

Brussels, 30 September 2010

Digital Agenda: Commission refers UK to Court over privacy and personal data protection

The European Commission has decided to refer the United Kingdom to the EU's Court of Justice for not fully implementing EU rules on the confidentiality of electronic communications such as e-mail or internet browsing. Specifically, the Commission considers that UK law does not comply with EU rules on consent to interception and on enforcement by supervisory authorities. The EU rules in question are laid down in the ePrivacy Directive [2002/58/EC](#) and the Data Protection Directive [95/46/EC](#). The infringement procedure was opened in April 2009 ([IP/09/570](#)), following complaints from UK internet users notably with regard to targeted advertising based on analysis of users' internet traffic. The Commission previously requested the UK authorities in October 2009 ([IP/09/1626](#)) to amend their rules to comply with EU law.

The Commission launched the legal action against the UK in April 2009 following citizens' complaints about how the UK authorities had dealt with their concerns about the use of behavioural advertising by internet service providers (targeted advertising based on prior analysis of users' internet traffic). These complaints were handled by the UK Information Commissioner's Office, the UK personal data protection authority and the police forces responsible for investigating cases of unlawful interception of communications.

The Commission considers that existing UK law governing the confidentiality of electronic communications is in breach of the UK's obligations under the ePrivacy Directive [2002/58/EC](#) and the Data Protection Directive [95/46/EC](#) in three specific areas:

- there is no independent national authority to supervise the interception of some communications, although the establishment of such authority is required under the ePrivacy and Data Protection Directives, in particular to hear complaints regarding interception of communications
- current UK law authorises interception of communications not only where the persons concerned have consented to interception but also when the person intercepting the communications has 'reasonable grounds for believing' that consent to do so has been given. These UK provisions do not comply with EU rules defining consent as "freely given, specific and informed indication of a person's wishes"
- current UK law prohibiting and providing sanctions in case of unlawful interception are limited to 'intentional' interception only, whereas EU law requires Members States to prohibit and to ensure sanctions against any unlawful interception regardless of whether committed intentionally or not.

Background

The EU Directive on privacy and electronic communications requires EU Member States to ensure confidentiality of the communications and related traffic data by prohibiting unlawful interception and surveillance unless the users concerned have consented to this (Article 5(1) of [Directive 2002/58/EC](#)). The EU Data Protection Directive specifies that user consent must be 'freely given specific and informed' (Article 2(h) of [Directive 95/46/EC](#)). Moreover, Article 24 of the Data Protection Directive requires Member States to establish appropriate sanctions in case of infringements and Article 28 says that independent authorities must be charged with supervising implementation. These provisions of the Data Protection Directive also apply in the area of confidentiality of communications.

An overview of telecoms infringement proceedings is available at:

http://ec.europa.eu/information_society/policy/ecomm/implementation_enforcement/infringement/index_en.htm

For more information on EU infringement procedures, see [MEMO/10/457](#).