e-mail headers. A phishing attack begins with an e-mail which claims to be from a service to which the recipient belongs and might make electronic payments to such as: a bank or online retailer. The e-mail claims that the recipient must update his personal information for this service to continue, by filling in an online form on a site which resembles the true Web site of the bank or retailer represented. The online form typically includes space for credit card numbers and identifying information such as social security numbers, date of birth account number and address. Once the information is sent, the defendant could use the information to transfer funds from victim's bank accounts, apply for credit cards in their names or purchase goods on-line.</p>	<p>§5(a) of the FTC Act and Section 521 of the Gramm-Leach-Bliley (GLB) Act</p>	<p>A settlement bans defendants from sending spam and requires them to give up \$60,500 in ill-gotten gains.</p>	<p>Unknown.</p>	<p>Co-ordination of efforts with other federal, state and local law enforcers.</p>
	<p>FTC vs. Patrick Cella et al  <a href="http://www.ftc.gov/os/caselist/doisweep/031119cellastipjudg.pdf">www.ftc.gov/os/caselist/doisweep/031119cellastipjudg.pdf</a>  <a href="http://www.ftc.gov/os/caselist/doisweep/031119hererazezulastip.pdf">www.ftc.gov/os/caselist/doisweep/031119hererazezulastip.pdf</a></p>	<p>The defendants used deceptive spam and Web sites to advertise that for a USD 50 advance payment, consumers would receive envelopes and pamphlets. They claimed that they would pay consumers USD 1 apiece for stuffing the envelopes and claimed that consumers could make USD 500 to USD 1 500 a week doing so. Some of the spam promised that consumers' payments were fully refundable. Instead of receiving envelopes and pamphlets, consumers received a booklet containing instructions on how to market the defendants' deceptive credit repair manual to other consumers. No consumers made the promised earnings, and consumers did not receive refunds.</p>	<p>§5(a) of the FTC Act</p>	<p>Settlements with the defendants permanently bar them from sending spam, from making deceptive representations, and from providing others with the means and instrumentalities to commit deception. Defendants will provide USD 7 000 for consumer redress. If the financial representations are found to be inaccurate, USD 536 412, the total of their ill-gotten gains, will be due.</p>	<p>Unknown.</p>	<p>Unknown</p>

<p>United States</p>	<p>FTC vs. K4 Global Publishing <a href="http://www.ftc.gov/os/caselist/doisweep/031014k4globalstfp.pdf">http://www.ftc.gov/os/caselist/doisweep/031014k4globalstfp.pdf</a></p>	<p>Defendants sent spam with a subject line of "Instant Internet Empires" touting the money-making potential of five pre-packaged Internet businesses. For their USD 47 77 investment, consumers received the right to reproduce the defendants' Web site and the right to try to resell its contents to other consumers. The FTC alleged that to achieve the promised earnings, consumers each would have to sell the product to 2, 00 additional consumers, who would each need to sell to 2 400 additional consumers to achieve the same earnings, and so on. According to the FTC, by the third generation of the scheme, participants would need to make a total of 13 829 760 000 sales, more than twice the earth's population, for each of them to achieve the advertised earnings.</p>	<p>§5(a) of the FTC Act</p>	<p>A stipulated final judgement and order bars making false or misleading income claims, from participating in chain marketing schemes, and from providing others with the means and instrumentalities to violate federal laws. Based on financial statements provided by the defendants, USD 247 000 will be provided for consumer redress. Should the financial representations be found to be inaccurate, the total of their ill-gotten gains, USD 634 222, will become due.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>FTC vs. Christopher Baith, Monarrez and Verma <a href="http://www.ftc.gov/os/caselist/0223291/040211baithcmp0223291.pdf">www.ftc.gov/os/caselist/0223291/040211baithcmp0223291.pdf</a></p>	<p>Defendants sent spam promising a free Sony Playstation to lure consumers to pornographic Web sites, then redirected consumers' internet connections through a 900-number with a significant per minute charge.</p>	<p>§5(a) of the FTC Act</p>	<p>A settlement resulted in a permanent injunction barring the defendants from sending any e-mail that misrepresents the identity of the sender or the subject of the e-mail, and a USD 10 000 fine, and USD 25 000 in ill-gotten gains.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>FTC vs. BTV industries <a href="http://www.ftc.gov/os/2002/04/btvcmp.pdf">www.ftc.gov/os/2002/04/btvcmp.pdf</a></p>	<p>Defendants sent spam promising free gifts to consumers, who were redirected to telephone pay services when they made downloads required to claim their prize.</p>	<p>§5(a) of the FTC Act</p>	<p>A settlement resulted in a permanent injunction barring the defendants from sending any e-mail that misrepresents the identity of the sender or the subject of the e-mail, and a USD 10 000 fine, and USD 25 000 in ill-gotten gains.</p>	<p>FTC worked with UK and Canary Islands</p>	<p>Unknown</p>
	<p>FTC vs. Benoit <a href="http://www.ftc.gov/opa/1999/05/audiot10.htm">www.ftc.gov/opa/1999/05/audiot10.htm</a></p>	<p>Scammers duped consumers into making costly international telephone calls in an attempt to ward off bills for merchandise they never ordered. The defendants contacted the consumers using bulk e-mail with a variety of forged addresses which prevented consumers from refusing the orders by e-mail. When consumers called the number to cancel orders for merchandise that they had never made they were automatically connected to a pay adult phone service</p>	<p>§5(a) of the FTC Act</p>	<p>US telephone carriers would ordinarily bill consumers for their pay-per-call charges and forward the funds to the Dominica telephone company which in turn distributes portions of the revenue to the providers of the audiotext service. Due to time lags between billing, collection and remission payments, it would typically take about 60 days for the funds to reach the audiotext business. The court order will prevent the telephone carriers from remitting the funds now in the revenue stream and preserve the money for consumer redress.</p>	<p>Consumers injured by placing calls to West Indies.</p>	<p>Unknown</p>

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. TLD Network Ltd. et. al. <a href="http://www.ftc.gov/opa/2003/11/fv0365.htm">www.ftc.gov/opa/2003/11/fv0365.htm</a>	Defendants used to spam to market the sale of non-existent domain names.	§5(a) of the FTC Act, 108(c) of the TILA, and 505(a)(7) and 522(a) of the GLB Act	Unknown	Unknown	FTC work with UK Office of Fair Trading
	FTC vs. 30 minute mortgage et al <a href="http://www.ftc.gov/os/2003/03/30mincmp.pdf">www.ftc.gov/os/2003/03/30mincmp.pdf</a>	Defendants sent fraudulent spam advertising "3.95% 30 Year Mortgages" and described itself as a "national mortgage lender." The company urged potential customers to complete detailed online loan applications that included social security numbers, income, and assets, and assured them that transmission of the sensitive information would be protected using Secure Sockets Layer (SSL) technology	§5(a) of the FTC Act, 108(c) of the TILA, and 505(a)(7) and 522(a) of the GLB Act	Agreed-upon settlement bars the illegal practices permanently and orders the defendants to give up their ill-gotten gains. The judgements require posting USD 1 million bonds before sending unsolicited commercial e-mail. A USD 57 500 judgement against the company President has been suspended.	Unknown	Unknown
6 separate but related cases	FTC vs. Larsen, Va, Lutheran, Panchoero, Estenson and Boivin <a href="http://www.ftc.gov/opa/2002/02/leileenspam1.htm">www.ftc.gov/opa/2002/02/leileenspam1.htm</a>	Six defendants were charged with sending spam to consumers containing deceptive chain letters. The letters promised "USD 46 000 or more in the next 90 days," to recipients who were to send USD 500 in cash to each of four participants at the top of the list. In return for a \$5.00 payment, recruits received "reports" providing instructions about how to start their own chain letter schemes and recruit tens of thousands of others via spam.	Unknown	The stipulated final judgements and orders for permanent injunction bar all the defendants from promoting, marketing, advertising, offering for sale, selling, or assisting others in any chain marketing scheme.	The investigation found more than 2,000 participants in the chain letter from almost 60 countries around the world.	The addresses were culled from the FTC's unsolicited commercial e-mail (UCE) database
	FTC vs. Chase Financial Funding <a href="http://www.ftc.gov/os/caselis/t/0223287/040602com0223287.pdf">www.ftc.gov/os/caselis/t/0223287/040602com0223287.pdf</a>	The defendants have sent spam with false and deceptive content promoting "FIXED PAYMENT" loans with rates such as 3.5 percent and 2.95 percent.	§5(a) of the FTC Act;	Court was asked to bar the defendants permanently from engaging in deceptive lending practices, and to award relief, including consumer redress and disgorgement of the defendants' ill-gotten gains.	Unknown	Unknown
	FTC vs. Clickformail.com <a href="http://www.ftc.gov/os/2003/10/clickformailfinalord.pdf">www.ftc.gov/os/2003/10/clickformailfinalord.pdf</a>	The defendants sent spam e-mail telling consumers they were approved and guaranteed to receive major, unsecured credit cards with credit limits up to USD 5 000 for an advance fee of USD 49.95. However, consumers who paid the fee did not receive the promised card. Instead, they allegedly received access to a set of hyperlinks to companies where consumers could apply for credit cards.	§5(a) of the FTC Act	Defendants agreed to a settlement in which they are to pay USD 815 000 in consumer redress. In addition to paying redress, the settlement prohibits the defendants from making any false claims to consumers in the future.	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<p><b>United States</b></p>	<p>FTC vs. Universal Direct et al <a href="http://www.ftc.gov/os/2002/04/universaldirectcmp.pdf">www.ftc.gov/os/2002/04/universaldirectcmp.pdf</a></p>	<p>Defendants used deceptive spam and a Web site to recruit consumers into an illegal chain letter, by sending spam that promoted "a multi-level marketing "Gifting Program ". The spam claimed that participants could earn USD 10 000 in cash gifts within a few months of joining and urged consumers to recruit other participants.</p>	<p>§5(a) of the FTC Act</p>	<p>The settlement bars the defendants from promoting or selling pyramid or chain mail schemes, misrepresenting potential earnings claims, misrepresenting the legality of such schemes, failing to disclose the profits or earnings of other participants in any multilevel marketing programme, and providing others with the means to make misrepresentations. Following the preliminary injunction, the defendants refunded all the money they had collected from investors in the scheme.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>FTC vs. Walker <a href="http://www.ftc.gov/os/2002/04/davidwalkercomp.pdf">www.ftc.gov/os/2002/04/davidwalkercomp.pdf</a></p>	<p>Defendant used an Internet site to market products he claims cure cancer. The site claimed that the treatments, which cost between USD 2, 00 and USD 5 200, make surgery, chemotherapy, and other conventional cancer treatments unnecessary. A declaration from a distinguished oncologist suggested the therapies are potentially harmful to cancer patients.</p>	<p>§5(a) of the FTC Act</p>	<p>Pending. The agency asked the court to bar the unsubstantiated claims permanently, and order consumer redress</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>FTC vs. Cyber Data <a href="http://www.ftc.gov/os/2002/10/scottford.pdf">www.ftc.gov/os/2002/10/scottford.pdf</a></p>	<p>Defendant sent spam to consumers claiming that by purchasing his bulk e-mail lists, they could make money selling products and services on the Internet. Cyber Data's e-mail claimed that purchasers reasonably could expect to earn "over USD 10 000,000" by selling a USD 5 product via bulk e-mail.</p>	<p>§5(a) of the FTC Act</p>	<p>Defendant agreed to a settlement permanently barring any false, misleading, or deceptive claims about potential earnings from any bulk e-mail list, software, service, or marketing programme, or any other business opportunity. Based on financial documents that the defendant provided, the settlement requires Cyber Data to pay USD 20 000 in consumer redress.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>U.S. vs. Internet Specialists <a href="http://www.usdoj.gov/usao/da/News/PI/2003/oct/carlson.pdf">www.usdoj.gov/usao/da/News/PI/2003/oct/carlson.pdf</a></p>	<p>A disgruntled baseball fan hacked into computers and from those computers launched spam e-mail attacks with long messages voicing his complaints about his favorite team's management. When launching the spam e-mails, many of the addresses on the long list were no longer current. When those e-mails arrived at their destinations, the indictment charges that they were "returned" or "bounced" back to the person who purportedly sent them – the persons whose e-mail addresses had been "spoofed" or hijacked. This caused floods of thousands of e-mails into these accounts in a very short period of time, disrupting their service.</p>	<p>§18 USC 1028, 1030</p>	<p>Unknown</p>	<p>Defendant gained control of a computer in Canada to make the denial of service attacks</p>	<p>Unknown</p>

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
<p align="center"><b>United States</b></p>	<p>SEC vs. Scott Flynn <a href="http://www.sec.gov/litigation/admin/34-41102.txt">www.sec.gov/litigation/admin/34-41102.txt</a></p>	<p>In a typical touting fraud, the defendant Flynn, a former stockbroker convicted of securities fraud in another matter, used spam to spread information about certain companies, without properly disclosing the receipt of compensation from those companies. The SEC alleged that unbeknownst to investors, Mr. Flynn spread information through his company, Strategic Network Development, Inc., without disclosing cumulative compensation of at least USD 183 200 in cash and 322 500 shares of stock from at least ten of the companies.</p>	<p>SEC Act of 1934</p>	<p>The SEC instituted cease and desist proceedings against the defendant for violations of the anti-touting provisions of the federal securities laws. Outcome pending.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>SEC vs. Smith <a href="http://www.sec.gov/litigation/litleases/lr18130.htm">www.sec.gov/litigation/litleases/lr18130.htm</a> <a href="http://www.sec.gov/litigation/litleases/lr18130.htm">www.sec.gov/litigation/litleases/lr18130.htm</a></p>	<p>Defendant admitted to conducting two fraudulent investment schemes through Web sites and spam e-mail during 2002. The SEC charged him with fraudulently raising USD 102 554 by falsely guaranteeing double-digit monthly returns on two Web sites and in approximately 9 million spam e-mail messages.</p>	<p>SEC Act of 1934, Rule 10-b(5)</p>	<p>Defendant consented to an order requiring him to pay \$107,510 in disgorgement and pre-judgement interest and enjoining him from further violating the Securities laws.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>SEC vs. 2DoTrade <a href="http://www.sec.gov/litigation/litleases/lr18381.htm">www.sec.gov/litigation/litleases/lr18381.htm</a></p>	<p>The defendants engaged in a fraudulent scheme in which they artificially pumped 2DoTrade's stock with false press releases in spam e-mail linked to a fraudulent Web site and then illegally dumped millions of shares into the inflated market.</p>	<p>Sections 5(a), 5(c), and 17(a) of the Securities Act of 1933 and sections 10(b) and 13(a) of the Securities Exchange Act of 1934.</p>	<p>Pending. The SEC seeks permanent injunctions, disgorgement of ill-gotten gains with pre-judgement interest, and civil money penalties against all the defendants.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>SEC vs. Garst <a href="http://www.sec.gov/litigation/litleases/lr18381.htm">www.sec.gov/litigation/litleases/lr18381.htm</a></p>	<p>Defendant allegedly sent a large number of unsolicited spam e-mail messages containing false and misleading statements concerning the product, revenue sources and business relationships of one of the touted issuers, as well as her stock-picking track record and the trading intentions of the persons responsible for the e-mail messages. Finally, the spam did not disclose cash compensation paid to her by the statutory underwriter.</p>	<p>Sections 10(b)5 of the Securities Exchange Act of 1934 and, and violated Section 17(b) of the Securities Act of 1933</p>	<p>Pending. The SEC seeks disgorgement of payments plus reasonable interest.</p>	<p>Unknown</p>	<p>Unknown</p>
	<p>SEC vs. Rice <a href="http://www.sec.gov/litigation/litleases/lr17377.htm">www.sec.gov/litigation/litleases/lr17377.htm</a></p>	<p>Defendant allegedly carried out "pump and dump" schemes to manipulate the stock of four companies, including his own. The schemes for all four companies involved issuing unsolicited fraudulent e-mail messages. The false statements concerned, among other things, his company's product (purportedly an advanced Internet search engine), its revenue sources and business relationships with third parties, as well as his stock-picking track record and trading intentions.</p>	<p>Sections 10(b) of the Securities Exchange Act of 1934 and Section 17(b) of the Securities Act of 1933</p>	<p>Defendant consented to an order enjoining future violations of Securities laws and directing him to pay disgorgement and pre-judgement interest.</p>	<p>Unknown</p>	<p>Unknown</p>

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	<p>FTC vs. Kalvin P. Schmidt  <a href="http://www.ftc.gov/opa/1998/07/meganet.htm">www.ftc.gov/opa/1998/07/meganet.htm</a></p>	<p>Defendant sent spam e-mail to consumers directing them to Web sites, which promoted a chain letter based pyramid investment scheme. The scheme was based on false and unsubstantiated earnings claims.</p>	<p>\$5(a) FTC Act</p>	<p>The FTC settlement bans Schmidt from participating in any chain letter schemes or pyramid sales schemes, and requires him to have a basis for any earnings claims. Schmidt would need evidence to substantiate any representation about the income, profits, or sales of any marketing plan or programme or any material fact. Finally, the settlement contains various recordkeeping requirements.</p>	Unknown	Unknown
United States	<p>FTC vs. Dixie Cooley, d/b/a DWC  <a href="http://www.ftc.gov/opa/1998/10/operaset1-3.htm">www.ftc.gov/opa/1998/10/operaset1-3.htm</a></p>	<p>Defendant used e-mail to scam consumers into believing that he could restore their creditworthiness for a fee. Sometimes charging more than USD 1 000, defendant purported to guarantee consumers they could remove negative information from their credit reports -- even if the negative information was accurate and timely. But, these companies cannot remove legitimate negative information and, where there are actual errors in credit reports, consumers have the legal right to have those corrected for free most of the time.</p>	<p>FTC Act and the Credit Repair Organizations Act (CROA)</p>	<p>Defendant ordered to pay USD 15 451.75 in consumer redress.</p>	Unknown	Unknown
	<p>FTC vs. Epic Resorts, LLC  <a href="http://www.ftc.gov/opa/2000/08/traveluntravel.htm">www.ftc.gov/opa/2000/08/traveluntravel.htm</a></p>	<p>Defendants allegedly marketed travel packages through spam that misled consumers by failing to disclose the actual cost, or concealing that they had to attend one -- and possibly more - timeshare presentations.</p>		<p>The FTC sought redress for consumers.</p>	Unknown	Unknown
	<p>FTC vs. Associated Record Distributors, Inc  <a href="http://www.ftc.gov/opa/2002/06/bizopswe.htm">www.ftc.gov/opa/2002/06/bizopswe.htm</a></p>	<p>Defendants sent spam e-mail promoting false work at home opportunities. The promotions exaggerated earnings potential and assistance that respondents would receive.</p>	<p>Franchise Rule</p>	<p>FTC sought consumer redress, civil penalties, and a permanent halt to the deceptive claims.</p>	Unknown	<p>Florida Police Department assisted the FTC in the case.</p>
	<p>FTC vs. NetSource One</p>	<p>No further information available.</p>				
	<p>United States vs. A. James Black  <a href="http://www.ftc.gov/opa/1999/02/consumerweek2.htm">www.ftc.gov/opa/1999/02/consumerweek2.htm</a></p>	<p>Defendants advertised fraudulent services through e-mail using claims such as "BRAND NEW CREDIT FILE IN 30 DAYS". The firms sold instructions to consumers how to substitute federally-issued, nine-digit employee identification numbers or taxpayer identification numbers for social security numbers, and use them illegally to build new credit profiles that would allow them to get credit they may be denied based on their real credit histories.</p>	<p>Credit Repair Organizations Act and the FTC Act</p>	<p>Unknown</p>	Unknown	<p>Department of Justice filed 3 cases and the FTC 14</p>

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
	<p>United States vs. David Story  <a href="http://www.ftc.gov/opa/1999/05/td21a4.htm">www.ftc.gov/opa/1999/05/td21a4.htm</a></p>	<p>Approximately same facts as above.</p>	<p>Credit Repair Organizations Act and the FTC Act</p>	<p>Unknown</p>	<p>Unknown</p>	<p>DOJ and US Postal Inspection Service.</p>
	<p>United States vs. PVI, Inc.  <a href="http://www.ftc.gov/opa/1998/09/vendup2.htm">www.ftc.gov/opa/1998/09/vendup2.htm</a></p>	<p>The defendant made oral and written earnings claims to potential investors about digital photo vending machines via spam e-mail, but failed to provide either a basic disclosure document or an earning claims document.</p>	<p>Franchise Rule</p>	<p>Unknown</p>	<p>Unknown</p>	<p>DOJ filed the case at the request of FTC.</p>
	<p>FTC vs. LS Enterprises  <a href="http://www.ftc.gov/opa/1999/04/spam2.htm">www.ftc.gov/opa/1999/04/spam2.htm</a></p>		<p>§5(a) FTC Act</p>		<p>Unknown</p>	<p>Unknown</p>
	<p>FTC vs. Tim Cho Investment Corporation and Timothy Cho  <a href="http://www.ftc.gov/opa/2001/03/cho.htm">www.ftc.gov/opa/2001/03/cho.htm</a></p>		<p>§5(a) FTC Act</p>		<p>Unknown</p>	<p>Unknown</p>
	<p>FTC vs. TrendMark International, Inc.  <a href="http://www.ftc.gov/opa/1998/06/trendmrk.htm">www.ftc.gov/opa/1998/06/trendmrk.htm</a></p>		<p>§5(a) FTC Act</p>		<p>Unknown</p>	<p>Unknown</p>
	<p>FTC vs. Ralph Lewis Mitchell, Jr.  <a href="http://www.ftc.gov/opa/1999/02/consumerweek2.htm">www.ftc.gov/opa/1999/02/consumerweek2.htm</a></p>					
	<p>FTC vs. Reverseauction.com, Inc.  <a href="http://www.ftc.gov/opa/2000/01/reverse4.htm">www.ftc.gov/opa/2000/01/reverse4.htm</a></p>					

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. Rosalind Leahy <a href="http://www.ftc.gov/opa/2002/11/netforce.htm">www.ftc.gov/opa/2002/11/netforce.htm</a>					
	FTC vs. Sandra L. Rennert, et al. <a href="http://www.ftc.gov/opa/2000/07/iog.htm">www.ftc.gov/opa/2000/07/iog.htm</a>					
	FTC vs. Scott d/b/a Cyber Data FTC vs. Seasilver USA, Inc. et al. <a href="http://www.ftc.gov/opa/2003/06/seasilver.htm">www.ftc.gov/opa/2003/06/seasilver.htm</a>	No further information available.				
	FTC vs. StuffingforCash.com Corp <a href="http://www.ftc.gov/opa/2002/07/mwneiforce.htm">www.ftc.gov/opa/2002/07/mwneiforce.htm</a>					
	FTC vs. West Coast Publications, LLC <a href="http://www.ftc.gov/opa/1999/9905/td21a4.htm">www.ftc.gov/opa/1999/9905/td21a4.htm</a>					
	FTC vs. Yad Abraham <a href="http://ftc.gov/os/2003/08/ipsettlementabrahamstip.pdf">ftc.gov/os/2003/08/ipsettlementabrahamstip.pdf</a>					
	FTC vs. Nancy H. Merrill <a href="http://www.ftc.gov/opa/2002/11/netforce.htm">www.ftc.gov/opa/2002/11/netforce.htm</a>					

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. Nia Cano, et al. <a href="http://www.ftc.gov/opa/1997/11/cdi.htm">www.ftc.gov/opa/1997/11/cdi.htm</a>					
	FTC vs. One or More Unknown Parties <a href="http://www.ftc.gov/opa/2003/01/dpfinal.htm">www.ftc.gov/opa/2003/01/dpfinal.htm</a>					
	FTC vs. Para-Link International, Inc., et al. <a href="http://www.ftc.gov/opa/2000/10/paralink.htm">www.ftc.gov/opa/2000/10/paralink.htm</a>					
	FTC vs. Cliff Cross and d/b/a Build-It-Fast <a href="http://www.ftc.gov/opa/1999/02/consumerweek2.htm">www.ftc.gov/opa/1999/02/consumerweek2.htm</a>					
	FTC vs. D Squared Solutions <a href="http://www.ftc.gov/opa/2003/11/dsquared.htm">www.ftc.gov/opa/2003/11/dsquared.htm</a>					
	FTC vs. David Martinelli, Jr. <a href="http://www.ftc.gov/opa/1999/07/dpmarket.htm">www.ftc.gov/opa/1999/07/dpmarket.htm</a>					