On-line privacy and data protection in the EU

Merijn Schik,
DG Information Society, European Commission

Disclaimer

This presentation is provided for information purposes only
It does not constitute an official position of the European Commission. The Commission cannot accept any responsibility or liability. The Commission is not the arbiter for interpretation of Community law. Only the European Court of Justice can decide finally on the interpretation of Community law.





Introduction

- Actions taken by Member States 2006-2008 in the fight against spam, spyware and malware (stock taking exercise prepared by Timelex CVBA)
- Telecom Review proposals

Background: 2006 Communication on stepping up the Fight against spam, spyware and malware

Content

- Stakeholders actions to raise awareness
- Protective measures taken by industry/best practices
- Enforcement efforts by competent authorities
- State of international cooperation

2006 Communication on stepping up the Fight against spam, spyware and malware

Identified critical success factors for enforcement

- A strong commitment by central government
- Clear organisational responsibility
- Adequate resources for the enforcement authority

2006 Communication on stepping up the Fight against spam, spyware and malware

Action list

- Enforcement efforts should be stepped up
- Clear responsibilities for national agencies should be established and effective coordination should be ensured
- Knowledge and expertise of market players should be put to use
- Agencies should be adequately resourced
- International cooperation procedures should be put into practice
- Industry responsibility (filtering, information standards etc.)

Main findings of the Study

- Legislation to combat spam and online malware is in place in the EU. Enforcement has increased.
- There are informative websites and/or complaint channels in place in all Member States
- In general the industry has implemented and provides technical measures against spam and malware
- There are several examples of well organized cooperation between government agencies and with the industry

However the activity level and availability of information differs between Member States

- In general the level of cooperation between government agencies and with industry should be improved
- Effective sanctions are not always imposed and the number of cases prosecuted varies considerably
- Not enough cooperation schemes are in place at the international level
- More resources should be dedicated to competent authorities (budget and staff)

Examples

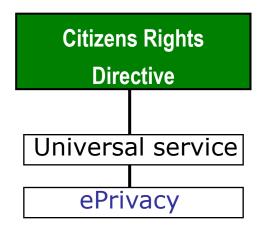
- More than 140 cases investigated in EU Member States (Spain (39), Slovakia (39) and Romania (20)) while some countries investigated only a handful of complaints.
- The highest fines were imposed in the Netherlands (€1 000 000), Italy (€570 000) and Spain (€30 000) while in other countries spammers received very modest fines ranging from several hundreds to several thousands of Euros
- Good examples of cooperation schemes such as Signalspam (France), eCops (Belgium), the Cybercrime Working group (the Netherlands)

Commission concludes

- Member States and all stakeholders should reinforce their efforts to fight on-line privacy threats from spam, spyware and malware
- Evidence shows that while progress has been made, we need to do more (resources, national/international cooperation)
- The Commission has already played a significant part by proposing new instruments in the Telecom Reform Package which will support these efforts once the new telecom rules are adopted

The Telecom Reform package





Digital Dividend Communication

Review Communication

Regulation on Authority

Recommendation relevant markets + Explan Note

Impact Assessment + Summary



Directive 2002/58 on privacy and electronic communications (ePrivacy Directive)

Art 13 of Directive 2002/58 (ePrivacy Directive) puts a ban on spam:

- Direct marketing using electronic mail (automated calls, e-mail, SMS, fax) is subject to prior consent of subscribers. There is a limited exception for communications sent to existing customers by the same person on its similar services or products
- > This regime applies to subscribers who are natural persons, but Member States can choose to extend it to legal persons
- Disguising or concealing the identity of the sender on whose behalf the communication is made is prohibited
- All e-mails must include a valid return address where to opt-out



Telecom Reform Package

Strengthening the existing rules on spam

- Including the sending of 'phishing' messages in the activities banned by art. 13 by prohibiting the sending of e-mail that is in contravention of art. 6 of Directive 2000/31/EC;
- Introducing a new paragraph to art. 13 which provides natural or legal persons with a private right of action against spammers;
- Formalizing cross border enforcement cooperation mechanisms by including art. 13 in the EU Regulation on Consumer Protection Cooperation (CPC Regulation)

Directive 2002/58 on privacy and electronic communications (ePrivacy Directive)

Article 5 of Directive 2002/58 (ePrivacy Directive)

 Allows the storing of information/access to information stored in terminal equipment using electronic communications networks under specific conditions (prior information, right to refuse)

Telecom Reform Package

Strengthening the existing rules on spyware and malware

 Storing information/access to information stored in terminal equipment using spyware, malware is always illegal, irrespective whether this is installed using a electronic communication network or from an "offline" source (CD-ROM, USB key etc.).

Other proposals included in the Telecom Reform Package: security

Stronger obligations for operators to ensure the integrity and security of their networks and services

- Consumer contracts to provide minimum of information related to security of electronic communications services
- Mandatory breach notification
 - to competent authority: significant impact on operation
 - to competent authority and consumers: personal data compromised

Other proposals included in the Telecom Reform: empowering national authorities

Increased enforcement capability

- Binding instructions on security measures (set at national or EU level)
- Better information
 - notifications
 - security audits
- Sufficient resources
- Better cooperation and support
 - CPC Regulation

References

Commission Telecom Reform proposals:

http://ec.europa.eu/ecomm

European Parliament legislative observatory:

http://www.europarl.europa.eu/oeil/FindByProcnum.do?lang=2&procnum=COD/2007/0248

The Study:

The press release: IP/09/1487 (Commission press room)