GLOBAL INTERNET POLICY INITIATIVE

EU Directive on Privacy Protection
in the Electronic Communications Sector

October 2002

I. Overview

In July 2002, the European Union approved a new directive establishing legal standards for the processing of personal data and the protection of privacy in the electronic communications sector.[1] The purpose of the new directive is to update EU law to reflect continuing technological developments in telecommunications and other electronic communications services and to provide an equal level of privacy protection to personal data regardless of the technologies used to provide the services.[2]

The new directive adopts several new or clarified policies:

- On unsolicited marketing messages or "**spamming**," the new directive adopts an "opt-in" approach, which means that users must give prior permission before being sent unsolicited electronic communications (via e-mail, faxes and automated calling systems) for marketing purposes.
- However, the directive allows merchants to use e-mail addresses collected from customers in the course of a sale to market similar products or services to those customers under an "opt-out" rule.
- The directive also adopts an opt-in rule for use of **traffic data** (transactional data showing patterns of usage of communications services) for the purpose of marketing electronic communications services or providing value added services.

[1] The new directive is 2002/58/EC, published in the Official Journal at OJ L 201/37, on 31/7/2002. It can be found, along with other EU directives relating to electronic communications services, at http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm . The new directive replaces Directive 97/66/EC of December 15, 1997, OJ L 024, 30/01/1998 ("Directive 97/66/EC").

[2] For example, while Directive 97/66/EC referred to "telecommunications services," the new directive applies to the broader category of "electronic communications services." See Proposal for a Directive of the European Parliament and of the Council concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, Commission of the European Communities, Com (2000)385 available at http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm .

- As regards "**cookies**," the directive adopts an opt-out approach, specifying that cookies cannot be used unless users have been provided with clear and precise information on their purposes and the opportunity to refuse them.
- On the inclusion of personal data (physical addresses, fixed and mobile phone numbers, and e-mail addresses) in **public directories**, the directive also adopts an opt-out rule, stating that subscribers must be informed of all the possible uses of publicly available directories, (e.g., that a reverse search can be made from a telephone number in order to obtain a name and address) and must be provided free of charge the right not to appear in a public directory.
- The directive adopts special rules for the collection and use of **location data** (other than traffic data). It bars collection or use of location data other than traffic data without the explicit prior permission of the phone's owner and requires that users must be able to withdraw their consent for the collection or other processing of location data at any time.

A major issue in the debate over the new directive involved the question of whether governments could require service providers to retain traffic data (transactional information, not content) associated with the communications of their subscribers so that it would be available if subsequently requested for law enforcement and national security purposes. The new directive states that Members of the EU may, but are not required to, adopt such "**data retention**" requirements in their national laws. This actually involved no change in EU law – data retention laws were probably consistent with the prior directive. However, the decision of the EU Parliament to explicitly permit data retention will likely be seen by some Member States as an encouragement for the adoption of such requirements. However, the new directive makes it clear that such data retention requirements can be imposed only by national legislation and only when such requirements constitute "a necessary, appropriate, and proportionate measure within a democratic society." Moreover, the disclosure of such data can be required only in specific cases pursuant to the authority of an independent official acting under rules consistent with human rights protection. The preamble makes it clear that interceptions of electronic communications and access to traffic data must be subject to adequate safeguards in accordance with the European Convention on Human Rights, as interpreted by the rulings of the European Court of Human Rights. Recital 11.

The new privacy directive for electronic communications services must be read in conjunction with the EU's landmark 1995 directive on data protection.[3] The new directive translates the 1995 directive into specific rules for the electronic communications sector. The definitions and basic rules of the 1995 directive apply to the electronic communications sector. For example, the key term "processing" is defined in the 1995 data protection directive.[4] And

---

[3] The 1995 data protection directive, 95/46/EC, is available online at http://www.cdt.org/privacy/eudirective/EU_Directive_.html (unofficial) and at http://europa.eu.int/eur-lex/en/search/search_lif.html (type in the date (1995) and the number (46) and search "Directives").

[4] Under the 1995 data protection directive, "processing of personal data" ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration,

the key elements of data protection in the 1995 directive – including the data quality principle, the essential components of notice, and the data subject's right of access to data – apply to the electronic communications sector.

Each Member State has until October 31, 2003 to pass implementing legislation that incorporates the new EU directive into its own legal structure.

II. Key Provisions of the New Communications Privacy Directive

1. Security and Confidentiality of Communications (Articles 4 and 5)

Under Article 4, a provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard the security of its services. Under Article 5, Member States are required to adopt national legislation to ensure the confidentiality of communications. The new directive expressly extends this confidentiality obligation to traffic data.[5] Such laws should prohibit listening, tapping, storage or other kinds of interception or surveillance of communications without the consent of the users concerned or pursuant to strictly limited legal authority, as permitted under Article 15 (see below).

2. Automatic Erasure of Traffic Data -- Information Gathered for Billing (Articles 6 and 7)

As a general rule under the new directive, as under the previous Directive 97/66/EC, traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. The provision, however, was always subject to exceptions, which are spelled out in the new directive:

- Limited Data Storage for Billing Permitted. Providers may process traffic data for the purposes of subscriber billing and interconnection payments. However, such storage will be permitted only up to the end of the period during which such bills may be lawfully challenged or the payment pursued. Article 6(2).

- Must Inform Subscribers of Data Uses. The service provider must inform the subscriber or user of the types of traffic data that are being processed and of the duration of such

---

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available … ."

[5] Traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. It includes data referring to the routing, duration, time or volume of a communication; the protocol used; the location of the terminal equipment of the sender or recipient; the network on which the communication originates or terminates; or the beginning, end or duration of a connection. It also may consist of the format in which the communication is conveyed by the network. Article 2 and Recital 15.

processing, both in order to use the data for billing and prior to obtaining consent for marketing electronic communications services or providing value added services.

- Consent Needed for Data Use to Market Electronic Communications Services or Provide Value Added Services. Providers may process traffic data for marketing electronic communications services or for the provision of value added services, if the subscriber or user at issue has given his prior consent. Users and subscribers must be given the opportunity to withdraw their consent for the processing of traffic data at any time. Article 6(3).

- Itemized Billing. Subscribers shall have the right to receive non-itemized bills if they do not want records kept of their calling behavior. Article 7 and Recital 33.

3. Law Enforcement and National Security Exception (Article 15)

Article 15 (1) provides that Member States may adopt legislative measures to restrict the scope of rights and obligations provided in Articles 5, 6, 8 (regarding caller ID) and Article 9 (regarding location information) when the restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defense, or public security or for the prevention, investigation, detection and prosecution of criminal offenses or to prevent unauthorized use of the electronic communications system. A similar exemption is contained in Article 13(1) of Directive 95/46/EC.

- Data Retention Permitted. Governments were concerned that the automatic erasures of traffic data mandated by the 1995 data protection directive and the prior telecommunications directive permitted no exception and therefore impeded law enforcement and national security. They noted that it was impossible for investigators to know in advance which traffic data would prove useful in an investigation and that, with automatic erasure, the relevant information could be gone by the time the authorities realized their need for it.

  Traffic data includes a significant amount of information on an individual's personal life. Traffic data includes, for example, a list of all those to whom a person has sent email or made a telephone call, when and for how long, and which Internet sites have been visited.

  The new directive clarified the issue by specifically permitting Member States to adopt legislative measures providing for the retention of data "for a limited period" if justified on the grounds outlined in Article 15.

- Privacy Standards Necessary. Any measure adopted, however, must be in accordance with general principles of Community law and the Treaty on European Union. Also, Recital 11 also states that any action by Member States must be "in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by rulings of the European Court of Human Rights."

Therefore, any nation choosing to impose a data retention requirement must develop strict legal protections for data retention. These legal standards must address two issues: The data retention requirement itself must be expressed in national legislation and must be only as extensive as is "necessary, appropriate, and proportionate … within a democratic society." Secondly, data retention is distinct from data disclosure. In order to compel disclosure of traffic data, the government must proceed on a cases-by-case basis, seeking only the data of a particular subject and should act only pursuant to the permission of a judicial official or other independent overseer, under the principles laid down by the European Court of Human Rights.[6]

The new Directive does not clearly define several key terms, such as what will qualify as "data" that is subject to retention. The directive also fails to define a maximum length of time that data can be required to be retained. These questions must be carefully examined by any nation considering a data retention requirement. It should be noted that some nations, including the United States, do not mandate data retention.

The Directive does not discuss service provider obligations in terms of real-time interception of communications.

4. Caller ID (Article 8)

Article 8 governs the presentation of calling and connected line identification (caller ID), seeking to balance the interests of called parties and calling parties.

- Per-Line and Per-Call Blocking Required. Where Caller ID is offered, the service provider must offer calling parties, free of charge, the possibility to easily block presentation of the calling line number on a per-call and per-line basis.

- Refusing Blocked Calls. Where Caller ID is offered and where the calling identification is presented prior to the call being established, the service provider must offer the called party the possibility to reject incoming calls where presentation of Caller ID has been blocked by the calling party.

5. Location Data Other than Traffic Data (Article 9)

The new directive gives special protection to location data, which is increasingly generated by mobile phones and other mobile devices for use in providing location-based services.

---

[6] For a fuller discussion of legal standards for interception of communications, see the GIPI paper "Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime," August 2002, available at http://www.internetpolicy.net/practices/ .

- Definition. Location data means any data processed in an electronic communications network that indicates the geographic position of the terminal equipment of a user of a publicly available electronic communications service. It may refer to the latitude, longitude or altitude of the user's terminal equipment, the direction of travel, the level of accuracy of the location information, the identification of the network cell in which the terminal equipment is located at a certain point in time; and the time or the location where the information was recorded. See Article 2 and Recital 14. Some location data, such as cell site information, may be included within traffic data. The special provisions of Article 9 apply to location data that is not traffic data.

- Consent Needed for Data Use with Value Added Services. The new directive provides that location data can be collected and used only in anonymous form or with the consent of users to the extent and for the duration necessary for the provision of value added services.[7]

- Users Can Withdraw Consent at Any Time. Users or subscribers must have the possibility, using a simple means and free of charge, to withdraw their consent for the processing of location data for each connection to the network or for each transmission of a communication. See Article 9(2).

6. Directories of Subscribers (Article 12)

- Inform Subscribers of Possible Uses of Data. Member States shall ensure that subscribers are informed, free of charge and before they are included in a printed or electronic directory that is available to the public or obtainable through directory inquiry services, of the possible uses that may be made of such directories.[8] See Article 12(1) and Recitals 38 & 39.

- Subscribers Can Opt-Out Free of Charge. Subscribers have the right to determine whether they are listed in a public directory. They also have the right, free of charge, to verify, correct, or withdraw personal data listed in a directory. See Article 12(2).

- Notification Needed if Data To Be Shared with Third Parties. If personal data will be shared, subscribers should be informed of the possibility that their personal data may be transmitted to one or more third parties. The subscriber should be informed of the recipients or possible categories of recipients. See Recital 39.

---

[7] "Value added services" may consist, for example, of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information. See Recital 18.

[8] Such uses may include, for example, search functions that are embedded in the software. This may include, for example, reverse search functions that enable users of the directory to discover the name and address of the subscriber using a telephone number.

- Transitional Rules. Article 12 does not apply to directories already printed. Where personal data of fixed line or mobile telephone subscribers is included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and Article 11 of Directive 97/66/EC before national legislation implementing the new Directive becomes effective, the personal data of such subscribers may remain in the public directory (including versions with reverse search functions) unless subscribers indicate otherwise. Article 16.

7. Unsolicited Communications for Direct Marketing (Article 13)

- Prior Consent / Opt-In Standard Adopted for Commercial E-Mail. The directive adopts an opt-in approach to unsolicited commercial e-mail. The new standard provides that the use of electronic mail, automatic calling machines or facsimile machines for the purposes of direct marketing may be allowed only with subscribers who have given their prior consent.

- Data Use Permitted within "Existing Customer Relationship." A company that has obtained electronic contact details (in accordance with Directive 95/46/EC) within the context of an existing customer relationship may use that information to offer users its own similar products or services. Consumers, however, must have the right to object, free of charge and in an easy manner, to receiving such materials. See Recital 41 and Article 13(2).

- Definition of Consent. Consent of a user or subscriber as used in this directive is defined in the same manner as used in Directive 95/46/EC. Generally, consent may be provided by any appropriate method that indicates "a freely given specific and informed indication of the user's wishes, including by checking a box when visiting an Internet web site." See Recital 17.

- Unsolicited Direct Marketing Materials Must Include the Identity of Sender. The Directive prohibits sending direct marketing e-mails that disguise or conceal the identity of the sender, or that do not include a valid address to which the recipient may send a request that such communications cease. This requirement is necessary in order to facilitate effective enforcement of the rule on unsolicited messages. See Article 13(4).

Conclusion

Privacy protection is an important component of the policy framework for development of information and communications networks. The new EU directive of 2002 provides an important model for detailed rules for communications services, within the broader context of privacy protection established by the EU's 1995 data protection directive.

For more information, contact: Paige Anderson, GIPI Counsel, panderson@cdt.org, or Jim Dempsey, GIPI Policy Director, jdempsey@cdt.org