IP/09/570

Brussels, 14 April 2009

Telecoms: Commission launches case against UK over privacy and personal data protection

The Commission has opened an infringement proceeding against the United Kingdom after a series of complaints by UK internet users, and extensive communication of the Commission with UK authorities, about the use of a behavioural advertising technology known as 'Phorm' by internet service providers. The proceeding addresses several problems with the UK's implementation of EU ePrivacy and personal data protection rules, under which EU countries must ensure, among other things, the confidentiality of communications by prohibiting interception and surveillance without the user's consent. These problems emerged during the Commission's inquiry into the UK authorities' action in response to complaints from internet users concerning Phorm.

"Technologies like internet behavioural advertising can be useful for businesses and consumers but they must be used in a way that complies with EU rules. These rules are there to protect the privacy of citizens and must be rigorously enforced by all Member States," said EU Telecoms Commissioner Viviane Reding. *"We have been following the Phorm case for some time and have concluded that there are problems in the way the UK has implemented parts of EU rules on the confidentiality of communications. I call on the UK authorities to change their national laws and ensure that national authorities are duly empowered and have proper sanctions at their disposal to enforce EU legislation on the confidentiality of communications. This should allow the UK to respond more vigorously to new challenges to ePrivacy and personal data protection such as those that have arisen in the Phorm case. It should also help reassure UK consumers about their privacy and data protection while surfing the internet."*

Since April 2008, the Commission has received several questions from UK citizens and UK Members of the European Parliament concerned about the use of a behavioural advertising technology known as 'Phorm' by Internet Service Providers in the UK. Phorm technology works by constantly analysing customers' web surfing to determine users' interests and then deliver targeted advertising to users when they visit certain websites. In April 2008, the UK fixed operator, BT, admitted that it had tested Phorm in 2006 and 2007 without informing customers involved in the trial. BT carried out a new, invitation-based, trial of the technology in October-December 2008. BT's trials resulted in a number of complaints to the UK data protection authority – the Information Commissioner's Office (ICO) and to the UK police.

The Commission has written several letters to the UK authorities since July 2008, asking how they have implemented relevant EU laws in the context of the Phorm case. Following an analysis of the answers received the Commission has concerns that there are structural problems in the way the UK has implemented EU rules ensuring the confidentiality of communications.

Under UK law, which is enforced by the UK police, it is an offence to unlawfully intercept communications. However, the scope of this offence is limited to 'intentional' interception only. Moreover, according to this law, interception is also considered to be lawful when the interceptor has 'reasonable grounds for believing' that consent to interception has been given. The Commission is also concerned that the UK does not have an independent national supervisory authority dealing with such interceptions.

The UK has two months to reply to this first stage of an infringement proceeding, the letter of formal notice sent today. If the Commission receives no reply, or if the observations presented by the UK are not satisfactory, the Commission may decide to issue a reasoned opinion (the second stage in an infringement proceeding). If the UK still fails to fulfil its obligations under EU law after that, the Commission will refer the case to the European Court of Justice.

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 (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.

A detailed overview of telecoms infringement proceedings is available at:

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