FOI Case 9187

1 – a copy of any advice that the Home Office may have provided to Phorm Inc relating to possible criminal liability for the operation of their advertising platform in the UK, as may occur under the Regulation of Investigatory Powers Act 2000 or any other legislation.

The Home Office has not provided any advice to Phorm directly relating to "possible criminal liability for the operation of their advertising platform in the UK".

The Home Office was asked by a number of parties, including Phorm's legal representative, for a view on the compatibility of targeted advertising services with the Regulation of Investigatory Powers Act 2000.

In response to those requests the Home Office produced a note which offers informal guidance on issues relating to the provision of targeted online advertising services. The note explicitly states: "[this note] should not be taken as a definitive statement or interpretation of the law, which only the courts can give."

A copy of that note has been published at: http://cryptome.org/ho-phorm.pdf

The text of the note was also made public in an e-mail sent from a member of the Home Office to the ukcrypto mail list, on 11 March 2008, a copy of which is archived at:http://www.chiark.greenend.org.uk/pipermail/ukcrypto/2008-March/083561.html

2 – a copy of any advice that you may have provided to BT, Tiscali, Talk Talk or any other Internet Service Provider (ISP) relating to possible criminal liability for the operation of the Phorm advertising platform in the UK, as may occur under the Regulation of Investigatory Powers Act 2000 or any other legislation.

> Only the one note has been produced by the Home Office about targeted online advertising.

3 – a copy of any relevant Home Office policy statement regarding the circumstances in which advice will be provided to companies such as Phorm, or ISPs, as to the applicability of criminal statutes such as the Regulation of Investigatory Powers Act 2000.

There is no such policy statement. The Home Office deals with many enquiries and correspondence from Members of Parliament, members of the public and from private companies seeking information.

Working to protecting the public, part of the role of the Home Office is to help industry understand threats to public safety and law enforcement from emerging technologies and to work with business in order to achieve a workable balance between commercial and public safety interests. The Home Office welcomes companies sharing sensitive ideas and proposals in commercial confidence if that means public safety considerations and potential legal obligations can be taken into account in the conception of new products and services.

However in a free market, providers of goods and services need only ensure they are compliant with relevant legislation, and it is not a role of the Home Office to provide legal advice for that purpose.

4 – a copy of any correspondence held by the Home Office, about the provision of advice to Phorm Inc, or any ISP, or any other entity which relates to the expression of an opinion about the lawfulness of the operation of the Phorm advertising platform within the UK.

See Annex A.

5 I am requesting all such correspondence, including without limitation, correspondence with Phorm, with any ISP, with any other Government department, including BERR, CESG and GCHQ, as well as any internal Home Office correspondence.

See Annex A.

6 – details of any face-to-face meetings held with Phorm employees.

Two members of the Home Office met with representatives of Phorm Inc and their legal representatives on 23 August 2007.

7 – any minutes that may have taken of telephone conversations held with Phorm employees.

There are none.

8 – details of any face-to-face meetings with ISPs, other Government Departments, or any other entity which discussed the lawfulness of the operation of the Phorm advertising platform.

There have been none.

9 – a copy of any minutes of the meetings of the Intelligence and Security Liaison Group (or subsequent renamings of this entity) or other ISP industry liaison meetings, that relate to the operation of the Phorm advertising platform.

There have been none.

Annex A

Home Office official to Phorm's legal representative (16/08/2007)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 16 August 2007 5:37 PM
To: ***
Subject: RE: Phorm and RIPA

***,

We now both have our holidays out of the way. ***. However I'm back and have gone through the 572 e-mails that greeted me.

Given the various interested parties seeking our view on the compatibility of the Phorm service with Part I of RIPA I have concluded that it needs a more learned consideration than I can give it. I have sought advice from my own lawyer. My personal view accords with yours that, even if it is "interception", which I'm doubtful of, it is lawfully authorised under section 3 by virtue of the user's consent obtained in signing up to the ISPs terms and conditions.

What I would find helpful, and my legal adviser might also, would be a presentation on how it works (whether on paper or in personal). Would that be possible?

***

***
Home Office
2 Marsham Street
LONDON
SW1P 4DF
Tel: 020 7035 ****

Phorm's legal representative to Home Office official (04/9/2007)
Redaction made under sections 40 and 43

-----Original Message-----
From: *** [mailto:***@***.com]
Sent: 04 September 2007 3:05 PM
To: ***
Subject: FW: Phorm Inc

***,

Further to my message below, it seems the *** meeting has been put back a week.

Any chance of getting your letter before then?

Kind regards

***

Home Office official to Phorm's legal representative (12/11/2007)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 12 November 2007 10:43 PM
To: ***
Subject: RE: Phorm

***,

I should be able to complete what I'm proposing to send you tomorrow.

***
Home Office
☎ 020 7035 ****

Phorm's legal representative to Home Office official (15/11/2007)
Redaction made under sections 40 and 43

-----Original Message-----
From: *** [mailto:***@***.com]
Sent: 15 November 2007 11:43 AM
To: ***
Subject: RE: Phorm

***,

You're obviously very busy (as I saw from the timing on your email) - but any chance of getting your letter this week?

Regards

***

Phorm's legal representative to Home Office official (10/12/2007)
Redactions made under sections 40 and 43

-----Original Message-----
From: *** [mailto:***@***.com]
Sent: 10 December 2007 5:02 PM
To: ***
Subject: RE: Phorm

***,

Thanks; sorry to hassle you.

Can you also confirm that, based on what has been presented to you, HO has no objection to the marketing and operation of the Phorm product in the UK?

Regards

***

Phorm's legal representative to Home Office official (04/01/2008)
Redactions made under sections 40 and 43

-----Original Message-----
From: *** [mailto:***@***.com]
Sent: 04 January 2008 11:10 AM
To: ***
Subject: FW: Phorm

***,

Happy New year to you.

Can we start 2008 on a positive note by you sending me the short email requested below, please?

Your message of 7 December doesn't quite say that and I don't think there's a huge leap to add that; certainly Leading Counsel is clear on that score.

Regards

***

> -----Original Message-----
> **From:** *** [mailto:***@***.com]
> **Sent:** 10 December 2007 5:02 PM
> **To:** ***
> **Subject:** RE: Phorm
>
> ***,
>
> Thanks; sorry to hassle you.
>
> Can you also confirm that, based on what has been presented to you, HO has no objection to the marketing and operation of the Phorm product in the UK?
>
> Regards
>
> ***

Home Office official to Phorm's legal representative (22/01/2008)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 22 January 2008 4:00 PM
To: ***
Subject: RE: Phorm

***,

I should be grateful if you would review the attached document, and let me know what you think. I would appreciate that you not distribute it more widely at this time.

I'm sorry not to have come back on this before now. I'm sure you'll appreciate the complexities involved and the importance which will be attached to whatever we say, by your clients, their clients, and by your clients competitors (which is why I've not written it specific to Phorm but to the general principle).

***

***

***
Office of Security and Counter Terrorism | OSCT
LONDON
020 7035 ****

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 create an online broadcast network to market to advertisers and content creators a way to target consumers for 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.

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)?

2. The meaning and scope of interception of communications is set out in sections 2(2) to 2(8) of RIPA.

3. 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".*

4. 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."*

5. 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.

6. 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).

7. For the purposes of section 2(2), "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. The wording in section 2(8) *"recorded so as to be available to a person subsequently"* should be read, given the terms of the offence of unlawful interception in section 1, as recorded with the intention that they be available to a person subsequently.

8. 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.

9. 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 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*.

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.

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:

- 3(1), interception with consent under section 3(1); and
- 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). Each service will have 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) is arguably satisfied.

15. A question arises as to whether a targeted online advertising provider need argue that they have reasonable grounds for believing the host or publisher of a web page consents to the interception. It can be argued that 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 as relevant:

> *"(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 tailors 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. That two party consent is recognised as impractical in practice.

22. Targeted online advertising, as a part of telecommunications services, 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 that conduct or for it to be interpreted as criminal conduct.

23. 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

Home Office policy to Phorm's legal representative (23/01/2008)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 23 January 2008 4:01 PM
To: ***
Subject: RE: Phorm

***,

Thanks for reading through the draft paper carefully annd for your comments, with which I had no problems. I've marked up the attached revision with tracked changes.

If we agree this, and this becomes our position do you think your clients, and their prospective partners will be comforted…..

***

***
Office of Security and Counter Terrorism | OSCT
LONDON
020 7035 ****

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.

Deleted: to create an online broadcast network to market to advertisers and content creators a way

Deleted: for

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)?

2. The meaning and scope of interception of communications is set out in sections 2(2) to 2(8) of RIPA.

3. 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".*

4. 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."*

5. 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.

6. 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).

7. For the purposes of section 2(2), "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. The wording in section 2(8) *"recorded so as to be available to a person subsequently"* should be read, given the terms of the offence of unlawful interception in section 1, as recorded with the intention that they be available to a person subsequently.

8. 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.

9. 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 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*.

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.

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:

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

Deleted: under section 3(1)

Formatted: Font: (Default) Times New Roman

Formatted: Indent: Left: 18 pt

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). 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) is arguably satisfied.

15. A question arises as to whether a targeted online advertising provider need argue that they have reasonable grounds for believing the host or publisher of a web page consents to the interception. It can be argued that the host or publisher who makes a web page available for download from a server impliedly consents to those pages being downloaded.

Deleted:

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

Deleted: as relevant

> *"(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

Deleted: s

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) would stand in the absence of any specific express consent.

Deleted: That two party consent is recognised as impractical in practice.

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. Where targeted online advertising is 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.

Deleted: T

Deleted: , as a part of telecommunications services,

Deleted: conduct

Deleted: it

Deleted: ¶
¶
23.

HOME OFFICE

January 2008

Home Office official to Phorm's legal representative (01/02/2008)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 01 February 2008 2:51 PM
To: '***'
Subject: Targeted Online Advertising

***,

I should be grateful if you would review the attached document, and let me know what you think. I would appreciate that you not distribute it more widely at this time.

***,

Not too much change. I've add a disclaimer at a paragraph 2. All the paragraphs now have consecutive numbers, paragraph 11 was missing before! And paragraphs 9 and 10 (I think) are reversed.

If you can agree this, I can issue it to you properly for you to send to whomsoever you wish (and I'll be doing similarly).

***

***
Office for Security and Counter Terrorism | OSCT
HOME OFFICE
020 7035 ****

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 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:

- 3(1), interception with consent; and
- 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

Home Office official to Phorm's legal representative (04/02/2008)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 04 February 2008 10:45 AM
To: ***
Subject: Targeted Online Advertising

***,

As promised. Hard copies follow in the post.

***

***
Office for Security and Counter Terrorism | OSCT
HOME OFFICE
020 7035 ****

Enclosures: Documents A and B

Home Office official to a third party's legal representative (04/2/2008)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 04 February 2008 11:08 AM
To: ***; ***
Subject: Targeted Online Advertising

***, ***

You were in touch about to the provision of targeted online advertising services in the UK. You were interested in the view of the Home Office on your clients' proposal for the roll out of an internet based advertising service in the UK. I am now able to let you have our considered view.

Please feel free to make the attached document available to your clients, who may in turn share it with their clients and prospective clients.

***
Office for Security and Counter Terrorism | OSCT
☎ 7035 ***

Enclosure: Document B

Home Office official to a third party's legal representative (04/2/2008)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 04 February 2008 4:37 PM
To: ***
Subject: Targeted Online Advertising

***,

You were in touch some while ago about to the provision of targeted online advertising services in the UK. You were interested in the view of the Home Office on an offering proposed by Phorm Inc. I am now able to let you have our considered view. I should emphasise this is intended to address the provision of targeted online advertising services in general rather than about the services that Phorm is offering specifically. Feel free to share this document as you wish.

***

Hope to see you around.

Best wishes

***

***
Office for Security and Counter Terrorism | OSCT
☎ 7035 ****

Enclosure: Document B

Home Office official to a third party's legal representative (04/2/2008)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 08 February 2008 11:16 AM
To: ***@***.com
Cc: ***@***.com
Subject: Targeted Online Advertising

***,

Thank you for your letter of 19 November about ***'s proposal to deliver targeted online advertising to its internet subscribers. As you know we have, for some time, at the request of prospective suppliers of targeted online advertising services and ISPs interested in such services, been interested in the view of the Home Office on the issues around the provision of such services. I am now able to let you have our considered view.

I should emphasise this view is intended to address the provision of targeted online advertising services in general rather than any specific offering.

***
Office for Security and Counter Terrorism | OSCT
☎ 7035 ****

Enclosure: Document B

Home Office official to Home Office colleagues (04/2/2008)
Redaction made under sections 40 and 43

-----Original Message-----
From: ***
Sent: 08 February 2008 11:24 AM
To: ***
Cc: ***; ***;
Subject: Targeted Online Advertising

***,

This is to let you know that I have sent the paper on targeted online advertising services, which *** and I agreed, to those who were asking for our view: *** (on behalf of Phorm Inc) and *** (on behalf of ***), both providers of the advertising technology, and two ISPs, *** and ***.

***

***
Office for Security and Counter-Terrorism | OSCT
☎ 7035 ****

Enclosure: Copies of the four e-mails dated 04/02/2008 addressed to Phorm's legal representative and third parties' legal representatives

Document A

Home Office

Covert Investigation Policy Team
Crime Reduction and Community Safety Group
2 Marsham Street, London SW1P 4DF
Direct number: 020 7035 [redacted] Switchboard 0870 000 1585 Fax 0870 336 [redacted]
E-mail: [redacted]@homeoffice.gsi.gov.uk Website: www.homeoffice.gov.uk

[redacted]

LONDON
[redacted]

4 February 2008

Dear [redacted]

TARGETED ONLINE ADVERTISING

You and I have been in touch for some time about issues relating to the provision of targeted online advertising services in the UK. You were interested in the view of the Home Office on your clients' proposal for the roll out of an internet based advertising service in the UK.

I am now able to let you have our considered view. Please feel free to make the attached document "Targeted Online Advertising: interception of communications or not? If it is, is it lawful interception?" available to your clients, who may in turn share it with their clients and prospective clients.

Yours sincerely

[redacted]

Document B

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 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:

- 3(1), interception with consent; and
- 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