The Phorm "Webwise" System - a Legal Analysis

Nicholas Bohm

23rd April 2008

Introduction

1 On 4th April 2008 Dr Richard Clayton published a technical analysis of the Phorm "Webwise" System for targeted advertising on the Internet. This paper is intended to complement Dr Clayton's note by setting out a legal analysis of the same system. References in this paper to "Clayton" are to the numbered paragraphs of his note, which is at www.cl.cam.ac.uk/~rnc1/080404phorm.pdf

2 The following brief summary is from Clayton 1:

"The basic concept behind the Phorm architecture is that they wish to take a copy of the traffic that passes between an end-user and a website. This enables their systems to inspect what requests were made to the website and to determine what content came back from that website. An understanding of the types of websites visited is used to target adverts at particular users."

3 Because three of Britain's largest Internet Service Providers, BT, Talk Talk and Virgin Media, are considering whether to deploy the Phorm architecture, and because BT has already conducted trials of it involving tens of thousands of their customers (although without their knowledge), the lawfulness of such a deployment is a matter of significant public importance.

4 This paper concludes that deployment by an ISP of the Phorm architecture will involve the following illegalities (for which ISPs will be primarily liable and for which Phorm Inc will be liable as an inciter):

- interception of communications, an offence contrary to section 1 of the Regulation of Investigatory Powers Act 2000
- fraud, an offence contrary to section 1 of the Fraud Act 2006
- unlawful processing of sensitive personal data, contrary to the Data Protection Act 1998
- risks of committing civil wrongs actionable at the suit of website owners such as the Bank of England.

The effect of the legislation is addressed in detail in separate sections below.

5 But there are certain further preliminary points to be made. First, Phorm's public announcements go to great length to emphasise the anonymity it claims for its processes. These processes are embodied in software which is not open to inspection, either by the public or by the ISPs who will run the software, and Phorm can in any case change the software whenever it wishes without anyone's knowledge. Phorm's claims cannot therefore be verified, and rest entirely on placing trust in Phorm.

6 There are grounds for doubting that this trust is well placed. Whenever a participating user visits a website, her ISP uses Phorm's processes to carry out an elaborate masquerade described at Clayton 8 to 26. Its effect is to enable the ISP to place a cookie on the user's computer in a form which makes it appear to have been placed by the website to be visited. It contains a unique identifier, the Phorm UID, which acts as a pseudonym for the user and enables her browsing to be recognised as hers whenever she visits that site again. Although the Phorm system attempts to remove the cookie before it is sent to the visited site on a later visit, this attempt does not always succeed. If parts of the visited site use the HTTPS protocol for secure browsing, the cookie containing the Phorm UID will be sent to the site, where the UID can be read; and if a webmaster wishes to do so, he can read the UID in any case using Javascript. The result is that any site which holds any personally identifying information about a user, and many do, can associate that information with the Phorm UID and indeed also with the user's IP address visible to the site. In view of this, Phorm's claims for the anonymity of its processes are, to put it no higher, a considerable exaggeration.

7 In these circumstances a legal analysis of Phorm's processes is not just an inquiry into technicalities. The Phorm system presents real risks to the compromise of its users' privacy by unknown third parties in any part of the world where the marketability of personal information linked by a Phorm UID may not be restrained by effectively enforced data protection or privacy laws. There are good reasons why those who commit breaches of the legislation mentioned above can face serious consequences.

8 Finally, there is the Home Office note dated January 2008, published on 11th March 2008 on the ukcrypto mailing list by Mr Simon Watkin of the Home Office. It expresses certain views about the legality of targeted advertising on the Internet in the light of the Regulation of Investigatory Powers Act 2000 ("RIPA"), although Mr Watkin subsequently made the points that

"- the note is not advice, it doesn't claim to be advice, legal or otherwise, it's just a view, and

- the note wasn't, and doesn't purport to be, based upon a detailed technical

examination of any particular technology."

Phorm have nevertheless relied on the note for comfort as to the lawfulness of their system; and the Information Commissioner has relied on it as an excuse for refusing to consider whether the Phorm system is unlawful under RIPA. In view of that reliance, this paper refers to the paragraphs of the note (as "HO Note") by way of rebuttal where necessary.

9 It is also possible that the HO Note has come to the notice of the police. At the beginning of April 2008 Mr Peter John, of Bath, made an online enquiry to Avon and Somerset Police about whom to approach with a complaint under RIPA. On 8th April 2008, not having received a response to his enquiry, he made a specific complaint at the Manvers Street police station in Bath about illegal interception by BT and another ISP during the BT trial in 2006. He was interviewed in some detail by Detective Constable Richard Kitchener, to whom he provided a file of evidence. A week later he received a telephone reply to his online enquiry from Detective Inspector Simon Crisp at Feeder Road Police Station in Bristol. DI Crisp told him that he thought RIPA was a matter for the Home Office, and that in any case the police had other priorities. Following the telephone call from DI Crisp, Mr John enquired of DC Kitchener about progress, and learned that DI Mark Sanders had instructed him not to proceed with an investigation. Mr John made an enquiry to the Home Office, who told him that the Home Office did not have an investigative role to play in the matter.

10 It would have been useful to refer not only to the HO Note but similarly to the substance of the advice on these topics, legal or otherwise, obtained by BT and the other ISPs mentioned above, and by Phorm itself. None has been willing to offer any explanation of the basis on which they have been advised that use of the Phorm system is lawful, if that is indeed the advice they have received.

11 Various terms are in use to signify the person who controls the content of a website, such as website owner, website publisher, webhost and others. This paper uses "webmaster" below to mean whoever owns or otherwise controls the content of relevant websites.

The Regulation of Investigatory Powers Act 2000

12 RIPA section 1 makes it an offence, punishable by up to two years' imprisonment, for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a public telecommunication system. RIPA s2 provides that a person intercepts a communication in the course of its transmission by means of a telecommunication system if he so modifies or

interferes with the system, or its operation, or so monitors transmissions made by means of the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

13 The communications systems of major ISPs are public telecommunication systems for this purpose. Clayton at 46 to 61 describes how (according to Phorm's explanations) the content of the user's communications to a website and the website's responses are inspected and analysed by the ISP using equipment and software provided by Phorm. The output of this process is to classify the user, under the pseudonym of the Phorm UID, into one or more categories called "channels," which are used subsequently to determine which advertisements will be presented to the user when he visits a website which uses the Phorm system to decide which advertisements to show to which users.

14 Before the ISP releases information about the user to Phorm, everything is discarded except the UID, the channels and a datestamp (Clayton 58). HO Note 9 says cautiously:

"Where the provision of a targeted online advertising service involves the content of a communication passing through a filter for analysis and held for a nominal period before being irretrievably deleted – there is an argument that the content of a communication has not been made available to a person."

15 The legal question is whether information – the content of a communication – that has been processed by a machine and used to classify the user, and is then discarded, has been made available to a person other than the sender or intended recipient of the communication. HO Note 9 appears to rely on the fact that no human individual will in practice have access to the content as showing that it was not made available to a person. But if Phorm can distill from that content just the channel information it requires, it is impossible to see how the content cannot have been made available to it for that purpose. Nothing in the context suggests that "available" means "available to the human eye."

16 The courts and legal writers have varied in their views on the use of information by machines. The Law Commission argued in 2002 that "A machine has no mind, so it cannot believe a proposition to be true or false, and therefore cannot be deceived. A person who dishonestly obtains a benefit by giving false information to a computer or machine is not guilty of any deception offence." As a result of this fairly traditional view, in which the person behind the machine was ignored, the law on the point was changed by the Fraud Act 2006. Meanwhile, in 2004, the Queen's Bench Divisional Court in *O'Shea v City of Coventry Magistrates' Court* [2004] EWHC 905 (Admin) had no difficulty in

discerning that when an incitement was offered to a machine, it was being offered to the person behind the machine.

17 Common sense apart, RIPA s16 happens to put the matter beyond doubt. It deals with bulk interception authorised by the Secretary of State by warrant. In such cases, for the protection of those whose communications are caught up in bulk interception, it is laid down that only part of the material, as specified by a separate certificate, may actually be inspected. (It is assumed to be filtered from the bulk by technical means.) RIPA s16 deals with this by requiring that "the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that" certain conditions are satisfied. Material is thus treated as having been intercepted, and as having been made available to its interceptors, before any processing is applied to determine whether it is in fact to be inspected by any individual. From this it is perfectly clear that in the Phorm system, the pages that it scans have been made available, and have been intercepted, before they are subsequently discarded.

18 In these circumstances the HO Note 9 argument is bound to fail, and there has been interception when a user is classified by reference to the content of his communications. But RIPA s3 is relevant to whether that interception can be lawful. RIPA s3(1) makes it lawful if the interception has the consent of *both* sender *and* recipient (or if the interceptor has reasonable grounds for believing that it does). This raises the question of whose consent is required for the interception of communications of those using web browsers.

19 For the purpose of issues relating to interception of communications, this paper assumes that the consent of the user, the person initiating the communication, has been obtained. This is in a number of respects a doubtful assumption. There are cases where the existence of true consent is questionable: for example, where consent is derived from a change to the ISP's terms of service which the user cannot in practice reject without some material disadvantage, such as losing her existing email address; or where the user is not the ISP's customer but may be a family member, or a casual visitor to the user's home, or may connect to the user's open wireless connection. There are many cases where an ISP would have difficulty in establishing that the user had consented. But in dealing with a criminal offence where the prosecutor must prove that the ISP had no reasonable grounds for believing the user had consented, and bearing in mind that a defendant is entitled to the benefit of the doubt, it is preferable for the purposes of analysis to assume the user's consent. The consent of the other parties to the user's communications is another matter.

20 Four cases can usefully be taken separately for the purpose of analysing the consents required. The first is the use of search engines to locate content. The

second may be thought of as conventional browsing by visiting websites, reading their content and carrying out transactions with the webmaster. The third is the use of web-based email to communicate with third parties through a website which hosts email processes. The fourth is the use of websites hosting discussion forums or social networking sites, where the user can read or view materials placed by third parties, and can place material of his own for the use of third parties.

21 The process in all cases is as described in Clayton at 46 onwards. In the case of searches, the search terms sent by the user to a search engine are intercepted and analysed by the ISP using the Phorm system. This requires the consent of the provider of the search engine. Search engine providers derive revenue from advertisements based on their users' searches and on their users' selection from among search results, and they are in competition with Phorm for advertising revenues based on their customers' activities. There is not the slightest basis for supposing that they consent to the interception of their customers' communications with them, expressly or by implication, nor has any such basis been suggested. (The HO Note entirely overlooks this significant point.)

22 In the case of conventional browsing, the user who visits a website is sent a page by the site. The ISP intercepts that page and analyses it using the Phorm system. The HO Note at 15 says:

"A question may also arise as to whether a targeted online advertising provider has reasonable grounds for believing the host or publisher of a web page consents to the interception for the purposes of section 3(1)(b). It may be argued that section 3(1)(b) is satisfied in such a case because the host or publisher who makes a web page available for download from a server impliedly consents to those pages being downloaded."

(Section 3(1)(b) requires the consent of the recipient. The HO Note is mistaken in assuming that the webmaster is the recipient of the page, when of course it is the sender of the intercepted page, so that it is in fact section 3(1)(a) which is relevant. This technical misunderstanding does not affect the underlying argument.)

What the HO Note does not try to explain, however, is why the webmaster who sends a page to a user in response to a request should be taken to consent to that communication being intercepted for analysis by a third party. The fact (where it is a fact) that the webmaster is willing to send a particular page to anyone does not begin to justify the inference that it is willing have the use of that page by a particular user profiled and added to a collection of other data about that user (whether or not under a pseudonym). And it is very common for a webmaster to

personalise the pages he sends to a particular user, using cookies for one of their intended purposes, which makes the implication of consent even harder to sustain. A webmaster might, for example, offer different prices to different customers, so that the page sent to a customer would contain commercially sensitive information. In such a case there would obviously be no consent to interception.

23 Phorm may seek to contend that its system allows webmasters to prevent the pages they send to users from being examined, and that this justifies an inference that a webmaster who fails to take the necessary steps has given consent for the purposes of RIPA s3(1)(a). Perhaps surprisingly, this feature of Phorm was first publicly described at Clayton 39 to 45. Webmasters can include on their site a file called "robots.txt." This file is read by search engines and other systems that carry out automated processing of websites. It can be set to prohibit automatic processing. The Phorm system will examine the robots.txt file when a user visits a website, and will not scan the page returned by the webmaster unless the webmaster consents to automated processing of the site.

24 Any claim that webmasters who do not prohibit automatic processing thereby consent to interception cannot succeed. First, silence does not amount to consent, especially as many webmasters may be unaware of the Phorm system and its use of interception. Second, the use of robots.txt does not enable a webmaster to reject interception by the Phorm system while allowing other automatic processing. Because some automatic processing may be acceptable (for example, to enable a site to be ranked by search-engines) without any implication that interception of a page sent to a particular user is acceptable, failure to use robots.txt cannot be a consent to that interception. Third, even if robots.txt is in fact set by a particular website to exclude automatic processing, and even if the Phorm system as a result does not intercept pages sent *by* that site *to* its users, the system will nevertheless still intercept communications sent *to* that site *by* the user. The intercepted communications would include such things as search terms sent to a search-engine within the site.

25 Finally, so far as conventional browsing is concerned, there are private web pages. These are pages for which the webmaster provides a link only to persons of his choosing, without that link being published anywhere, and without the page being indexed by search-engines. The number of such pages is not known, but since this is such a common occurrence, even the most conservative of estimates would be in the millions. Any argument that their webmasters impliedly consent to their interception is not just wrong but untenable. (The HO Note overlooks their existence.)

26 Web-based email systems present a new element, since they handle

communications between the user and third parties, not just the provider of the email system. There is no possible reason for supposing that those third parties consent to their communications with the user being intercepted, or intend to authorise the host of the email system to give that consent on their behalf. Indeed, even the user who apparently consents to the use of the Phorm system by her ISP cannot easily be imagined to intend to consent to the interception of her email. The HO Note overlooks the matter entirely.

27 Phorm have tried to deal with email not by claiming that anyone consents to the interception, but by claiming that their system will not analyse emails. They maintain a blacklist to exclude web-based mail systems, containing a list of "more than 25 sites" (Clayton 38). But www.wantdbest.com/services/webmail.html alone lists 45 providers; the Yahoo directory lists nearly 100; web-based email services are provided to closed user groups by Universities, ISPs and many large companies; and Squirrelmail, one of many popular open source webmail packages, has at least 6,000 deployed systems whose login pages can be found by a Google search. Any attempt to exclude web-based email by the use of a list is condemned to obvious futility.

28 Phorm also exclude sites where the browser remembers a user name and password and supplies it with each request to avoid the need to log in again (Clayton 37). But there are many web-based email systems that do not use this "simple auth" mechanism but some other less standard system. There are also many web-based mail systems which use a secure (HTTPS) connection for the login process, but (on grounds of processing overhead) not for the exchange of email itself. The effect is that Phorm systems would be unable to detect the login process, and therefore unable to exclude the email from its analysis.

29 The inevitable conclusion is that no ISP can have reasonable grounds for believing that Phorm systems' interception processes will exclude web-based email. ISPs therefore know that the content of their users' emails will be intercepted without the consent of those who exchange email with their customers.

30 Lastly there is the use of websites hosting discussion forums or social networking sites, where the user can read or view materials placed by third parties and place material of his own for the use of third parties. If email may be seen as "one-to-one", forums are "many-to-many." There are huge numbers of such forums, of which many have private sections or otherwise restrict membership. As in the case of email, but probably on an even larger scale, communications will be intercepted by the Phorm system without the consent of the third parties to those communications.

31 Establishing that interception of communications is taking place, and that it is not made lawful by the consent of both the parties, leads to the question of whether it might be lawful under section 3(3), which provides as follows:

"Conduct consisting in the interception of a communication is authorised by this section if:

(a) it is carried out by or on behalf of a person who provides a ... telecommunications service; and

(b) it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of ... telecommunications services."

HO Note 17 says of this:

"The provision of a targeted online advertising service, contracted by an ISP as part of the service to the ISP's users, can probably be regarded as being carried out "on behalf of" the ISP for the purposes of section 3(3)(a)."

The definition of "telecommunications service" is in section 2(1):

"any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service)."

32 ISPs clearly provide a telecommunications service. What interception can be regarded as taking place "for purposes connected with the provision or operation of that service"? HO Note 18 quotes the official explanatory notes to the Act, which are not authoritative, but often provide helpful comments:

"Subsection (3) authorises interception where it takes place for the purposes of providing or operating a postal or telecommunications service, or where any enactment relating to the use of a service is to be enforced. This might occur, for example, where the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown."

This illustration, like the concluding reference to enforcement in section 3(3)(b) quoted above, suggests a close connection with operational matters.

33 The two cases of interception which are generally regarded as justified under section 3(3) are of filtering to prevent the distribution of (a) bulk unsolicited email (spam) and (b) viruses and other malicious code. (See for example the

reasoning, in a data protection context, in Opinion 2/2006 of the Article 29 Working Party.) Filtering is carried out partly by reference to the source of the material, and partly by machine-based inspection of its content. The justification in each case is wholly operational. Email would be unusable if all spam were delivered – users can from time to time receive many thousands of emails in a day. Malicious code can render users' computers useless, or more commonly turn them into sources of spam and malicious code inflicted on others. The Internet would not continue to function without persistent efforts to purge it of malicious code.

34 HO Note 18 argues:

"Examples of section 3(3) interception, very relevant to the provision of internet services, would include the examination of e-mail messages for the purposes of filtering or blocking spam, or filtering web pages which provide a service tailored to a specific cultural or religious market, and which takes place with user's consent whereby the user consents not to receive the filtered or blocked spam or consents (actively seeks) a service blocking culturally inappropriate material. The provision of targeted online advertising with the user's consent where the user is seeking an enhanced experience and the targeted advertising service provides that."

35 This argument relies on the assumption that the ISP is providing a targeted advertising service. But the suggestion in HO Note 17 that targeted advertising providers like Phorm provide their service "on behalf of" the ISP makes no commercial sense. If Phorm were acting as the agent of the ISP in providing the service, this would imply that the revenue stream earned by Phorm belonged to the ISP, not to Phorm; and that the liabilities incurred by Phorm to third parties under its contracts with them for the service were in truth liabilities of the ISP. Neither conclusion is commercially plausible, especially as ISPs cannot lightly be assumed to be willing guarantors of Phorm's obligations to its customers. It follows that the interception carried out by the ISP does not fall within the requirement of RIPA s3(3)(b), because it does not take place for purposes connected with the provision or operation of any service by the ISP, but for the purposes of the service provided by Phorm.

36 The principle that both sender and recipient must consent to an interception to render it lawful was introduced by the Act as a matter of deliberate policy. An example which might be thought equally extreme is that the consent of a kidnap victim's family is not sufficient to justify interception of their telephone calls by the police. RIPA s3(2) is however perfectly clear that such an interception is an offence against RIPA s1 unless a surveillance authorisation has been granted under Part II of the Act.

37 It is clear that the policy of the Act is to recognise the intrusiveness of the interception of communications. The authorisation of interception is hedged about with safeguards. There is no basis in RIPA s3(3) for a broad exception to the Act's newly established principle that both sender and recipient must consent to make an interception lawful.

38 The inevitable conclusion is that an ISP who operates the Phorm system will commit offences under RIPA s1 on a large scale. Phorm is inciting the commission of those offences, which is itself an offence at common law (and will be an offence under section 44 of the Serious Crime Act 2007 when it is brought into force to replace the common law offence).

The Fraud Act 2006

39 Under FA s1 the offence of fraud carries a maximum sentence of ten years' imprisonment. FA s2 provides that it is committed by anyone who dishonestly makes a false representation with the intention that by doing so he will make a gain for himself or for someone else. (It is not necessary to show that anyone was harmed, although some people may suffer adverse consequences - see below under "Incidental matters".) The representation may be express or implied. A representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

40 Clayton 8 to 11 provides a brief overview of cookies, and 12 to 33 describes in detail the steps taken by the ISP using the Phorm system. In particular, Clayton 20 shows that a dedicated machine operated by the ISP is designed to masquerade as the target of a user's web browsing activity for the purpose of writing to the user's computer a cookie purporting to be written by that target. That cookie contains the pseudonym by which the user is identified for tracking purposes when visiting the target of his web browsing.

41 The masquerade is necessary because web-browsers that conform to Internet standards will not allow cookies containing the name of a website to be written to a user's machine unless they come from that website (or from another closely related to it). In many browsers there may be further, stricter, rules set by default or at user request when parts of web pages are served from a third party machine.

42 The result is that a cookie is written by the ISP to the user's machine. The cookie contains a tracking identifier for the user, together with the name of the website which is the target of his web browsing. The machine under the ISP's control falsely pretends to be the true host of the target website. It makes that

false representation about itself in order to induce the user's web browser to accept the cookie it sets. The ISP knows that without making this false representation, the user's web browser would not accept a cookie using the name of the target website. The placing of the cookie in the name of the target website involves an implied representation that it was set by the target website, when in fact it was set by the ISP's machine. (This is made clear in RFC 2109, where paragraph 4.3.2 explains the purpose of the rule as being "To prevent possible security or privacy violations." The corresponding provisions are found in RFC 2965 paragraph 3.3.2.) The tracking of the user's web browsing is undertaken to enable Phorm and the ISP to earn increased revenues from advertising by reason of it being targeted on the user's interests.

43 This leaves only the question of whether the false representation is dishonest. That is of course a question for a jury, but it must depend at least in part on whether the user is given a proper opportunity to consider an adequately detailed, truthful and intelligible explanation of what is entailed by giving consent to the operation of Phorm's system. No such explanation is as yet offered by Phorm, BT, Talk Talk or Virgin Media. The complexity of the process revealed by Clayton makes it a challenging task to provide a simple but accurate explanation. It is notable that neither before nor since the publication of Clayton has Phorm published anything about the masquerade described by Dr Clayton. An explanation larded with exaggerated claims for the anonymity of the Phorm system might well seem dishonest. Phorm's evasive refusal to accept that a user cannot be taken to give consent merely because a subscriber fails to opt out of its system could well suggest dishonesty to a jury. The same consequence would be likely to follow from a failure to disclose that emails might be analysed in tracking the user's interests. And if users are not even told that the Phorm system is being operated, as occurred during the BT trials in 2006 and 2007, a jury would have strong grounds for inferring dishonesty.

44 On the basis of the facts presently available, an ISP operating the Phorm system will commit an offence under FA s1. Phorm will be committing the offence of incitement.

The Data Protection Act 1998

45 By DPA s1, "data" includes information which is being processed by means of equipment operating automatically in response to instructions given for that purpose; and "personal data" means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of the data controller. "Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to

be, processed.

46 An ISP who installs the Phorm system becomes the data controller of the data on which it operates. An ISP has the names and addresses of its subscribers, and can connect them with the IP addresses allocated to them from time to time. It can likewise connect those IP addresses with the UIDs allocated by the Phorm system to each user. (The fact that the ISP can make that connection is sufficient to qualify the data as personal, even if the connection is not made in normal operation of the system.)

47 The personal data about users which is analysed for the purpose of classifying them into channels for advertising purposes can include any of the following information, since it may be found in search terms they use or web pages they browse or forums they read or email they send or receive:

- their racial or ethnic origin,
- their political opinions,
- their religious or similar beliefs,
- whether they are members of a trade union,
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

As result, the data processed by an ISP in relation to an individual may include "sensitive personal data" under DPA s2.

48 Phorm and BT have made the point that data about individuals is processed in the Phorm system without being seen by any person, and is discarded as soon as classification is complete. This just serves to emphasise that personal data – perhaps sensitive personal data – is indeed being processed. That processing, however brief, must nevertheless comply with the requirements of the Act. Brevity is no defence.

49 DPA s4 requires a data controller to comply with the data protection principles set out in DPA Schedule 1. The first principle is as follows:

> Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
>
> (a) at least one of the conditions in Schedule 2 is met, and
>
> (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

50 The only condition in Schedule 3 which can be met in the case of the Phorm system is the first one, that the data subject has given his explicit consent to the processing of the personal data. (If this condition is met, then the consent condition in Schedule 2 is also met.)

51 The requirement of explicit consent obliges the data controller to obtain the user's positive approval for the processing of sensitive personal information, given in the knowledge that data of this kind will be included in the processing. It is not enough to allow the user to opt out of the processing, and to carry it out in the face of the user's inaction.

52 Each individual user must give his or her explicit consent. Consent cannot be given for them by another person (except perhaps a parent or guardian in the case of a child not old enough to understand the necessary explanations). ISPs are unlikely to be able to fulfil this requirement in a case where several individuals share a single personal computer. (With modern operating systems it is possible for each user to have a separate account, which would facilitate the obtaining of the necessary separate consents. This is not possible on some older systems still in use; and many families, especially those living in adverse social conditions, may be unable to manage the computer disciplines necessary to achieve separation in this way. And some parents may believe that they can better supervise their children's use of the Internet if a single account is shared.)

53 Because the use of the Phorm system is liable to involve offences under the Regulation of Investigatory Powers Act 2000 or the Fraud Act 2006, or both, it cannot comply with the requirement of the first data protection principle that data processing be carried out lawfully.

54 The sanctions available under the Act to prevent unlawful data processing include the use of enforcement notices to prohibit breaches of the Act. Criminal penalties apply to breaches of enforcement notices.

The Privacy Regulations

55 The Information Commissioner has drawn attention to the provisions of the Privacy and Electronic Communications (EC Directive) Regulations 2003 relating to traffic data. The regulations define "traffic data" as "any data processed for the purpose of the conveyance of a communication on an electronic communications network ... and includes data relating to the routing ... of a communication." The Regulations implement Directive 2002/58/EC, and recital 15 to the Directive specifically includes "the protocol used" as part of what constitutes traffic data.

56 PECR r7 imposes restrictions on the processing of traffic data by ISPs. But it permits processing for the purpose of providing value added services to the user. "Value added service" is defined as "any service which requires the processing of traffic data ... beyond that which is necessary for the transmission of a communication or the billing in respect of that communication". The Phorm service falls within this definition because it relies on the URL of the user's target website to place a cookie in the name of that website in his browser. Placing such a cookie is not necessary for the transmission of the communication involved.

57 One of the conditions of the permission granted by PECR r7 is that the user "has given his consent." That condition is elaborated by PECR r8(1), which requires that before such a consent is obtained, the user must first be given "information regarding the types of traffic data which are to be processed and the duration of such processing." The Information Commissioner infers that this requires the user to opt in to the Phorm service. This inference seems inescapable when it is noted that Directive 2002/58/EC relies for the meaning of "consent" on the meaning given to it in Directive 95/46/EC; and that meaning is "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement."

58 This is the same conclusion already reached above in relation to the processing of sensitive personal data. It presents ISPs with the same formidable difficulties over obtaining fully informed consent from all the different users of a single home machine. (Directive 2002/58/EC, which is implemented by PECR, draws specific attention at recital 25 to the significance of the fact that the user during a particular session may not be "the original user," i.e. the subscriber.) And since PECR r4 provides that "nothing in these Regulations shall relieve a person of his obligations under the Data Protection Act 1998 in relation to the processing of personal data," the Regulations do nothing to render lawful the processing that has already been shown above to be unlawful.

Incidental matters

59 Where offences under the Regulation of Investigatory Powers Act or under the Fraud Act are committed by companies or other bodies corporate, such as ISPs, their individual directors and managers will also be criminally liable if the offences are committed with their consent or connivance.

60 There are also civil law liability issues. A number of websites publish privacy policies which deny that their owners use cookies when the site is visited. One example is the Bank of England, whose privacy statement includes the assurance, "We do not use cookies to collect information about you."

61 The effect of Phorm's system is to place in consenting users' web browsers a cookie in the name of the site they are trying to visit. This falsely purports to have been set by the site whose name it bears, when in fact it has been set by the ISP using Phorm's system, using the process described at Clayton 13 to 20. A user who sees this cookie, but has not been given a detailed explanation of the Phorm system, will have every reason to believe that it was set by the visited site. If that site contains a privacy statement denying that it places cookies, the presence of the cookie implies that the statement is untrue, or that the promise it makes is being broken.

62 The owners of sites affected may have civil remedies for the false implication. It may be regarded as defamatory. And in cases where the name in the cookie includes a trademark, the cookie appears to be designating its tracking pseudonym, the UID, with the site owner's trademark. The ISP may therefore be seen to be passing off its tracking activities as being carried out with the authority of the site owner. This could involve an additional claim for passing off or trademark infringement. These matters are not investigated further in this paper, and are mentioned to show the wide ramifications of the use of the Phorm system.

63 I am grateful for helpful comments on an earlier draft from Ross Anderson, Richard Clayton, Peter Sommer and Martyn Thomas. Responsibility for the paper remains mine alone.