BERR | Department for Business Enterprise & Regulatory Reform

Fabio Colosanti

Director-General

Information Society and Media Directorate-General

The European Commission

Rue de la Loi 200

B-1049 Brussels

11 September 2008

Dear Mr Colosanti,

The Use of Phorm Technology by Internet Service Providers

Thank you for your letter of 3rd July 2008 concerning the use by some UK internet service providers of technology provided by a company called Phorm.

The UK is committed to providing a high level of consumer protection. In the context of internet services, we have established a robust framework to give users confidence that they can safely participate in the information society. We take our community obligations very seriously especially in the area of data protection and e-privacy. The possible future use of Phorm technology has raised material concerns in this area and the UK authorities are working to ensure that if it is introduced into the market for internet based advertising services, this is done in a lawful, appropriate and transparent fashion.

Phorm has developed a system where, with the cooperation of an individual's ISP they can profile the addresses and certain contents of websites visited by users and then use that information to match that user against predefined broad advertising categories. After conducting its enquiries with Phorm the UK authorities consider that Phorm's products are capable of being operated in a way that do not contravene the E-Privacy or Data Protection Directive on the following basis:

- the user profiling occurs with the knowledge and agreement of the customer;
- the profile is based on a unique ID allocated at random which means that there is no need to know the identity of the individual users;
- Phorm does not keep a record of the actual sites visited;
- search terms used by the user and the advertising categories exclude certain sensitive terms and have been widely drawn so as not to reveal the identity of the user;
- Phorm does not have nor want information which would enable it to link a user ID and profile to a living individual;

- users will be presented with an unavoidable statement about the product and asked to exercise a choice about whether to be involved; and
- users will be able to easily access information on how to change their mind at any point and are free to opt in or out of the scheme.

The UK does not know what if any plans there are to roll-out this technology by ISPs, but future developments will be closely scrutinised and monitored by the enforcement authorities.

The UK welcomes the Commission's interest in this issue and is keen to do whatever it can to assist with its inquiries. I hope you will find the UK's response to the Commission's satisfaction, but please do not hesitate to contact me if you require any further clarification or if you would like to arrange to meet in order to discuss these points in greater detail.

Q1. What are the United Kingdom laws and other legal acts which govern activities falling within the scope of Articles 5(1) and 6 of Directive 2002/58/EC on privacy and electronic communications and Articles 6, 7, and 17(1) of Directive 95/46/EC?

Directive 2002/58/EC (E-Privacy Directive)

The web-site references are to the original un-amended legislation, as enacted to give effect to community obligations.

The requirements under Article 5(1) are satisfied under UK law by the Regulation of Investigatory Powers Act 2000 (c23) (RIPA)[1].

Article 6(1) was transposed into UK law through Regulation 7(1) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI2003/2426) (PECR) [2].

Article 6(2) was transposed into UK law under Regulation 7(2) and (5) of the PECR.

Article 6(3) was transposed into UK law by regulation 7(3) and (4) of the PECR.

Article 6(4) was transposed into UK law by regulation 8(1) of the PECR.

Article 6(5) was transposed into UK law by regulation 8(2) and (3) of the PECR.

Article 6(6) was transposed into UK law by regulation 8(4) of the PECR.

Directive 95/46/EC (Data Protection Directive)

The Data Protection Directive was transposed into UK law by the Data Protection Act 1998 (DPA), c29[3].

---

[1] http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

[2] http://www.opsi.gov.uk/si/si2003/20032426.htm

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI2003/2426)

Articles 6 and 7 are reflected in the 8 data protection principles found in part 1 of schedule 1, and schedules 2 and 3 to the DPA.

Article 17(1) is reflected in the 7th Data Protection Principle found in Schedule 1 part 1 to the DPA.

Q2. Which United Kingdom Authorities are competent (i) to investigate whether there have been any breaches of the national law transposing each of the above mentioned provisions of Community law arising from the past trials of Phorm technology carried out by BT and (ii) to impose any penalties for infringement of those provisions where appropriate?

The Information Commissioner's Office (ICO) is responsible for seeking to ensure compliance with both the Data Protection Directive and the E-Privacy Directive, which complements and supplements the Data Protection Directive in the electronic communications sector. The UK has complied with its duty under Article 28 of the Data Protection Directive by ensuring that ICO acts with complete independence in exercising the functions entrusted to it.

The ICO is competent to investigate breaches of national law implementing community obligations under the E-Privacy Directive and Data Protection Directive, except for those provisions implemented by RIPA. The UK police forces are competent to instigate a criminal investigation into an allegation of unlawful interception as defined by RIPA.

The ICO currently has the legal powers to:

- conduct assessments of organisations' compliance with the DPA or PECR (s.42 DPA);
- serve an 'Information Notice' requiring that an organisation supply the ICO with information to assist in conducting such assessments (s.43 DPA);
- obtain a warrant from a court authorising the Commissioner to enter premises to gather evidence of contraventions of the data protection principles or offences committed under the DPA or PECR (s.50 and Schedule 9 to DPA); and
- serve an 'Enforcement Notice' to ensure organisations are complying with, or refraining from activity which could contravene the DPA or PECR (s.40 DPA).

If a person fails to comply with an Enforcement Notice or Information Notice, that person would be guilty of an offence (S.47 DPA) and liable upon summary conviction to a fine up to the statutory maximum of £5,000 or on conviction on indictment to an unlimited fine.

---

[3] http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Q3. Have there been any investigations about the past trials of Phorm technology by BT and what were their results and the conclusions of the competent authorities? Are there ongoing investigations about possible similar activities by other ISPS?

The ICO did not become aware that BT had carried out trials of Phorm technology in September/October 2006 and June 2007 until the BBC reported them on 1 April 2008. Though the ICO have regular dialogue with BT, and have had discussions regarding the potential DPA and PECR implications of possible commercial initiatives, BT had not informed ICO of its plans to carry out the trials of Phorm technology.

ICO contacted BT and was told that BT had obtained appropriate legal advice before carrying out the trials. ICO then sought further clarification in order to examine the complaints it had received, including from two people who thought that they had been involved in the trials.

The facts of the case and the information provided by BT in response to ICO's enquiries led the ICO to conclude that, even if there had been a technical breach of the DPA or PECR, there was no evidence of harm to any individual caused by intrusion into his or her private life as a result. On this basis, the ICO determined that, in this case, a formal investigation into the trial would be an inappropriate and unjustified use of public resources and not in line with ICO's stated enforcement guidelines. BT was made aware that ICO would closely monitor future developments and expect BT to observe rigorous practices and procedures in order to ensure compliance with the DPA and PECR. Furthermore, ICO did consider and publish on its web-site its view that Phorm's products were capable of being operated in a way that is compatible with the DPA and PECR[4] based on Phorm's description of the characteristics of those products.

If an allegation of unlawful interception is made to a police force (there are 52 local police forces) it will investigate and decide, on the basis of the evidence available, whether the case should be referred to the crown prosecution service. Although there have been suggestions in the media that material on the BT trials of Phorm technology has been provided to the police, the central UK authorities cannot require information from the police on ongoing investigations or in any way influence the outcome of those investigations. At this stage it would be inappropriate to speculate on the outcome.

Q4. What remedies, liabilities and sanctions are provided for by United Kingdom law in accordance with Article 15(2) of the Directive on privacy and electronic communications which may be sought by users affected by the past trials of the Phorm technology and may be imposed by the competent United Kingdom authority including the courts?

PECR

Regulation 30 allows a person to bring a claim for compensation against any person who has contravened the requirements of PECR.

[4] http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/phorm_webwise_and_oie.aspx

Regulation 31 extends the enforcement provisions contained under Part V of the DPA and Schedules 6 and 9 to that Act to PECR.

DPA

Generally, where data processing affects the rights of individuals under the Data Protection Directive, individuals are entitled to exercise various rights under section 7, 10 and 13 of the DPA and may seek a range of remedies before the UK Courts, including requesting the rectification, blocking, erasure or destruction of relevant personal data, and making claims for compensation.

The UK has recently introduced changes under the Criminal Justice and Immigration Act 2008 to further increase the powers of the Information Commissioner under the DPA.

RIPA

Interception of communications without lawful authority is a criminal offence by virtue of section 1 of RIPA for all public communications networks. Section 2 of RIPA provides for a similar offence within private networks. The police forces are the competent authorities for investigating allegations of offences and the Crown Prosecution Service is the competent prosecuting authority. Proceedings can be instituted with the consent of the Director of Public Prosecutions in England and Wales. RIPA provides for an offence of up to two years imprisonment or a fine.

Q5. According to the information available to the United Kingdom authorities, what exactly will be the methodology followed by the ISPs in order to obtain their customers' consent for the deployment of "Phorm" technology in accordance with the relevant legal requirements and what is the United Kingdom authorities' assessment of this methodology?

Since it became aware of BT's trials of the technology provided by Phorm, the ICO has had detailed discussions with both BT and Phorm regarding their obligations under the DPA and PECR. These discussions covered the definition of consent included in the Data Protection Directive and consideration of the practicalities involved in obtaining customer consent. The ICO is not aware of and has not seen a precise methodology to be followed by BT or other ISPs. If asked to do so, the ICO will comment on the suitability of particular methodologies, but its main role is to seek to ensure that organisations are aware of the need to take steps to comply with their legal obligations.

Further to the publication of an article on "The Register" web-site on 12 August, which included a copy of the Commission's letter (that was disclosed by an unidentified source), BT wrote to the Department for Business with its views. Accordingly, we are able to inform the Commission about BT's future plans, as they were set out in that letter. BT stated that it will shortly commence a technical test involving approximately 10,000 of its broadband users who will be invited to participate on an opt-in basis. BT will announce the trial details 24 hours in advance. BT stated that invitations for the trial will be issued anonymously via a special webpage in the

users' web browser. Users will only be included in the trial if they accept the invitation. Furthermore, they are always in control of the system and can choose to switch it on and off as they wish (via BT's website at www.bt.com/webwise). According to BT, its exact plans and methodologies will only be firmed up after this initial test.

The ICO has not been asked to comment on the methodology to be used in this proposed trial, but it maintains its view that Phorm technology is capable of being operated in a way that does not contravene the DPA and PECR. The ICO will be closely monitoring the future use of Phorm technology. Where it is not satisfied by these developments, it possesses the power to undertake investigations, and if necessary, issue enforcement notices against any person who has contravened or is contravening the DPA and PECR. As stated above, a person's failure to comply with an Enforcement Notice may result in that person being prosecuted and fined.

Yours sincerely
Debbie Gillatt
Director, Communications Networks