From: Watkin Simon [[redacted]@[redacted].gov.uk]
Sent: 18 April 2008 16:18
To: 'Pete [redacted]'; Knight Andrew
Cc: [redacted]; [redacted]; Knight Andrew
Subject: RE: Phorm: Request for Immediate Disclosure

Dear Mr [redacted],

You write:

> "…. it is clear your office were advising Phorm in January 2008. Well before the public announcement of agreements between Phorm and Internet Service Providers"

The Home Office was approached by a number of parties, both technology providers and ISPs, seeking a view about issues relating to the provision of targeted online advertising services, particularly their relation to Part 1 of the Regulation of Investigatory Powers Act 2000. The single response to those requests was made in the informal guidance note, dated January 2008, which was not made available to any of those parties until 4 February 2008.

> Please now inform me
>
> - Whether the Home Office were made aware of the secret trials conducted by Phorm in 2006/7

It wasn't.

> - Whether the Home Office authorised secret trials conducted by Phorm in 2006/7

The Home Office was not aware of the trials/tests.

> - When you first started advising BT and Phorm (and other ISPs)

Asked for a view we gave that view to all parties who asked for it on or after 4 February 2008.

> - What advice Police Detective Inspectors are being given by the Home Office concerning prosecutions of BT (and other ISPs)

No such advice has been sought.

I have asked my press office to communicate this response to [redacted] at TheRegister.

Simon Watkin
HOME OFFICE

> -----Original Message-----
> **From:** Pete [redacted] [mailto:[redacted]@[redacted].co.uk]
> **Sent:** 18 April 2008 6:47 AM
> **To:** Watkin Simon; Knight Andrew
> **Cc:** [redacted]; [redacted]; [redacted]
> **Subject:** Phorm: Request for Immediate Disclosure
> **Importance:** High
>
> Dear Mr Knight/Mr Watkin
>
> with respect to the item posted to the UK Crypto list below (by Mr Watkin), it is clear your office were advising Phorm in January 2008. Well before the public announcement of agreements between Phorm and Internet Service Providers.
>
> Please now inform me

- Whether the Home Office were made aware of the secret trials conducted by Phorm in 2006/7
- Whether the Home Office authorised secret trials conducted by Phorm in 2006/7
- When you first started advising BT and Phorm (and other ISPs)
- What advice Police Detective Inspectors are being given by the Home Office concerning prosecutions of BT (and other ISPs)

If I don't receive a response within 24 hours, I will commence a Freedom of Information action.

Please note that my account with my Internet Service Provider will be terminated in the next day.

Copy your response to [redacted] at "The Register",my MP [redacted], and the administrator of the BadPhorm site [redacted].

regards
Peter [redacted]

From: Watkin Simon <[redacted]@[redacted].gov.uk>
To: "'ukcrypto@chiark.greenend.org.uk'" <ukcrypto@chiark.greenend.org.uk>
Subject: Targeted Online Advertising
Date: Tue, 11 Mar 2008 18:02:53 -0000

> On Behalf Of Nicholas Bohm
> Sent: 11 March 2008 4:58 PM
>
> I now have a copy of a Home Office note dated January 2008. My source
> reports that Simon Watkin said that
> it could be distributed to whomever the source thought would like to see
> it. It is not uninteresting.
>
> It is, however, in the form of a pdf of a scanned image, and is 1 MB, so
> I don't propose to circulate it. If someone would offer to host it
> somewhere, and better still host a version converted to text, I'll
> provide a copy.

It says this:

TARGETED ONLINE ADVERTISING: INTERCEPTION OF COMMUNICATIONS OR NOT? IF IT IS, IS IT LAWFUL INTERCEPTION?

Targeted online advertising enables ISPs, web publishers and advertisers to target consumers with contextually and behaviourally relevant messages based upon real time analysis of users' browsing behaviour, and done anonymously without reference to any personally identifiable information. Equally it offers ISPs' users an enhanced user experience in terms of the advertising and marketing they may be exposed to.

2. This note offers informal guidance on issues relating to the provision of targeted online advertising services. It should not be taken as a definitive statement or interpretation of the law, which only the courts can give.

TARGETED ONLINE ADVERTISING: INTERCEPTION OF COMMUNICATIONS OR NOT?

** Do targeted online advertising services involve the interception of a communication within the meaning of sections 2(2) and 2(8) of the Regulation of Investigatory Powers Act 2000 (RIPA)? **

3. The meaning and scope of interception of communications is set out in sections 2(2) to 2(8) of RIPA.
4. Section 2(2), RIPA reads: "a person intercepts a communication in the

course of its transmission .... if, and only if he ..... 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".

5. Section 2(8), RIPA reads: "... contents of a communications are to be taken to be made available to a person while being transmitted ... [in] any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently."

6. The provision of a service to deliver targeted online advertising will tend to involve a person (an ISP and/or a targeted advertising provider on behalf of an ISP) monitoring transmissions made by means of a relevant telecommunications system so as to make some of the contents of a communication available, while being transmitted, to a person (the ISP and/or the targeted advertising provider) other than the sender or intended recipient of the communication.

7. Targeted online advertising services operate by delivering a cookie, including a unique user identity (UID), to an internet service user's computer which supports the advertising service. The UID is processed automatically in a closed system (which does not associate an IP address with the UID). The system performs an analysis of URLs and key words from web pages which allocates the UID to relevant advertising categories. Once

this analysis is completed the URLs and key words are deleted from the system. The system then uses that analysis to match advertisers' criteria and to enable ISPs' users to be targeted with advertising based on their browsing interests (which includes web pages viewed, search terms entered and responses to online advertisements).

8. For the purposes of section 2(2) and (8), "available" is likely to be taken to mean that a person could in practice obtain those contents for examination. Processing of the contents of a communication under human control will be likely to be regarded as having been made "available" to a person and will therefore have been intercepted within the meaning of RIPA.

9. 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.

10. Where the provision of a targeted online advertising service involves storing and processing the content of a communication in circumstances where it would be **technically possible** for a person to access the content that can be regarded as having been "diverted or recorded so as to be available to a person subsequently". This might include circumstances involving a proxy server analysing the request to view a web page, in the course of it being downloaded, and presenting the user with the web page and targeted advertising content.

11. Where the technology involves the user's browser executing a script to download targeted advertising content to complement a previously or near simultaneous download of a web page, it can be argued that the transmission of a communication ceased at the point the web page reaches the user's browser, that the end user's computer is not part of the telecommunications system and that the communication has not been made available to a person **while being transmitted**.

TARGETED ONLINE ADVERTISING: IS IT LAWFUL INTERCEPTION?

** To the extent that targeted online advertising services might involve interception of communications, can they be offered lawfully without an interception warrant in accordance with section 3 of RIPA? **

12. Section 3, RIPA, where relevant to targeted online advertising, creates two situations in which interception without a warrant may be lawful:

section 3(1), interception with consent and section 3(3), interception for purposes connected with the operation of the telecommunications service.

13. Section 3(1), RIPA, provides that: "conduct consisting in the interception of a communications is authorised if the communication is one which, or which that person has reasonable grounds for believing is, **both**: (a) a communication sent by a person who has consented to the interception; **and** (b) a communication the intended recipient of which has so consented."
14. The provision of a targeted online advertising service to an ISP user who has consented to receive the service should be able to satisfy section 3(1)(a). Each service will have its own relevant user agreements. Where

consent to receive targeted advertising is included in the user's contract and the user should be alerted to the possibility of opting out of the targeted online advertising service at regular intervals, 3(1)(a) is arguably satisfied.

15. 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.

16. Section 3(3), RIPA, provides that: "(3) 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 ..."

17. 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).

18. It is arguable that a targeted online advertising service can be "connected with the provision or operation of [the ISP] service". The RIPA explanatory notes for section 3(3) state: "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."
19. 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.

** Conclusion **

20. Targeted online advertising services should be provided with the explicit consent of ISPs' users or by the acceptance of the ISP terms and conditions. The providers of targeted online advertising services, and ISPs contracting those services and making them available to their users, should then - to the extent interception is at issue - be able to argue that the end user has consented to the interception (or that there are reasonable grounds for so believing). Interception is not likely to be at issue where the user's browser is processing the UID and material informing the advertising criteria.

21. Where targeted online advertising is determined and delivered to a user's browser as a consequence of a proxy server monitoring a communication to download a web page, there may be monitoring of a communication in the

course of its transmission. Consent of the ISPs' user and web page host would make that interception clearly lawful. The ISPs' users' consent can be obtained expressly by acceptance of suitable terms and conditions for the ISP service. The implied consent of a web page host (as indicated in paragraph 15 above) may stand in the absence of any specific express consent.

22. Targeted online advertising can be regarded as being provided in connection with the telecommunication service provided by the ISP in the same way as the provision of services that examine e-mails for the purposes of filtering or blocking spam or filtering web pages to provide a specifically tailored content service.

22. Targeted online advertising undertaken with the highest regard to the respect for the privacy of ISPs' users and the protection of their personal data, and with the ISPs' users consent, expressed appropriately, is a legitimate business activity. The purpose of Chapter 1 of Part 1 of RIPA is not to inhibit legitimate business practice particularly in the telecommunications sector. Where advertising services meet those high standards, it would not be in the public interest to criminalise such services or for their provision to be interpreted as criminal conduct. The section 1 offence is not something that should inhibit the development and provision of legitimate business activity to provide targeted online advertising to the users of ISP services.

HOME OFFICE
January 2008