Protecting Privacy and Fighting Spam

The EU's ePrivacy Directive sets strict limits on how personal data can be stored and used, particularly when it comes to sending spam and other forms of 'unsolicited communications'. Laws, however, are not always enough.

The Information Society offers users a potentially massive range of new products and services. With these new possibilities, however, come new risks to users' personal data and privacy; an avalanche of spam; and a host of new challenges for national authorities in collecting information for law enforcement and national security.

Advanced technologies can provide a large part of the solution. Networks, hardware and software can - and should - be designed to put users in control of their own personal information and private sphere.

Given the considerable commercial and state interests in collecting personal data, however, this will only happen with a clear, enforceable legal framework guaranteeing the individual's right to privacy and regulating the measures to achieve it.

ePrivacy Directive

Hence the **Privacy and Electronic Communications Directive** (2002/58/EC), part of the EU's eCommunications Regulatory Framework, which came into force in July 2002.

The 'ePrivacy Directive' protects fundamental rights and freedoms of natural persons with regard to automated storage and processing of their data, and sets strict limits on the use of "spam".

User Data

The e-Privacy Directive requires companies to:

- delete or render anonymous **traffic data -** from which a user's contacts, lifestyle, location, habits and more can be derived - after it is no longer needed for the provision of the service;
- **obtain subscriber consent** before marketing or offering other added value services;
- **inform customers** of the data processing to which their data will be subject;
- only use **location data** with the consent of the subscriber, and only to the extent and for the duration necessary to provide the service. Even when consent has been given, moreover, users should be able to temporarily block location tracing systems.

Confidentiality

The Directive does not just cover what companies can do with users' personal data – it also obliges service providers to take appropriate measures to safeguard the **security of the services** they provide and, if necessary, to do so jointly with network operators.

Networks, hardware and software should be designed to put users in control …

The aim is to ensure that users' on-line behaviour and data - the websites they visit, their credit card details, their emails and more - remain confidential.

The level of security should reflect the risks. Service providers must inform their customers of all risks of breach of network security and, where such risks lie outside of the service providers' own measures, they must advise users on possible remedies and the likely costs involved.

Malicious Software

The Directive also covers access to information stored on the **user equipment** connected to these networks, such as PCs and mobile phones. The ability of these devices to safeguard users' privacy can be compromised with software (viruses, spyware, Trojan horses), used to spy on the victim, take remote control of their equipment, or simply damage their data.

Alongside this malicious software, however, may sit perfectly innocent, useful programs, used for anything from copyright protection to helping the user navigate and use online services.

The Directive therefore empowers the users by giving them the right to clear information about what is stored on their equipment, the right to refuse such storage and the right to refuse access to information once stored. This includes 'cookies' – small files used to register users' preferences as they visit websites.

Keeping Your Number Private

While most people prefer to have their fixed line telephone number in their local 'white pages', fewer would want their mobile phone or email address listed, particularly as this data appears on-line.

The Directive therefore grants subscribers the right to decide for themselves what they want to list in public directories, and ensures that going 'ex-Directory' is free of charge.

The Directive also ensures users can both cancel Calling Line Identification (so the person called cannot see the caller's number before answering), and can request that their number not be displayed to the caller (e.g., when a business call is 'auto-forwarded' to the user's private number).

Exceptions

In several cases the protection offered by the Directive has to be balanced against other issues. The suppression of Calling Line Identification (CLI), for example, can be overridden if the call is made to Emergency Services (who can use CLI to locate the caller) or in the case of nuisance or malicious calls.

Member States can also take measures necessary for protecting public security, defence, State security and criminal law enforcement.

Nonetheless, the Directive explicitly states that such measures must be legislative in nature as well as appropriate, proportionate to the intended purpose, necessary within a democratic society and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950).

Fighting Spam

Spam is not a minor phenomenon – more than half of all EU e-mail traffic was estimated to be spam in December 2003. This represents a massive invasion of privacy; consumer fraud; an unregulated wave of harmful content received by minors; higher business costs; lower productivity and an overall brake on the growth of the Information Society as a whole.

Opting In

The Directive establishes an 'opt-in' regime: no direct marketing electronic mail can be legally sent without the express consent of the receiver, unless a pre-existing business or commercial relationship exists.

Even then, a specific opt out must be offered with each message. Disguised sender identities are prohibited, and a valid return address must be provided.

A Coordinated Fight Across Europe

Legislation, of course, is not enough, particularly as most spam received in the EU originates elsewhere.

Hence the **Communication on unsolicited commercial communications or 'spam'** (COM(2004) 28, January 2004), which identified a series of actions to complement the rules.

The actions focus on effective enforcement by Member States and public authorities, technical and self-regulatory solutions by industry, consumer awareness, and international cooperation.

Examples include providing competent authorities with the powers to trace and prosecute 'spammers', adapting marketing practices to the Directive's opt-in regime, and user education.

While the Commission will support these efforts, they are primarily for Member States and authorities, industry and consumers, both at the national and international level.

In March 2004, however, the Commission proposed the **Safer Internet Plus (2005-2008) programme,** which will fund, inter alia:

- technologies to empower users to limit the amount of unwanted and harmful content they receive;
- assessments of and further developments in filtering technology;
- exchanges of information and best practice.

International Cooperation

The EU is also tackling the international dimension, hosting an OECD workshop on spam in February 2004 and proposing a five point OECD framework:

- An effective 'anti-spam' law in all countries;
- Cross-border cooperation on enforcement in specific cases;
- Self-regulatory solutions by market players;
- Technical solutions to manage or reduce spam, such as filtering and other security features;
- Greater consumer awareness - e.g., how to minimise spam, how to react and complain, etc.

In July 2004 the OECD created a Task Force on Spam and the Commission presented its vision to the UN's World Summit on the Information Society (ITU WSIS) Thematic Meeting on Countering Spam.

The Commission will monitor the implementation of these actions, assessing by the end of 2004 whether additional or corrective action is needed.

See Also:

- FactSheets 13 & 14: eCommunications Regulation
- Factsheet 18: Safer Internet Programme

All Factsheets and more can be downloaded from "Europe's Information Society: Thematic Portal", below.

Further Information

- **eCommunications Regulation:** http://europa.eu.int/information_society/topics/ecomm/index_en.htm
- **Europe's Information Society: Thematic Portal** http://europa.eu.int/information_society/
- **Information Society Directorate-General:** Av. de Beaulieu 24, 1160 Brussels infso-desk@cec.eu.int