Protecting privacy and fighting spam.

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

The Information Society offers users a massive range of new products and services. With these new possibilities come new risks to users' personal data and privacy, such as an avalanche of e-mail spam.

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, there needs to be a clear, enforceable legal framework guaranteeing the individual's right to privacy and protection of personal data.

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

ePrivacy Directive

Hence the **Directive on Privacy and electronic communications** (2002/58/EC), part of the EU's eCommunications regulatory framework, which came into force in July 2002.

The 'ePrivacy Directive' protects the privacy and the personal data of natural persons (and the legitimate interests of legal persons) when using communications services. It also 'bans' spam and spy ware.

Confidentiality

In short, the ePrivacy Directive requires companies to ensure the confidentiality of your communications and of the generated traffic data and in particular to:

- delete or render anonymous traffic data generated by communications **-** 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;
- inform customers of the data processing to which their data will be subject and
- obtain subscriber consent before using traffic data for marketing or before offering added value services with traffic or location data.

Security

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.

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

Malicious software

The directive also covers access to the user equipment connected to the networks, such as PCs and mobile phones. The privacy of users can be compromised with software (viruses, spy-ware, 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 or useful programs, for anything from copyright protection to helping the user navigate and use online services.

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

The Directive empowers users by giving them right to information

Keeping your number private

While people generally 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 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 that users can both cancel Calling Line Identification (CLI - 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 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 to protect public security, defence, State security and criminal law enforcement. 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).

Moreover, the Commission has recently proposed a Directive on data retention which aims to harmonise further data retention for serious criminal offences. The European Parliament and the Council are at present discussing its final wording.

Fighting spam

Spam is not a minor phenomenon (more than half of all EU e-mail traffic was estimated to be spam in 2005) and one that undermines consumer confidence in electronic communications. 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. (Consent is however not mandated for marketing to legal persons.)

Also, 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', developing technology and adapting marketing practices to the directive's regime, and user education.

While the Commission supports these efforts (it has for instance set up a contact network of spam authorities to facilitate enforcement and helped create the OECD Task Force on Spam) they are primarily a matter for Member State authorities, industry and consumers, both at national and international levels.

However, in May 2005, the EU adopted 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 and
- exchange of information and best practice.

See Also:

- Fact sheets 13 & 14: eCommunications Regulation
- Fact sheet 18: Safer Internet Programme

More fact sheets 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
- **Privacy Protection**
  http://europa.eu.int/information_society/policy/ecomm/todays_framework/privacy_protection/index_en.htm
- **Europe's Information Society: Thematic Portal**
  http://europa.eu.int/information_society/
- **Information Society and Media Directorate-General:**
  Av. de Beaulieu 24, 1160 Brussels
  infso-desk@cec.eu.int