E-mail Message

S40

Cc:
Sent: 04/02/2010 at 14:11
Received: 04/02/2010 at 14:11
Subject: RE: Ref. IRQ0290193 - FOI Case for information between MoJ and ICO re: Infraction proceedings

Thanks S40

Yes, that reflects our conversation. We agreed that we could give out details that an series of emails were exchanged between us after that, but not the content of those emails as it could prejudice international relations.

S40 if you need to discuss, please contact me.

S40

S40
Sent: 04 February 2010 14:09
To: casework
S40
Subject: Ref. IRQ0290193 - FOI Case for information between MoJ and ICO re: Infraction proceedings
Importance: High

Dear S40

Thank-you for your emails of 29 January and 3 February in relation to a recent FOI request that has been received in the ICO. As you probably established - I been out of the office, today has been my first day back so hope that these comments reach you in time.

I have spoken with S40 today and also had a meeting with him on 26 January, with regard to this FOI case. We discussed the issues at hand, and were in agreement that it would not be suitable for any of the emails or attachments to be released except that of the 12th January sent from S40 titled 'Summary of RIPA and DPA' at 15:43. This is due to the fact that a lot of the further discussions after this initial email have been used to reply to the European Commission regarding the Infraction. These documents sent between the UK Government and the European Commission are confidential and have been exempt under section 27 of the FOIA for the prejudicial effect on international relations. If you need more information regarding why and how we have reached this decision, I would be happy to send you some further text/information.

I have copied S40 into this email, as he may have more to add to reflect our discussions. In any event, I would be happy to discuss in further details at any time.

Kind regards,

S40

S40

Out of Scope

E-mail Message

S40

Cc:
Sent: 03/02/2010 at 09:32
Received: 03/02/2010 at 09:32
Subject: IRQ0290193,ICO[Ref. IRQ0290193]

Attachments: further email for consultation,MoJ.htm

3rd February 2010

Case Reference Number IRQ0290193

Dear S40

Further to my email of 29 January 2010, please find attached another email that we are considering for disclosure. Your views would be greatly appreciated as explained in my previous email.

Please contact me S40 if you need to discuss any aspect of this request.

Yours sincerely

S40

Out of Scope

S40

Sent: 14 January 2010 10:23
To:
Cc:
Subject: RE: DPA & RIPA lines

Importance: High

S40

Thanks for this. It does seem to leave out the rub of the issue, which is that the ICO are not in a position decide whether an interception is lawful or not, limiting any action we can take beyond that if other DP provisions are met is. Our concern is that the form of words without our revisions might give the impression that the ICO would be in the position to decide the lawfulness of an interception.

To that end we have expanded on your form of words a little. Changes in blue.

S40

Information Commissioner's Office, Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

S40

www.ico.gov.uk

S40

Sent: 13 January 2010 16:06
To: S40
Cc:
Subject: DPA & RIPA lines
Importance: High

S40

Thanks to both you and S40 for sending over the lines on the DPA and RIPA. As we discussed earlier – we are looking for something a lot shorter. The paragraphs below are largely taken from the text that you sent us, with a few tweaks. I would be very grateful for your thoughts and comments by tomorrow morning.

Out of Scope

Kind regards,

S40

The Information Commissioner's Office (ICO) is the independent supervisory body that regulates the processing of personal data across all subject areas, wherever the Data Protection Act 1998 (DPA) applies.

The Regulation of Investigatory Powers Act 2000 (RIPA) is the main legislation regulating the interception of communications. The ICO has no statutory responsibility in relation to the regulation of 'interception' as defined and prohibited in RIPA. However it is recognised that both DPA and RIPA together form part of the framework of regulation that limits excessive surveillance and provides safeguards for individuals. Where an interception involves the processing of personal data the ICO is empowered to regulate that processing and investigate whether the processing in interception complies with the 8 Data Protection Principles. However, the ICO is not itself in a position to determine whether an interception is unlawful under RIPA.

The Information Commissioner's interest stems from the connection between RIPA and the DPA. The first data protection principle states that processing of personal information must be fair and lawful. Any processing of personal information which is in contravention of the provisions of section 1(1) of RIPA would also be a breach of the first principle. Where there has been an authoritative declaration that an interception is unlawful (for example by the Courts) the ICO will then be able to intervene on the basis that the associated processing of personal data is unlawful.

S40

Information Policy Division | Ministry of Justice

S40

E-mail Message

S40

Cc:
Sent: 29/01/2010 at 09:31
Received: 29/01/2010 at 09:31
Subject: IRQ0290193,consultation[Ref. IRQ0290193]

Attachments: Doc1.doc.doc
FW_ The Remit of the ICO with regards to the Data Protection Act 1998, consultation info.html
Belinda Lewis letter to David Smith re ICO remit in DPA & RIPA.pdf, consultation info.pdf
FW_ DPA & RIPA lines,consultation info.html
FW_ DPA & RIPA lines, consultation info.html
Covering email to RIPA and DP.html

29th January 2010

Case Reference Number IRQ0290193

Dear S40

The Information Commissioner's Office has received a request for information which has been passed to the Internal Compliance Team for action.

The requestor has asked us for all the information which we hold regarding correspondence with government departments in relation to the infraction proceeding regarding the implementation of PECR in the last 3 months.

In accordance with the requirements of the Freedom of Information Act 2000, we need to ensure that we provide him/her with all the information to which s/he is entitled. Although we are exempt from disclosing certain types of information, it is in the public interest that we are open, transparent and accountable for the work that we do.

Therefore, (given your close involvement with this case) we would be grateful if you could let us know if any of the information you have provided to the ICO on behalf of the Ministry of Justice in relation to this request should not, in your view, be provided to him/her. I should make it clear that even if it is your preference that the requestor should not see this information this may not be enough to exempt it from disclosure to him/her. Therefore, we would ask that if you do object to any of the information being disclosed to the requestor you should clearly indicate what information you would wish to be withheld from him/her, and why, so that we can take your views into account when considering his/her request.

The documents and information which are held relating to this case that have been provided to us by the MoJ, and which I have identified for possible disclosure, are:

· Email to S40 + attachment (doc.1)

· Email dated 14 January 2010 from MoJ to David Smith+ attached letter to Belinda Lewis)

Out of Scope

· String of emails dated 13 and 14 January 2010 between S40 and MoJ

· Email dated 13 January 2010 to S40

Please do contact me if you wish to discuss any other aspect of this request to the ICO. I can be contacted on S40 .I would be grateful if you can provide me with your views before 5 February 2010 to allow me to consider your views before responding to the requestor within the statutory time limit.

I am consulting with another colleague on whether any other email exists, if so, I will be sending you a copy for consultation by Tuesday.

Thank you very much for your assistance in this matter, and I look forward to hearing from you shortly.

Yours sincerely

S40

Section 1(1) of RIPA makes it an offence to “intentionally and without lawful authority” intercept any communication in the course of its transmission by means of a postal service or a public communications system. There are several means by which one can obtain lawful authority to intercept a communication. One of these is where both the sender and recipient of the communication have consented to the interception.

Section 2 of RIPA provides some definition of when an interception of communication occurs. The interception must occur in the “course of transmission” of the communication and must modify or interfere with the system or its operation; must monitor the transmissions made by use of the system; or monitor transmissions made by wireless telegraphy to or from apparatus comprised in the system. Interceptions of communications do not include references to the interception of communications broadcast for general reception.

This approach to the meaning of “interception” is relatively easy to apply in the context of traditional telephony. However, this concept and the concept of both the “sender” and “recipient” consenting is less easy to apply to internet based communications, particular when dealing with transmission of information between a website and an individual’s personal computer. On the one hand this can, in some circumstances, leave those developing internet based services exposed to the risk of criminal prosecution even if these services pose little or no threat to privacy. On the other hand the development of some otherwise acceptable services may be curtailed because the developers are not prepared to take the risk of committing the criminal offence of interception.

This issue has been brought into greater focus by the development of targeted online advertising (TOLA). Phorm has developed a system where, with the cooperation of an individual’s ISP they can profile the addresses and certain content of websites visited by users and then use that information to match that user against predefined broad advertising categories. The ICO is aware that other products are being developed which could operate in a similar way. Indeed some such as Gmail, which scans the content of subscribers’ email, are already in operation.

Exponents of TOLA state that the user profiling occurs with the knowledge and agreement of customer and within the technological infrastructure of the ISP and that the advertising and profiling can take place in such a way that there is no need to know the identity of the individual users.

The problem is that there is confusion over whether the operation of individual TOLA systems constitute an “interception of a communication” under RIPA and, if it does, can companies imply the consent of the website the individual visits to justify the interception?

Effectively, this means that if an organisation develops a product where its operation might be seen as an interception of a communication, they have nowhere to turn for advice.

The Information Commissioner’s interest stems from the connection between RIPA and the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations. The first data protection principle states that processing of personal information must be fair and lawful. Any processing of personal information which is in contravention of the provisions of section 1(1) of RIPA would also be a breach of the first principle. Understandably organisations approach the ICO for advice. However, it is inappropriate and arguably beyond

his powers for the Information Commissioner to advise on the nuances of RIPA. He does not have particular expertise in this area. Furthermore, this advice could expose those seeking it to criminal prosecution, given that the Information Commissioner is not the prosecuting authority for offences under RIPA.

PECR…..

Section 57 of RIPA creates the role of Interception of Communications Commissioner, but his role is limited to overseeing the persons who issue warrants, and the procedures of those who are acting under warrant or who are assisting those acting under warrant. RIPA places no duty on the Interception of Communications Commissioner to provide advice to those who want to ensure they are acting in a manner which is in compliance with RIPA, nor is he resourced to provide such advice.

The Interception of Communications Commissioner has no remit to investigate complaints about those bodies outside RIPA who have contravened the requirements for “lawful interception” of communications. This also applies to the Investigatory Powers Tribunal. Effectively, what this means is that where the private sector, either through their own provision of services, or through being placed under a legal obligation, are intercepting communications of services users, there are gaps in the regulatory regime. The only recourse for a private sector breach is prosecution for a criminal offence. In many cases it is arguable whether there would be a public interest in pursuing these prosecutions, but this accentuates the gaps in the regulatory regime.

This situation is different from the position that applies to the public sector. Arguably there is a need for an appropriately empowered regulator, who can provide advice and guidance and ultimately impose civil sanctions against private sector players.

The Home Office has issued general guidance on the operation of RIPA in relation to targeted online advertising, but this general statement did not address the specific concerns about the operation of individual TOLA systems, or the technical issues around whether the specific actions of such systems would constitute an interception of communications.

In contrast, when the ICO is approached for advice as to the application and applicability of data protection law, the ICO is empowered to provide such advice under section 51of the Data Protection Act 1998. Indeed, the ICO is under a specific obligation to promote the following of good practice which includes but is not confined to compliance with the requirements of data protection law. The problem is that whilst the DPA and RIPA together form part of the framework of regulation that limits excessive surveillance and provides safeguards for individuals it is only in relation to the DPA that there is an organisation charged with promoting compliance with the legislation and with providing authoritative advice to those who need it.

S40

Sent: 14 January 2010 18:58
To: David Smith
Cc: Lewis, Belinda; S40
Subject: The Remit of the ICO with regards to the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000
Importance: High

Dear David,

Please find attached a letter from Belinda Lewis. This is following recent discussions between officials, regarding the Infraction Proceedings against the UK Government. We would be very grateful for a response by close of play tomorrow.

Kind regards,

S40

S40

Information Policy Division | Ministry of Justice

S40

Ministry of JUSTICE

Belinda Lewis
Head of Information Policy Division
102 Petty France
London
SW1H 9AJ
S40

www.justice.gov.uk

David Smith
Deputy Commissioner
Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow,
Cheshire,
SK9 5AF, UK

14 January 2010

Dear David,

RE: THE REMIT OF THE ICO REGARDING THE INTERACTION BETWEEN THE DATA PROTECTION ACT 1998 AND THE REGULATION OF INVESTIGATORY POWERS ACT 2000

Thank you for your support and help with the several queries we have had regarding the scope of the Information Commissioner's remit in respect of the Data Protection Act 1998 (DPA) and the Regulation of Investigatory Powers Act 2000 (RIPA). As you know, these queries stem from the recent Infraction Proceedings against the UK Government on the transposition of Electronic Communications and Privacy Directive 2002.

We have drafted the following paragraphs on the basis of our exchanges to reflect the nature of the ICO's remit in this area. I would be grateful for your written comments on the text below:

The Information Commissioner's Office (ICO) is the independent supervisory body that regulates the processing of personal data across all subject areas, wherever the Data Protection Act 1998 (DPA) applies.

The Regulation of Investigatory Powers Act 2000 (RIPA) is the key legislation regulating the interception of communications. The ICO has no statutory responsibility in relation to the regulation of 'interception' as defined and prohibited in RIPA.

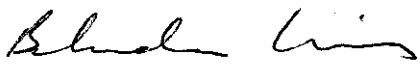
However, it is recognised that together the DPA and RIPA form part of the framework of regulation that limits excessive surveillance and provides safeguards for individuals. While the ICO is not empowered to determine whether an interception is lawful under RIPA, the ICO

may regulate that processing and consider whether it complies with the eight Data Protection Principles where an interception involves the processing of personal data.

The first Data Protection Principle states that processing of personal data must be fair and lawful. Therefore, where an interception involves the processing of personal data, the ICO is empowered to consider whether the processing meets this requirement. An example might be where a court has ruled that a particular interception is in contravention of the provisions of section 1(1) of RIPA, and that interception also involved the processing of personal data. In such a case, the ICO could rule that the breach of RIPA indicates that the processing is in breach of the first Data Protection Principle, on the grounds that it is unlawful. In this situation, the ICO could take appropriate action against the data controller.

Please do not hesitate to contact me or any member of the domestic data protection team to discuss this further if that would be helpful.

Yours sincerely,



Belinda Lewis

Sent: 14 January 2010 11:08
S40
Subject: FW: DPA & RIPA lines
Importance: High

S40

Thank you for your patience and help on this. As you can see from the red text below, the main substance is the added sentence in the last paragraph. I would be grateful to receive any comments you may have, as soon as possible. We are aiming to get the text to Home Office by midday.

Kind regards,

S40

S40
Information Policy Division | Ministry of Justice
S40

S40
Sent: 14 January 2010 10:23
To: S40
Cc: David Smith
Subject: RE: DPA & RIPA lines
Importance: High

S40

Thanks for this. It does seem to leave out the rub of the issue, which is that the ICO are not in a position decide whether an interception is lawful or not, limiting any action we can take beyond that if other DP provisions are met is. Our concern is that the form of words without our revisions might give the impression that the ICO would be in the position to decide the lawfulness of an interception.

To that end we have expanded on your form of words a little. Changes in blue.

Out of Scope

S40

S40

Information Commissioner's Office, Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

S40

www.ico.gov.uk

S40

Sent: 13 January 2010 16:06
To: S40
Cc:
Subject: DPA & RIPA lines
Importance: High

S40

Thanks to both you and S40 for sending over the lines on the DPA and RIPA. As we discussed earlier – we are looking for something a lot shorter. The paragraphs below are largely taken from the text that you sent us, with a few tweaks. I would be very grateful for your thoughts and comments by tomorrow morning.

Kind regards,

S40

The Information Commissioner's Office (ICO) is the independent supervisory body that regulates the processing of personal data across all subject areas, wherever the Data Protection Act 1998 (DPA) applies.

The Regulation of Investigatory Powers Act 2000 (RIPA) is the main legislation regulating the interception of communications. The ICO has no statutory responsibility in relation to the regulation of 'interception' as defined and prohibited in RIPA. However it is recognised that both DPA and RIPA together form part of the framework of regulation that limits excessive surveillance and provides safeguards for individuals. Where an interception involves the processing of personal data the ICO is empowered to regulate that processing and investigate whether the processing in interception complies with the 8 Data Protection Principles. However, the ICO is not itself in a position to determine whether an interception is unlawful under RIPA.

S40

S40

Sent: 13 January 2010 16:06
To: S40
Cc:
Subject: DPA & RIPA lines
Importance: High

S40

Thanks to both you and S40 for sending over the lines on the DPA and RIPA. As we discussed earlier – we are looking for something a lot shorter. The paragraphs below are largely taken from the text that you sent us, with a few tweaks. I would be very grateful for your thoughts and comments by tomorrow morning.

Kind regards,

S40

The Information Commissioner's Office (ICO) is the independent supervisory body that regulates the processing of personal data across all subject areas, wherever the Data Protection Act 1998 (DPA) applies.

The Regulation of Investigatory Powers Act 2000 (RIPA) is the main legislation regulating the interception of communications. The ICO has no statutory responsibility in relation to the regulation of 'interception' as defined and prohibited in RIPA. However it is recognised that both DPA and RIPA together form part of the framework of regulation that limits excessive surveillance and provides safeguards for individuals. Where an interception also amounts to the processing of personal data the ICO is empowered to regulate that processing and investigate whether the processing in interception complies with the 8 Data Protection Principles.

The Information Commissioner's interest stems from the connection between RIPA and the DPA. The first data protection principle states that processing of personal information must be fair and lawful. Any processing of personal information which is in contravention of the provisions of section 1(1) of RIPA would also be a breach of the first principle.

S40
Information Policy Division | Ministry of Justice

S40

S40

Sent: 12 January 2010 15:43

S40

Subject: Summary of RIPA and DPA

S40

S40 has asked me to forward you the following summary of RIPA and DPA and who does what. There is nothing in it on PECR at present as it is basically a distillation of our evidence to the Home Affairs Committee for their "A Surveillance Society?" inquiry and the Home Office's consultation on the IMP.

Have a look and see what you can use. S40 has said if you need something on PECR as well, then get in touch.

S40

Information Commissioner's Office, Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

S40

www.ico.gov.uk

S40

Sent: 12 January 2010 15:09

S40

Subject: Document1

Here you go.

E-mail Message

S40

Cc:
Sent: 30/04/2009 at 10:58
Received: 30/04/2009 at 11:01
Subject: FW: BF 24/3 - 233262 - Letter from S40

Attachments: Phorm letter - S40 - MW changes.doc

S40
Domestic Data Protection Policy
102 Petty France
S40

S40
Sent: 27 April 2009 10:01
S40
Subject: RE: BF 24/3 - 233262 - Letter from S40

S40

Thanks for this. Michael has added some text to the final paragraph - could you confirm you are content with the version attached before it is issued?

Also, I am concerned that Michael's signature appeared again on the version that was sent up on Friday. As S40 said in his email below, although it is probably our fault that you have it you should not have it, so I would appreciate it if you could delete all copies you have and avoid putting it on future letters.

Thanks

S40

S40
Sent: 24 April 2009 15:31
S40
Subject: RE: BF 24/3 - 233262 - Letter from S40

S40

Out of Scope

Sorry - slightly later than planned a fleshed out sub. It got a bit longer than I had anticipated as the more I thought, the more I put in! But I think the content is relevant to the response and the wider context.

Thanks

S40

Ministry of Justice

S40

S40

Sent: 24 April 2009 11:06

S40

Subject: RE: BF 24/3 - 233262 - Letter from S40

Just to note I copied in the wrong S40 the message below (no excuse, really) so please don't reply all.

Thanks

S40

S40

Sent: 24 April 2009 11:01

S40

Subject: RE: BF 24/3 - 233262 - Letter from S40

Importance: High

S40

Could you give me a call to talk about how the revised sub is coming along? I haven't managed to get through to you, which I presume is due to the office move.

Thanks

S40

S40

Sent: 23 April 2009 15:05

S40

Subject: RE: BF 24/3 - 233262 - Letter from S40

Importance: High

S40

How is the revised sub going? Given the delay I'd like to put this to Michael today, if at all possible, so I'd appreciate it if you could send it to me by 4pm.

Thanks,

S40

From: S40

Sent: 22 April 2009 18:46

To: S40

Cc: Lewis, Belinda;

Subject: RE: BF 24/3 - 233262 - Letter from S40

S40

Sorry, just to add, could the revised sub include more information - that is, a summary of the issues raised in S40 letter and of the draft response. I'd appreciate it if you could copy me in when you send it up, as with all other subs on information/data issues.

Thanks

S40

S40

Sent: 22 April 2009 18:37

S40

Subject: RE: BF 24/3 - 233262 - Letter from S40

S40

Thanks for this, however, can the sub include an explanation of the delay that has occurred here (MW will ask and worth just popping in a quick apology) and also can you please delete all copies of MWs signature. Sure it is our fault you have this but you should not have it and grateful if you could avoid putting on future letters.

Out of Scope

Thanks

S40

From: S40
Sent: 22 April 2009 13:51
To: S40
Subject: RE: BF 24/3 - 233262 - Letter from S40

S40

Sorry for the delay - here is a brief sub etc

Thanks

S40

Ministry of Justice

S40

From: S40
Sent: 22 April 2009 12:42
To: S40
Subject: RE: BF 24/3 - 233262 - Letter from S40

Any news on this?

From: S40
Sent: 01 April 2009 16:09
To: S40
Subject: RE: BF 24/3 - 233262 - Letter from S40

Thanks. Probably won't get a chance to do this until tomorrow (am focussed down on a debate for Willie Bach that is taking place tomorrow am/early pm) but will get it up to you asap.

S40

S40

Ministry of Justice

S40

From: S40
Sent: 01 April 2009 16:08
To: S40
Cc:
Subject: RE: BF 24/3 - 233262 - Letter from S40

A brief one please

From: S40
Sent: 01 April 2009 16:06
To: S40
Cc:
Subject: FW: BF 24/3 - 233262 - Letter from S40

S40 is a sub required for this adr?

From: S40
Sent: 01 April 2009 16:04
To: S40
Subject: RE: BF 24/3 - 233262 - Letter from S40

S40

Sorry for the delay in getting this to you - response to S40 attached. I wasn't sure whether you wanted a sub with this - can you confirm?

Thanks

S40

Ministry of Justice

From: S40
Sent: 30 March 2009 14:40
To: S40

Subject: RE: BF 24/3 - 233262 - Letter from S40

Any news?

From: S40
Sent: 26 March 2009 14:51
To: S40
Subject: RE: BF 24/3 - 233262 - Letter from S40

Draft letter is in my inbox to check and send up to you. I'll try to get it to you either today or tomorrow, if that's ok?

S40

Ministry of Justice

S40

From: S40
Sent: 26 March 2009 14:11
To: S40
Subject: FW: BF 24/3 - 233262 - Letter from S40

Hi S40 what's the score on this adr?

S40

From: S40
Sent: 10 March 2009 16:51
To:
Cc:
Subject: BF 24/3 - 233262 - Letter from S40

Hi S40 could we please have advice and draft reply to the attached letter by 24 March (Michael did promise to write to him).

Many thanks.

S40

Michael Wills Private Office

Rt Hon Michael Wills MP
Minister of State
102 Petty France
London SW1H 9AJ

S40

E general.queries@justice.gsi.gov.uk

www.justice.gov.uk

S40

Our ref: MFD1099

April 2009

Phorm, Webwise and BT

Thank you for your letter of 8 March outlining your concerns regarding the use of behavioural advertising and in particular the company Phorm. You asked for more information concerning the Ministry of Justice's views surrounding the application of Phorm's technology.

It might be useful if I explain that the Data Protection Act 1998 (DPA) which governs the processing of personal data is administered and enforced by the Information Commissioner's Office (ICO) who are the UK's independent public body set up to promote access to official information and protect personal data. Neither Ministers nor departmental officials may intervene or comment on decisions reached by the ICO. I hope you understand, then, that I cannot comment on the application of the DPA in specific circumstances. However, it may be helpful if I briefly explain in general terms the department's response to this issue.

As you may be aware, an ICO statement of the 4 April 2008 states: "[Phorm] assure us that their system does not allow the retention of individual profiles of sites visited…and that they hold no personally identifiable information on web users." The City of London Police was asked to consider the matter and has stated: "it has been decided that no criminal offence has been committed." The Crown Prosecution Service (CPS) is currently considering whether any action needs to be taken with regards to this issue and will report on their decision shortly.

One of the key aims of the DPA is to ensure that personal data concerning any living individual is not disclosed to third parties in a manner that is not in compliance with legislation.

It is important to note that should the ICO have concerns with regard to any data controller's business practices, they have the power to assess, and where appropriate, force compliance. The ICO can currently:

- investigate whether a data controller is processing data without correct prior notification;
- issue an Information Notice where they reasonably require any information for the purpose of determining whether the data controller has complied or is complying with the DPA;
- issue an Enforcement Notice where they are satisfied that a data controller has or is contravening the DPA requiring the data controller to comply; or
- use their powers of entry and inspection under a Schedule 9 warrant, where there are reasonable grounds for suspecting that a data controller has or is contravening the DPA, or has committed an offence under the DPA.

You may be aware the Internet Advertising Bureau (IAB) has recently launched a code of practice specifically concerning behavioural advertising. Some key players including Microsoft, AOL, Google, Yahoo and Phorm have signed this code. The IAB code is designed to ensure that the behavioural advertising industry protects and educates consumers on their rights and choices. The code agrees on three key principles that set out minimum standards to ensure any company collecting or using data for behavioural advertising must:

- inform a consumer that information is being collected for this purpose;
- provide a mechanism for consumers to withdraw consent; and
- provide clear and simple information about the how information will be used and how to withdraw consent.

I trust that this information is helpful. As I said at the ICO conference, I am aware that your concerns about Phorm are more widely shared and I understand them. I shall continue to take a personal interest in these issues surrounding it as they develop in the months ahead.

MICHAEL WILLS MP

E-mail Message

From: S40

To:

Cc:

S40 Lewis, Belinda [EX:/O=HMCOURTS-SERVICE/OU=ARAMIS/CN=RECIPIENTS/CN=BLEWIS]

Sent: 18/09/2009 at 10:11
Received: 18/09/2009 at 10:11
Subject: RE: Update from discussions with the ICO re: Phorm technology

S40

Thank you for this update, which Michael has noted.

S40

From: S40
Sent: 17 September 2009 16:22
To: S40
Cc: Lewis, Belinda
Subject: FW: Update from discussions with the ICO re: Phorm technology

S40

Michael expressed his wish that I speak to the ICO regarding Phorm technology, following my submission to him on 4 September. After speaking to the relevant ICO official, it was confirmed that the Phorm lines which were in the draft correspondence reply to Annette Brooke (MC244845), are still applicable and reflect the current ICO position.

The ICO have noted several minor developments on the Phorm matter:

Firstly, BT (who originally conducted the secret Phorm trials), has announced that they have no immediate plans of rolling out Phorm technology.

Secondly, due to the fact that the main ISPs who were associated with the rollout of Phorm technology have all voiced that they will no longer be carrying this out, the ICO dont anticipate that advice in this area will need to be updated. However they are willing to keep the matter under review of any developments that cause concern.

In addition to the above, there are no other updates to note.

The statement of the ICOs opinion of Phorm technology is below:

The ICO has confirmed that it considers that targeted advertising technology is capable of being operated in compliance with the DPA and the Privacy and Electronic Communications Regulations 2003, provided that users are given clear information about the manner in which the advertising is carried out and that they are then able to make a meaningful choice over whether to allow browser details to be used by the service. It is

also the ICOs view that Phorm does not seek, nor have access to, information held by the Internet Service Provider (ISP) that could enable it to link a random user ID and profile to a living individual, and that it does not keep a record of the sites each individual has visited. Two of the ISPs who were in talks with Phorm over deployment of the technology have announced that they are not currently considering any further involvement. Further, BT have also announced that they have no immediate plans to roll out the use of Phorm's technology commercially. The ICO is keen to keep this issue under review.

Thanks,

S40

Information Policy Division | Ministry of Justice

S40

From: S40
Sent: 17 September 2009 15:11
To: S40
Cc: Lewis, Belinda; S40
Subject: RE: Update from discussions with the ICO re: Phorm technology

S40

Thanks for this. We spoke - as discussed, grateful if you could provide information in the form of an update for Michael (rather than in the context of lines on MCs).

Grateful to receive this by noon tomorrow.

Thanks

S40

From: S40
Sent: 17 September 2009 11:56
To: S40
Cc: Lewis, Belinda; S40
Subject: Update from discussions with the ICO re: Phorm technology

S40

Michael expressed his wish that I speak to the ICO regarding Phorm technology, following my submission to him on 4 September. After speaking to the relevant ICO official, it was confirmed that the Phorm lines which were in the draft correspondence reply to Annette Brooke (MC244845), are still applicable and reflect the current ICO position.

Out of Scope

E-mail Message

From: S40

To: S40 Wills, Michael (Submissions) [EX:/O=HMCOURTS-SERVICE/OU=ARAMIS/CN=RECIPIENTS/CN=MWILLS1]

Cc: Lewis, Belinda [EX:/O=HMCOURTS-SERVICE/OU=ARAMIS/CN=RECIPIENTS/CN=BLEWIS], S40
S40

Sent: 09/09/2009 at 15:31
Received: 09/09/2009 at 15:31
Subject: RE: MC 244845 - Submission on Reply to Annette Brooke's constituent's concerns regarding Phorm technology - 4 September 2009 (MC244845)

Attachments: MFD1036.PDF

S40 thank you. Letter to Annette Brooke MP sent as attached.

Regards
S40

From: S40
Sent: 04 September 2009 14:03
To: S40 Wills, Michael (Submissions)
Cc: Lewis, Belinda; S40
S40
Subject: MC 244845 - Submission on Reply to Annette Brooke's constituent's concerns regarding Phorm technology - 4 September 2009 (MC244845)
Importance: High

S40

Further to our discussion, please find attached a re-drafted version of the reply to Annette Brooke, with the related submission.

Thanks,

S40

S40

Information Policy Division | Ministry of Justice
S40

Ministry of JUSTICE

The Rt Hon Michael Wills MP
Minister of State
102 Petty France
London SW1H 9AJ

S40

E: general.queries@justice.gsi.gov.uk

www.justice.gov.uk

Annette Brooke MP
S40

Our ref: MC244845
Your ref: ab.ac.0113

4 September 2009

Dear Annette

Phorm technology

Thank you for your letter of 9 June on behalf of your constituent, who is concerned about Phorm technology and the outcome of some recent Freedom of Information (FOI) requests. I am replying further to the initial response from my department of 30 July and am sorry for the delay. I wanted to make sure that the issues that your constituent raised have been carefully investigated by policy officials across Government to ensure as full a response as possible is provided.

I am also sorry for the delay in the handling of some of the FOI requests referred to by your constituent. I would like to assure you that the Ministry of Justice (MoJ) takes its obligations under the Freedom of Information Act 2000 (FoIA) seriously. I acknowledge that the department's handling of some FOI requests has not been good enough and the MoJ has taken a number of steps to improve its performance in responding to requests within the statutory deadline. As a result, the department's performance has clearly shown an improvement in timeliness, as seen in the recently published statistics for requests received in the first quarter of this year. The department expects to see further improvements in the handling of FOI requests during 2009. The Information Commissioner's Office has been kept informed of progress and has provided helpful input.

I understand your constituent's concerns about the handling of these FOI requests. The original FOI request was received by the department on 19 November 2008 and so only information up to that date would fall within the scope of the request, as stated under section 10(1) of the FoIA, even though the request was answered much later. Further, although the information released in response to the FOI request and internal review was quite limited, this does not comprise all of the briefing that I have received on Phorm.

I am sorry that your constituent has felt entitled to question the veracity of statements I have made on this issue. If he had serious concerns about this, he might have been better advised to seek further information instead of leaping to an erroneous conclusion. For the Record, I have received both additional briefing that did not fall within the scope of the FOI request and verbal briefing on this subject. I retain a keen interest in this matter as I have said, and my interest does not stem from the allegations your constituent has made about me. I hope this will reassure your constituent and that he will now feel able to focus on the substantive issue. This is important and I welcome all dialogue about it. This is a complex and evolving area of public policy and we will only get it right through extensive dialogue with professionals and the public and your constituents clearly have a role to play in this dialogue.

Your constituent referred to the Information Commissioner's Office (ICO) in his letter and it may be helpful if I outline the role of the ICO. The Data Protection Act 1998 (DPA) governs the processing of personal data and is enforced by the ICO, independently of Government. The ICO was set up to promote access to official information and protect personal data. Neither Ministers nor departmental officials may intervene in decisions reached by the ICO. I hope you will understand, therefore, that I cannot comment on the ICO's consideration of this matter.

As your constituent may be aware, in a statement on the 4 April 2008, the ICO stated that: "*[Phorm] assure us that their system does not allow the retention of individual profiles of sites visited...and that they hold no personally identifiable information on web users.*" The City of London Police was also asked to consider the matter and noted: "*it has been decided that no criminal offence has been committed.*" MoJ officials also contacted the Crown Prosecution Service (CPS) in May this year and I understand that they are still considering whether any action is required.

The ICO has confirmed that it considers that targeted advertising technology is capable of being operated in compliance with the DPA and the Privacy and Electronic Communications Regulations 2003, provided that users are given clear information about the manner in which the advertising is carried out and that they are then able to make a meaningful choice over whether to allow browser details to be used by the service. It is also the ICO's view that Phorm does not seek, nor have access to, information held by the Internet Service Provider (ISP) that could enable it to link a random user ID and profile to a living individual, and that it does not keep a record of the sites visited. You will be aware that two of the ISPs who were in talks with Phorm over deployment of the technology have announced that they are not currently considering any further involvement. However, I am aware that the ICO is keen to keep this issue under review.

The DPA gives the ICO the ability to use legal sanctions against those who ignore or refuse to accept their obligations as data processors and data controllers, including compliance with the data protection principles. The ICO currently has a variety of powers to deal with both the private and public sectors, and in addition to these existing powers, the Government is also taking forward measures in the Coroners and Justice Bill to strengthen the DPA. These steps have led to an array of powers for the ICO, which can be used individually or in combination to provide a strong deterrent or punishment for those who do not abide by the correct procedures for processing personal data in accordance with the DPA.

For further information and details about the DPA and how it is enforced, your constituent might wish to contact the ICO, at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF, by telephone on 01625 545 745 or by visiting their website at www.ico.gov.uk.

Your constituent may also be aware that the Internet Advertising Bureau (IAB) has launched a code of practice specifically concerning behavioural advertising. Microsoft, AOL, Google, Yahoo and Phorm amongst others have signed this code. The IAB code is designed to ensure that the behavioural advertising industry protects and educates consumers on their rights and choices. The code includes three key principles that set out minimum standards to ensure any company collecting or using data for behavioural advertising must:

a) inform a consumer that information is being collected for this purpose;
b) provide a mechanism for consumers to withdraw consent; and
c) provide clear and simple information about how information will be used and how to withdraw consent.

For further information about the IAB code, your constituent may wish write to the IAB at 14 Macklin Street, London, WC2B 5NF, or contact them by telephone on 0207 050 6969, by fax on 0207 242 9928, or by email at info@iabuk.net.

Your constituent raised concerns about the role of the Home Office in this area following the release of information in response to the FOI request. A number of groups approached the Home Office seeking a view on the compatibility of the Regulation of Investigatory Powers Act 2000 (RIPA) with the use of targeted online advertising. A note (the background document) prepared subsequently to this, was informal and was neither departmental nor government policy. In fact, the note included a substantial disclaimer that it was not, nor was it intended to be, a definitive statement of the law, which only a court could give. The Home Office have confirmed that that there was no collusion with Phorm, or any other party, in the preparation of the note.

Your constituent also raised questions about the interception of communications by private organisations. RIPA provides an offence for any person who does not have lawful authority to intercept communications for the purpose of making it available to a third person. The Police, Security and Intelligence Agencies have the power to request a warrant of interception which are authorised, after due consideration, by a Secretary of State. This process is overseen by the Interception of Communications Commissioner who reports directly to the Prime Minister.

It is possible for a communications company, in certain circumstances covered in section 3 of RIPA, to intercept communications and for that interception to be lawful. Circumstances under which Communication Service Providers (CSP) can intercept a communication must be connected for the purpose of running their business. For example, if you complain to a CSP about the quality of sound when making or receiving a call, the CSP can record your conversation to prove whether or not this is the case. In addition when complaints have been made about a customer engaging in malicious phone calls, the CSP may intercept that customer's call to find out whether that is the case. Further, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, authorises certain interceptions of telecommunication communications (which would otherwise be prohibited by section 1 of RIPA), where it is necessary for purposes relevant to that person's business, for example to establish facts relevant to their business or to investigate or detect unauthorised use of telecommunication systems.
Any allegation about an individual, private sector company, or indeed a public body, intercepting communications without a warrant, is a matter for the police to investigate and for the appropriate prosecuting body (for example the CPS or Procurator Fiscal in Scotland) to determine whether a prosecution should take place.

Your constituent also questioned the Government's e-petition response to Phorm on 19 May 2009. There were several reasons why it was appropriate to focus on the role of the ICO, for example, the Government was still considering its response to the European Commission Infraction Letter and the CPS was considering material which might lead to a private prosecution being brought. It was therefore not considered appropriate to comment in the response to the petition on the relevance or otherwise of RIPA, since its applicability, and the position of Phorm under it, is still under consideration.

You refer in your letter to 2 written Parliamentary Questions that you tabled on this issue. I am aware of one of these, which I answered on 8 June and have attached for reference. However, MoJ officials are not aware of a second question that you have tabled in this area although I am, of course, happy to answer any follow up queries you may have.

I hope that you and your constituent find this information helpful. I enclose a copy of this letter for you to forward to your constituent, should you wish to do so.

Yours ever

Michael

MICHAEL WILLS MP

ANNEX A

The Rt Hon Michael Wills MP
Minister of State
102 Petty France
London SW1H 9AJ

S40

E: general.queries@justice.gsi.gov.uk

www.justice.gov.uk

Annette Brooke MP
House of Commons
London
SW1A

Our ref: MC244845
Your ref: ab.ac.0113

August 2009

Dear Annette,

CONSTITUENT'S CONCERNS REGARDING PHORM

Thank you for your letter of 9 June, sent on behalf of your constituent, who expressed several concerns regarding Phorm technology and the results of some recent Freedom of Information (FOI) requests. I am replying following a holding reply sent to you by a departmental official on 30 July.

Firstly, I apologise for the delay in relation to the handling of some FOI requests. I would like to assure you and your constituent that the Ministry of Justice takes its obligation under the Freedom of Information Act 2000 (FoIA) very seriously. The department has taken a number of steps to improve its performance on FOI requests, including the restructuring of its information-related functions. We continue to work closely with the Information Commissioner's Office (ICO) on this and other issues.

I have followed the Freedom of Information trail quite closely, and can understand some of your constituent's concerns. The original FOI request was dated as being received by the department on 19 November 2008; therefore the requester would be given information available up to that date, as is stated under section 10(1) of the Freedom of Information Act 2000. However, I can assure your constituent that while the trail of the FoI request does indeed relate to a briefing from March 2008 as part of a background note to a Parliamentary Question, this does not provide a full picture of the briefing that I have received on Phorm in full. I have received briefing which did not fall within the scope of your request and I have received verbal briefs on this subject.

It might be useful if I explain, at the outset, the role of the ICO. The Data Protection Act 1998 (DPA), which governs the processing of personal data, is administered and enforced by the ICO independently of the Government. The ICO is the UK's independent public body set-up to promote access to official information and protect personal data. Neither Ministers nor departmental officials may intervene nor comment on decisions reached by the ICO. I hope you understand, then, that I cannot comment on the application of the DPA in specific circumstances.

As your constituent may be aware, the ICO, in a statement on the 4 April 2008, said: "[Phorm] assure us that their system does not allow the retention of individual profiles of sites visited…and that they hold no personally identifiable information on web users." The City of London Police was asked to consider the matter and has stated: "it has been decided that no criminal offence has been committed." After contacting the Crown Prosecution Service (CPS) in May of this year, I can confirm that they are still currently considering whether any action needs to be taken with regards to this issue and will report on their decision shortly.

The ICO has confirmed that they consider that targeted advertising technology is capable of being operated in compliance with the DPA and the Privacy and Electronic Communications Regulations 2003, provided that users are given clear information about the manner in which the advertising is served and that they are then able to make a meaningful choice as to whether to allow browser details to be used by the service. It is also the ICO's view that Phorm does not seek, nor have access to information held by the Internet Service Provider (ISP) that could enable it to link a random user ID and profile to a living individual and that it does not keep a record of the sites visited. You will be aware that two of the ISPs who were in talks with Phorm over deployment of the technology have announced that they are not, at this moment, considering any further involvement. However, the ICO are keen to keep this issue under review, and are in regular contact with this department to keep us up to date of these matters.

Your constituent may also be aware that the Internet Advertising Bureau (IAB) has launched a code of practice specifically concerning behavioural advertising. Some key players including Microsoft, AOL, Google, Yahoo and Phorm have signed this code. The IAB code is designed to ensure that the behavioural advertising industry protects and educates consumers on their rights and choices. The code agrees on three key principles that set out minimum standards to ensure any company collecting or using data for behavioural advertising must:

- inform a consumer that information is being collected for this purpose;
- provide a mechanism for consumers to withdraw consent; and
- provide clear and simple information about the how information will be used and how to withdraw consent.

For further queries regarding the IAB code, the IAB can be contacted at 14 Macklin Street, London, WC2B 5NF, or alternatively you can telephone on 0207 050 6969, fax on 0207 242 9928 or email at info@iabuk.net.

One of the key aims of the DPA is to ensure that personal data concerning any living individual is not disclosed to third parties in a manner that is not in compliance with legislation. Technology is developing at a rapid speed and the landscape is changing under our feet. The flexibility of the principles within the DPA allows us to respond to technological advances, such as Phorm. I would also like to emphasis that we keep the framework of the DPA under constant review, and will not hesitate to legislate if and when necessary. Evidence of this can be found from the Coroners and Justice Bill, which is currently in the House of Lords. The Bill was a result of a consultation on the powers of the ICO, as well as a consequence of the Data Sharing Review, carried out by S40

S40

The DPA gives the ICO the ability to use legal sanctions against those who ignore or refuse to accept their obligations as data processors and data controllers, including compliance with the data protection principles. The ICO currently has a variety of powers to deal with both the private and public sectors, and in addition to these existing powers, the Government is also taking forward measures in the Coroners and Justice Bill to strengthen the DPA. These steps have led to an array of powers for the ICO, which can be used individually or in combination to provide a strong deterrent or punishment for those who do not abide by the correct procedures for processing personal data in accordance with the DPA.

For further information and details about the DPA and how it is used, your constituent might wish to contact the ICO who may be able to assist him/her further, at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF, or by telephone on 01625 545 745 or by visiting their website at www.ico.gov.uk.

Following on from this, Government has not endorsed Phorm, nor its technology. We are committed to protecting the privacy of UK consumers and will ensure that new technologies are applied in an appropriate and transparent manner, in full accordance with the law and with proper regulation from the appropriate authority. Your constituent raises some concerns regarding the Home Office being in 'collusion with Phorm' following the release of the "background document". A number of parties approached the Home Office seeking a view on the compatibility of the Regulation of Investigatory Powers Act 2000 (RIPA) with the use of targeted online advertising. The note (background document) which was prepared following this, was informal, was neither departmental nor government policy and did not claim to be. Additionally the note carried a substantial disclaimer that it was not nor was it intended to be a definitive statement of the law, which only a court could give. There was no collusion with Phorm or any other party in the preparation of the note.

Your constituent has also raised questions about the interception element of communications by private organisations. RIPA provides an offence for any person who does not have lawful authority to intercept communications for the purpose of making it available to a third person. The Police, Security and Intelligence agencies have the power to request a warrant of interception, which are authorised, after due consideration, by a Secretary of State. This process is overseen by the Interception of Communications Commissioner who reports directly to the Prime Minister.

It is possible for a communications company, in circumstances covered in section 3 of RIPA, to intercept communications and for that interception to be lawful. Additionally, under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, business communications can intercept communications for their business, for instance to establish facts relevant to their business.

Any allegation about any individual, private sector company or indeed a public body not able to request a warrant of interception and intercepting communications; is a matter for the police to investigate and for the appropriate prosecuting body (such as the Crown Prosecution Service or Procurator Fiscal in Scotland) to determine whether a prosecution should take place.

As your constituent may be aware, the European Commission have taken in interest in Phorm technology for some time and they issued an Infraction Letter to the UK Government on 14 April 2009, and the UK Government responded to this letter on 15 June 2009. Your constituent questions the Government's e-petition response to Phorm on 19 May 2009. There were several reasons why it was considered appropriate to concentrate the response to the petition on the role of the ICO, for example, the Government was still considering its response to the European Commission and had not come to a full view of the compatibility of UK law (including RIPA) and EU law in this area; additionally, the CPS were still considering a file of material presented to it on the subject which might lead to a private prosecution being brought. Therefore it was not considered appropriate to comment in the response to the petition on the relevance or otherwise of RIPA, since its applicability, and the position of Phorm under it, is still being considered by the CPS.

Lastly, in response to your queries regarding Parliamentary Questions, please find attached the answer to your written question on Phorm tabled on 2 June, and answered on 8 June 2009.

I hope that you and your constituent find this information helpful. I enclose a copy of this letter for you to forward to your constituent, should you wish to do so.

Yours ever,

MICHAEL WILLS MP

PQ as it appeared in Hansard:

Internet: Advertising

8 Jun 2009 : Column 770W

Annette Brooke: To ask the Secretary of State for Justice what recent representations he has received on the data sharing implications of Phorm. [278480]

Mr. Wills: The Ministry of Justice has recently received a number of representations on the data sharing implications of Phorm. Those representations tended to focus on issues surrounding privacy and consent regarding the Phorm Trial.

The Information Commissioner's Office is the independent regulator with responsibility for ensuring compliance with the Data Protection Act 1998. Representations have also been made to the Information Commissioner about the data sharing implications of Phorm and he has noted his intention to keep the matter under review.

ANNEX B

S40

Annette Brooke MP
House of Commons
London
SW1A 0AA

www.justice.gov.uk

Our ref: MC244845
Your ref: ab.ac. 0113

30 July 2009

Dear S40

CONSTIUENT'S CONCERNS RE: PHORM TECHNOLOGY

Thank you for your letter of 9 June, sent to Michael Wills on behalf of your constituent. I apologise most sincerely for my delayed reply.

Your constituent has raised a wide range of concerns regarding Phorm technology. As your constituent may be aware, the ICO made a statement on 4 April 2008 saying: "[Phorm] assure us that their system does not allow the retention of individual profiles of sites visited…and that they hold no personally identifiable information on web users." The ICO assure us that this remains their current position, but that they will continue to keep the matter under review.

I am sorry that we are not yet in a position to provide a substantive response to your correspondence regarding the privacy and other implications of Phorm technology in relation to Infraction Proceedings taken against the Government. I do apologise to you and your constituent for this delay. The issues that your constituent has raised are currently being carefully investigated by policy officials across Government, and unfortunately this is taking some time. We will endeavour to send a final reply to you, addressing all your constituents concerns as soon as possible.

In the meantime, if you have any further enquiries about this, please do not hesitate to contact me.

Yours sincerely,

Annex A – the request for information

1. Please disclose all correspondence (fax, email, letter, telephone records etc) that has been exchanged concerning internet advertising using Phorm 121/Media products between the Ministry of Justice and BT, and the Ministry of Justice and Phorm/121 Media since 2006.

2. On what dates have Ministry of Justice officials and Ministers met with BT and/or Phorm/121 Media to discuss internet advertising? What were the dates, minutes, and agenda of those meetings?

3. When were the Ministry of Justice first made aware of the trials of Phorm/121 Media systems in 2006/2007?

4. What evidence has the Ministry of Justice sought from BT concerning the secret trials in 2006/2007?

5. When was the Lord Chancellor and Secretary of State for Justice first advised that cover trials of Phorm/121 Media Systems had been conducted in 2006/2007?

6. When was the Minister of State Michael Wills first advised that covert trials of Phorm/121 Media systems had been conducted in 2006/2007?

7. What action has the Ministry of Justice taken as a consequence?

8. Please disclose all correspondence (fax, email, letter, telephone records etc) exchanged between MoJ and BERR concerning the 'issues' surrounding Phorm/BT Webwise since January 1st 2008, particularly those prior to April 2nd 2008.

9. Documentation and correspondence concerning the way the 'issues' were resolved by MoJ.

10. The dates of meetings between MoJ and BERR concerning the 'issues' surrounding Phorm/BT Webwise since January 1st 2008, please disclose the purpose, agenda, and minutes of those meetings.

On 14 April 2009, the requester clarified that 'issues' related to the following e-mail released by BERR. The e-mail was sent on 2 April 2008 from an employee of BT to an official in BERR: 'David I know you spoke to ? earlier today on this and mentioned that ? is taking the official lead now you have resolved the ministry of justice issue'.

Annex B – draft background note (unredacted with proposed redactions highlighted in grey)

Member: **David Hamilton has been Labour member for Midlothian since June 2001.**

He sits on the following All-Party Groups: Treasurer Civil Contingency and Preparedness Group 2004-; Vice-chair Occupational Safety and Health Group 2004-; Secretary Channel Islands Group 2006-; Chair Coalfield Communities Group 2007- .

He has been a member of the Commons Select Committee for Defence since 2005. Prior to that he was a member of the following Select Committees: Broadcasting 2001-05, Procedure 2001-05, Scottish Affairs 2003-05, 2007-08, Work and Pensions 2003-05, and European Scrutiny 2005-07.

He is Treasurer All-Party Civil Contingency and Preparedness Group 2004-; Vice-chair All-Party Occupational Safety and Health Group 2004-; Member Select Committee on Defence 2005-; Secretary All-Party Channel Islands Group 2006-; and Chair All-Party Coalfield Communities Group 2007- .

Under the Convention of Scottish Local Authorities (COSLA), he sits on the MidLothian Innovation Technology Trust (since 2002). Prior to that he was: Chair Economic Development, Planning and Transport Committee 1997-99, Midlothian Chamber of Commerce -2002; and Midlothian Enterprise Trust –2002.

As a councillor for Midlothian Council (1995-2001) he was Convenor Strategic Services Committee. He was also Chair of the PLP Scottish Regional Group (Commons Backbench Committee) 2007-08 and Vice-chair 2005-07.

Mr Hamilton has not previously raised any PQs with the DCA/MoJ. He asks most questions -

- of: Trade and Industry, Work and Pensions, Defence, Home Department, Treasury.
- about: Coal Industry, Terrorism: Detainees, Defence Activities: Scotland, Iraq, Gibraltar

Mr Hamilton's political interests include Defence, energy, Europe and biotechnology. His Countries of interest include EU, USA, Gibraltar and Cyprus.

The Earl of Northesk has raised a similar PQ for answer on 31 March:

QUESTION **Earl of Northesk**	To ask Her Majesty's Government whether they are taking any action on the targeted advertising service offered by Phorm in the light of the questions about its legality under the Data Protection and Regulation of Investigatory Powers Acts. HL2635

DN – answer will be inserted here when cleared.
The questions may have been raised following the statement by the Information Commissioner's office this month on the Phorm advertising system, and as a result of controversial media attention that Phorm has recently been receiving.

Subject:

Phorm is a company which tracks web activity to create personalised advertisements. Plans by leading Internet service providers (ISPs) such as BT, Talk Talk and Virgin Media to trial using Phorm have sparked controversy.

The Open Rights Group, which campaigns for the digital civil rights of British citizens, has concerns over potential privacy violations caused by the Phorm system. It is calling for a detailed explanation of the exact workings of Phorm to ensure that it complies with privacy legislation.

Approximately 6,500 people have signed up to a Downing Street petition highlighting their worries.

On 3 March 2008, the Information Commissioner's Office (ICO) published a statement on its web site to announce that, at the ICO's request, Phorm has provided written information about the way in which the company intends to meet privacy standards. The statement confirms that Phorm has informed the ICO about the product and how it works to provide targeted online advertising content. The ICO is currently reviewing the information, and is also in contact with the ISPs who are working with Phorm. The ICO says that it will be in a position to comment further in due course and will advise MoJ of the outcome.

On 17 March, the Foundation for Information Policy Research (FIPR) issued an open letter to the Information Commissioner urging him to look at the legality of the Phorm system http://www.fipr.org/080317icoletter.html. In FIPR's view, Phorm will be processing data illegally. Excerpts from the FIPR's press release of the same date include:

- (The Phorm system] will involve the processing of sensitive personal data: political opinions, sexual proclivities, religious views, and health -- but it will not be operated by all of the ISPs on an "opt-in" basis, as is required by European Data Protection Law.
- Despite the attempts at anonymisation within the system, some people will remain identifiable because of the nature of their searches and the sites they choose to visit.
- The system will inevitably be looking at the content of some people's email, into chat rooms and at social networking activity. Although well-known sites are said to be excluded, there are tens or hundreds of thousands of other low volume or semi-private systems.
  More significantly, the Phorm system will be "intercepting" traffic within the meaning of s1 of the Regulation of Investigatory Powers Act 2000 (RIPA). In order for this to be lawful then permission is needed from not only the person making the web request BUT ALSO from the operator of the web site involved (and if it is a web-mail system, the sender of the email as well).
  FIPR believes that although in some cases this permission can be assumed, in many other cases, it is explicitly NOT given -- making the Phorm system illegal to operate in the UK:
- Many websites require registration, and only make their contents available to specific people.
- Many websites or particular pages within a website are part of the "unconnected web" -- their existence is only made known to a small number of trusted people.

FIPR spokesperson (and Open Rights Group Advisory Council member) S40 has said:

> "The Phorm system is highly intrusive — it's like the Post Office opening all my letters to see what I'm interested in, merely so that I can be sent a better class of junk mail. Not surprisingly, when you look closely, this activity turns out to be illegal. We hope that the Information Commissioner will take careful note of our analysis when he expresses his opinion upon the scheme."

On 17th March, the creator of the Internet, Sir Tim Berners-Lee, told BBC News that consumers need to be protected against systems that can track their activity on the Internet, and that he would change his Internet provider if it introduced such a system http://news.bbc.co.uk/1/hi/technology/7299875.stm

Phorm describes itself on its web site as "an innovative digital technology company. Our company is focused on creating a new "gold standard" for user privacy, a more relevant Internet experience, and more value for advertisers, publishers, Internet Service Providers and others in the online ecosystem".

In response to the furore, Phorm issued a statement denying any lack of compliance with privacy legislation. "Our technology complies with the Data Protection Act, RIP Act and other applicable UK laws. Consumers are in control. They can switch the service off or on… Meanwhile the system does not know who they are or where they have browsed as it does not gather personally identifiable information, does not store IP addresses or retain browsing histories... We are currently in conversation with the Open Rights Group to meet with them and look forward to explaining how our technology sets a new standard in online privacy."

S40

has said that the onus would be on ISPs to ensure customers had enough information about the scheme in order to have "informed consent". He said unless ISPs were extremely clear they could run foul of the RIPA. 80/20 Limited conducted the Privacy Impact Assessment (PIA) for Phorm. The Open Rights Group is calling for the PIA to be published.

S36

S40

S40

BERR have been consulted because of their interest in internet issues. They have expressed the opinion that this particular issue is not within their remit.

Annex D – Text of draft reply to the requester

Dear X,

I am writing following on from my letter to you of 14 May 2009 setting out the Ministry of Justice's initial substantive response to your request for an internal review. Having now considered the public interest arguments in relation to the use of section 36(2)(b)(i) and (ii) of the Freedom of Information Act , I am now in a position to provide you with the Ministry of Justice's final reply.

I am releasing in part a draft background note to the parliamentary questions referred to in my previous letter. I am, however, withholding one paragraph of the note under section 36(2)(b)(i) and (ii) of the Freedom of Information Act.

Section 36 of the Freedom of Information Act states:

(2) Information to which this section applies is exempt information if, in the reasonable opinion of a qualified person, disclosure of the information under the Act –

(b) would, or would be likely to, inhibit –

(i) the free and frank provision of advice, or

(ii) the free and frank exchange of views for the purposes of deliberation, or

The use of section 36 requires an assessment of the public interest. Release of this information would improve public knowledge of the way government works and in particular how information is drawn together to help answer a parliamentary question. Confidence in both government and the parliamentary system of government may thereby be cemented and even improved.

However, in this case I believe that the public interest is weighted in favour of protecting ministers' ability to seek and to be provided with free and frank advice. It is stated in terms in the background note that some of the views provided were both personal and informal. There needs to be free space in which it is possible to 'think the unthinkable' and use imagination, without the fear that views or proposals would be held up to ridicule. Release of this information would undermine the space ministers and officials need to develop their thinking and explore options in communications and discussions with other officials. Disclosure of expert advice may mean that in future it will not be sought because of the reluctance of those who might supply it to engage in a debate where their contribution might be disclosable. It is in the public interest that officials are able to provide extensive briefing to ensure that ministers are able to respond fully to questions and discharge properly their duties to account for government policy to Parliament. If candid advice and views were released, officials would be more circumspect in drafting such briefing and ministers' ability to respond to questions would be compromised as a result.

I enclose a copy of the information we are releasing under the Freedom of Information Act. The Ministry of Justice does not hold any further information that falls within the scope of your original request.

I realise that this response will be disappointing to you, particularly in light of the substantial delay in responding to your original request. Once again, on behalf of the Ministry of Justice, I am very sorry for the unacceptable delay in responding to your first request for information. I hope, through this internal review, that we have been able to provide some reassurance to you that the Ministry of Justice will improve its performance in this area over 2009.

Should you remain dissatisfied after this internal review, you have the right of complain to the Information Commissioner, as established under section 50 of the Freedom of Information Act. You can write to him at:

To: 1. Michael Wills **Date:** 1 October 2008

S40

Information Directorate

Tel: S40 Yours sincerely,

Subject: **Phorm and the Thomas-Walport Review**

S40

Information Policy Division

Submission
ANNEX G

Issue

1. Phorm's data processing and data sharing capabilities and its relationship to work flowing from the Thomas-Walport Data Sharing Review (DSR).

Timing

2. Routine.

Recommendation

3. To note the following.

Argument

4. In the course of responding to a letter from Gillian Merron MP about direct marketing and trials of Phorm, you asked for advice on whether the latter constituted a kind of mechanistic data sharing and, if so, what plans were in place to consider the issue as part of the Government's follow-up to the DSR.

5. The DSR was set up to consider issues around the sharing of personal information in the public and private sectors. Follow-up work by Government is focused on responding to the recommendations of the DSR about the way in which personal information should be shared and processed generally in both the public and private sectors. Consideration of the specific issues raised by Phorm technology does not appear to fit comfortably with such follow-up work.

6. Phorm is a relatively new technology and there is a continuing lack of clarity around the precise way it operates and how existing rules should apply. Such uncertainty is unlikely to be resolved until the completion of further trials. The appropriate body to consider the specific issue of Phorm technology is the ICO, who have already completed a preliminary investigation. The ICO's preliminary conclusion is that Phorm technology is capable of being operated in compliance with the DPA. The ICO has powers to take any appropriate enforcement action, including the issuing of an enforcement notice requiring changes to the way Phorm operates if such changes are needed to bring the system into compliance with the DPA.

7. BT confirmed it began a trial of Phorm from yesterday, which is only taking place with customers' consent. The ICO will keep Phorm under review and its view will be strongly influenced by the experience of users who choose to participate in any trials. In addition, the ICO continues to take a keen interest in the dialogue between technical experts and Phorm about how it operates.

Background

8. It remains unclear to what extent personal data, as defined by the Data Protection Act 1998, is to be regarded as processed by Phorm technology or its commercial partners. Even if it is assumed that personal data is processed as a result of the application of Phorm technology, from our discussions with other Government Departments it does not appear likely that the application of Phorm technology would, as such activity if commonly understood, be judged to involve the sharing of such personal data. This is a further reason why the issue does not appear to be one that properly or naturally falls within the remit of follow-up work to the DSR.

9. The ICO's current understanding of the way Phorm technology operates is:

   - An Internet Service Provider (ISP - e.g. a company such as BT) enters into a partnership agreement with Phorm. Phorm technology then analyses the addresses and certain contents of websites visited by individual computers using the ISP's individual customer accounts. Those analyses are then used to match the apparent interests of the computer users to predefined broad advertising categories, so that ads may be targeted at the individual computer users when they access certain websites. The ICO has made clear its view that this must only be done with the prior knowledge and consent of the individual ISP customer at whom such ads may be targeted; both Phorm and BT have accepted this.

   - The information "seen" by Phorm technology does not include billing details or IP addresses held by an ISP – this would be the usual way in which an ISP could link information about internet traffic to a named individual. Instead, Phorm technology assigns a random, unique ID to an individual ISP customer's account, by placing a 'cookie' on the user's computer and builds a profile of internet activity around that random number in order to allow advertising to be targeted more effectively.

   - Phorm does not seek, nor have access to information held by the ISP that could enable it to link a random user ID and profile to a living individual. It does not keep a record of the sites visited using a named individual's ISP account. The technology's analysis of search terms used excludes certain sensitive words, and the advertising categories to which individuals may be matched have been drawn widely so as not to reveal the identity of individual users. However, due to the early stage of testing, it is not yet clear whether such safeguards will be effective in eliminating all personally identifiable information being "seen" by Phorm technology.

10. This is not to say Phorm technology does not raise privacy concerns, or does not require monitoring to ensure that such a new technology remains compliant with the DPA. We welcomed the DSR recommendations regarding transparency of data sharing for the private sector and Government is currently implementing the recommendations of the Cabinet Office's Data Handling Review for the public sector in this regard.

11. The ICO is aware of the concerns recently raised by the European Commission with regard to Phorm and is monitoring how these trials are

being conducted. We will continue to ensure MOJ views are factored into any future contacts between the UK Government and the European Commission.

MATTHEW BENSON

Cc: S40
S40

ANNEX A

The Rt Hon Michael Wills MP
Minister of State
102 Petty France
London SW1H 9AJ

S40

E: general.queries@justice.gsi.gov.uk

www.justice.gov.uk

Annette Brooke MP
House of Commons
London
SW1A

Our ref: MC244845
Your ref: ab.ac.0113

August 2009

Dear Annette,

CONSTITUENT'S CONCERNS REGARDING PHORM

Thank you for your letter of 9 June, sent on behalf of your constituent, who expressed several concerns regarding Phorm technology and the results of some recent Freedom of Information (FOI) requests. I am replying following a holding reply sent to you by a departmental official on 30 July.

Firstly, I apologise for the delay in relation to the handling of your constituent's FOI request. I would like to assure your constituent that the Ministry of Justice takes its obligation under the Freedom of Information Act 2000 (FoIA) very seriously. The department has taken a number of steps to improve its performance on FOI requests, including the restructuring of its information-related functions. We continue to work closely with the Information Commissioner's Office (ICO) on this and other issues.

In connection with this, I can understand your constituents concerns, having followed the Freedom of Information trail quite closely. The original FOI request was dated as being received by the department on 19 November; therefore the requester would be given information available up to that date, as is in stated under section 10(1) of the Freedom of Information Act 2000. However, I can assure your constituent that while the trail of the FoI request does indeed relate to a briefing from March 2008 as part of a background note to a Parliamentary Question, this does not provide a full picture of the briefing that I have received on Phorm in full. I have received briefing which did not fall within the scope of your request and I have received verbal briefs on this subject.

It might be useful if I explain, at the outset, the role of the ICO. The Data Protection Act 1998 (DPA), which governs the processing of personal data, is administered and enforced by the ICO independently of the Government. The ICO is the UK's independent public body set-up to promote access to official information and protect personal data. Neither Ministers nor departmental officials may intervene or comment on decisions reached by the ICO. I hope you understand, then, that I cannot comment on the application of the DPA in specific circumstances.

As your constituent may be aware, the ICO, in a statement on the 4 April 2008, said: "[Phorm] assure us that their system does not allow the retention of individual profiles of sites visited…and that they hold no personally identifiable information on web users." The City of London Police was asked to consider the matter and has stated: "it has been decided that no criminal offence has been committed." After contacting the Crown Prosecution Service (CPS) in May of this year, I can confirm that they are still currently considering whether any action needs to be taken with regards to this issue and will report on their decision shortly.

The ICO has confirmed that they consider that targeted advertising technology is capable of being operated in compliance with the DPA and the Privacy and Electronic Communications Regulations 2003, provided that users are given clear information about the manner in which the advertising is served and that they are then able to make a meaningful choice as to whether to allow browser details to be used by the service. It is also the ICO's view that Phorm does not seek, nor have access to information held by the Internet Service Provider (ISP) that could enable it to link a random user ID and profile to a living individual and that it does not keep a record of the sites visited. You will be aware that two of the ISPs who were in talks with Phorm over deployment of the technology have announced that they are not, at this moment, considering any further involvement. However, the ICO are keen to keep this issue under review, and are in regular contact with this department to keep us up to date of these matters.

Your constituent may also be aware that the Internet Advertising Bureau (IAB) has launched a code of practice specifically concerning behavioural advertising. Some key players including Microsoft, AOL, Google, Yahoo and Phorm have signed this code. The IAB code is designed to ensure that the behavioural advertising industry protects and educates consumers on their rights and choices. The code agrees on three key principles that set out minimum standards to ensure any company collecting or using data for behavioural advertising must:

- inform a consumer that information is being collected for this purpose;
- provide a mechanism for consumers to withdraw consent; and
- provide clear and simple information about the how information will be used and how to withdraw consent.

For further queries regarding the IAB code, the IAB can be contacted at 14 Macklin Street, London, WC2B 5NF, or alternatively you can telephone on 0207 050 6969, fax on 0207 242 9928 or email at info@iabuk.net.

One of the key aims of the DPA is to ensure that personal data concerning any living individual is not disclosed to third parties in a manner that is not in compliance with legislation. Technology is developing at a rapid speed and the landscape is changing under our feet. The flexibility of the principles within the DPA allows us to respond to technological advances, such as Phorm. I would also like to emphasis that we keep the framework of the DPA under constant review, and will not hesitate to legislate if and when necessary. Evidence of this can be found from the Coroners and Justice Bill, which is currently in the House of Lords, which was a result of a consultation on the powers of the ICO, as well as a consequence of the Data Sharing Review, carried out by S40

S40

The DPA gives the ICO the ability to use legal sanctions against those who ignore or refuse to accept their obligations as data processors and data controllers, including compliance with the data protection principles. The ICO currently has a variety of powers to deal with both the private and public sectors, and in addition to these existing powers, the Government is also taking forward measures in the Coroners and Justice Bill to strengthen the DPA. These steps have led to an array of powers for the ICO, which can be used individually or in combination to provide a strong deterrent or punishment for those who do not abide by the correct procedures for processing personal data in accordance with the DPA.

For further information and details about the DPA and how it is used, your constituent might wish to contact the ICO who may be able to assist him/her further, at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF, or by telephone on 01625 545 745 or by visiting their website at www.ico.gov.uk.

Following on from this, Government has not endorsed Phorm, nor its technology. We are committed to protecting the privacy of UK consumers and will ensure that new technologies are applied in an appropriate and transparent manner, in full accordance with the law and with proper regulation from the appropriate authority. Your constituent raises some concerns regarding the Home Office being in 'collusion with Phorm' following the release of the "background document". A number of parties approached the Home Office seeking a view on the compatibility of the Regulation of Investigatory Powers Act 2000 (RIPA) with the use of targeted online advertising. The note (background document) which was prepared following this, was informal, was neither departmental nor government policy and did not claim to be. Additionally the note carried a substantial disclaimer that it was not nor was it intended to be a definitive statement of the law, which only a court could give. There was no collusion with Phorm or any other party in the preparation of the note.

Your constituent has also raised questions about the interception element of communications by private organisations. RIPA provides an offence for any person who does not have lawful authority to intercept communications for the purpose of making it available to a third person. The Police, Security and Intelligence agencies have the power to request a warrant of interception, which are authorised, after due consideration, by a Secretary of State. This process is overseen by the Interception of Communications Commissioner who reports directly to the Prime Minister.

It is possible for a communications company, in circumstances covered in section 3 of RIPA, to intercept communications and for that interception to be lawful. Additionally, under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, business communications can intercept communications for their business, for instance to establish facts relevant to their business. These regulations are the responsibility of Business Innovations Skills Department, and, the responsibility for their enforcement is not part of my department's function.

Any allegation about any individual, private sector company or indeed a public body not able to request a warrant of interception and intercepting communications; is a matter for the police to investigate and for the appropriate prosecuting body (such as the Crown Prosecution Service or Procurator Fiscal in Scotland) to determine whether a prosecution should take place.

As your constituent may be aware, the European Commission have taken in interest in Phorm technology for some time and they issued an Infraction Letter to the UK Government on 14 April 2009. The UK Government responded to this letter on 15 June 2009. Your constituent questions the Government's e-petition response to Phorm on 19 May 2009. At the time of the response, there were several reasons why it was considered appropriate to concentrate the response to the petition on the role of the ICO. As your constituent may be aware, the European Commission have taken in interest in Phorm technology for some time and they issued an Infraction Letter to the UK Government on 14 April 2009. The UK Government responded to this letter on 15 June 2009 and at the time of the response to the e-petition, the Government was still considering its response to the EU Commission and it had therefore not come to a full view of the compatibility of UK law (including RIPA) and EU law in this area. In addition to this, when the Government responded to the e-petition, the CPS were still considering a file of material presented to it on the subject which might lead to a private prosecution being brought. Therefore it was not considered appropriate to comment in the response to the petition on the relevance or otherwise of RIPA, since its applicability, and the position of Phorm under it, is still being considered by the CPS.

Lastly, in response to your queries regarding Parliamentary Questions, please find attached the answer to your written question on Phorm tabled on 2 June, and answered on 8 June 2009.

I hope that you and your constituent find this information helpful. I enclose a copy of this letter for you to forward to your constituent, should you wish to do so.

Yours ever,

MICHAEL WILLS MP

PQ as it appeared in Hansard:

Internet: Advertising

8 Jun 2009 : Column 770W

Annette Brooke: To ask the Secretary of State for Justice what recent representations he has received on the data sharing implications of Phorm. [278480]

Mr. Wills: The Ministry of Justice has recently received a number of representations on the data sharing implications of Phorm. Those representations tended to focus on issues surrounding privacy and consent regarding the Phorm Trial.

The Information Commissioner's Office is the independent regulator with responsibility for ensuring compliance with the Data Protection Act 1998. Representations have also been made to the Information Commissioner about the data sharing implications of Phorm and he has noted his intention to keep the matter under review.

233262

S40

To:
The Rt Hon Michael Wills MP
Minister of State
102 Petty France
London SW1H 9AJ

Sunday, 08 March 2009

Phorm, Webwise, and BT.

Dear Mr. Wills,

Many thanks for taking the time to answer my question at the ICO Data Protection Officer's conference on 4 March.

As I highlighted in my question, approximately 200,000 people, and the businesses who served them, suffered the covert interception of their private communications by British Telecom in 2006 and 2007.

Since that time, there has been no penalty imposed by any of the regulators concerned. Complaints to the ICO, Ofcom, and even the Police have been ignored.

No one in BT or Phorm has been arrested, prosecuted, dismissed, or reprimanded.

The Web is Not Broadcast

It is important to understand, publishing a site on the internet is not 'broadcasting'. A connection between an internet user, and a web site is more like a private telephone call. It is a private data conversation, passing over a public communication network. The content of the communication is specific to the individual user, and often commercially and/or personally sensitive.

Phorm's Assurances

Most of the assurances offered by Phorm are, technically, a work of fiction. The claim to be "privacy enhancing", the claim the internet is funded by advertising, the claim to offer an "opt in" model of operation, the claim to anonymise the text they process… these are all simply fictitious misdirection.

Ministry of Justice

With respect to the responsibilities of the Ministry of Justice, BT/Phorm's conduct in 2006, 2007, and any future use of the system violates various specific acts of legislation (some highlighted overleaf).

- **Regulation of Investigatory Powers Act 2000**

Phorm intercept the private communication traffic between web site operators and users. The target of this interception are online businesses; with the intention to identify their customers, and market competitor products and services.

This is parasitic industrial espionage, and will profoundly damage small and medium businesses with a presence of any kind online.

This penalises people who spend time, effort, money writing, structuring, optimising their web sites and online services.

- **Copyright Designs and Patents Act 1988**

The Phorm system processes literary works and database content that are protected by Copyright (confirmed by the UK IPO).

BT/Phorm do not obtain a licence for the content they copy & process, and even use the content so obtained to the detriment of the original author.

This is no different to other methods of illegal media duplication, such as copying DVDs or CDs. Under the CD&PA, sections 107/110 make it a ***criminal*** offence to trade in infringing articles.

- **Fraud Act 2006.**

Phorm's method of operation impersonates, without licence, the identity of third party web sites for commercial gain.

- **Data Protection Act 1998**

In 2006 and 2007, BT/Phorm processed sensitive personal data unlawfully, in particular without consent or due information.

National Security. Consumer Confidence, and Economic Espionage

There will always be a need for targeted and warranted interception for civil security.

Yet commercial use of similar techniques risks a complete collapse of trust in UK communication services. Without corresponding law enforcement, the only responses available to internet users are strong encryption, or blocking communication with the UK.

The failure to protect the privacy/security/integrity of data communications will also harm consumer confidence in the net, and further undermine already fragile confidence in online services for both Government and private sector.

National security interests should ensure protection from mass economic espionage.

What is Required from Government

The Government ***must*** therefore commence criminal prosecutions against BT and Phorm for the 2006/7 trials.

There must be an absolute prohibition on communication interception without consent of both parties. The Telegraph Act 1868 s.20 made it a criminal offence to disclose the sender, recipient, or content of a telegram to a third party (with a 12 month penalty). This measure must be reinstated, simply replacing the term telegram with datagram.

Recognising the advent of mobile communications, data concerning the location of the parties concerned should also be protected.

The Government must prohibit trading in personal data without explicit consent of the data subject.

There must be harsh penalties for malicious commercial violation of the Data Protection Act. Presently the ICO claim there is no action they can take if the malicious misconduct has already ceased.

ICO must employ qualified IT expertise, and demonstrate a capability to conduct independent critical regulation of the IT industry. Presently, among 200 staff, I understand there is no one in ICO with an IT graduate qualification.

The statement published by the ICO claiming that the Phorm Webwise system can operate legally must be withdrawn, it is simply incorrect.

Conclusion

You said you would write to me, and explain the response of the Ministry of Justice to the Phorm affair.

I would be most interested to receive that explanation.

We have been waiting almost 12 months for the Government to prosecute those who carried out the obscene trials in 2006 and 2007.

Without resolute action to protect private communication, you will confirm the misgivings of those who distrust the commitment of the UK Government to data protection and electronic commerce.

Worse, those concerns will be entirely rational in that event.

Ministry of JUSTICE

Rt Hon Michael Wills MP
Minister of State
102 Petty France
London SW1H 9AJ

S40

E general.queries@justice.gsi.gov.uk

www.justice.gov.uk

S40

Our ref: MFD1099

27 April 2009

Dear S40

Phorm, Webwise and BT

Thank you for your letter of 8 March outlining your concerns regarding the use of behavioural advertising and in particular the company Phorm. You asked for more information concerning the Ministry of Justice's views surrounding the application of Phorm's technology.

It might be useful if I explain that the Data Protection Act 1998 (DPA) which governs the processing of personal data is administered and enforced by the Information Commissioner's Office (ICO) who are the UK's independent public body set up to promote access to official information and protect personal data. Neither Ministers nor departmental officials may intervene or comment on decisions reached by the ICO. I hope you understand, then, that I cannot comment on the application of the DPA in specific circumstances. However, it may be helpful if I briefly explain in general terms the department's response to this issue.

As you may be aware, an ICO statement of the 4 April 2008 states: "[Phorm] assure us that their system does not allow the retention of individual profiles of sites visited...and that they hold no personally identifiable information on web users." The City of London Police was asked to consider the matter and has stated: "it has been decided that no criminal offence has been committed." The Crown Prosecution Service (CPS) is currently considering whether any action needs to be taken with regards to this issue and will report on their decision shortly.

One of the key aims of the DPA is to ensure that personal data concerning any living individual is not disclosed to third parties in a manner that is not in compliance with legislation.

It is important to note that should the ICO have concerns with regard to any data controller's business practices, they have the power to assess, and where appropriate, force compliance. The ICO can currently:

- investigate whether a data controller is processing data without correct prior notification;
- issue an Information Notice where they reasonably require any information for the purpose of determining whether the data controller has complied or is complying with the DPA;
- issue an Enforcement Notice where they are satisfied that a data controller has or is contravening the DPA requiring the data controller to comply; or
- use their powers of entry and inspection under a Schedule 9 warrant, where there are reasonable grounds for suspecting that a data controller has or is contravening the DPA, or has committed an offence under the DPA.

You may be aware the Internet Advertising Bureau (IAB) has recently launched a code of practice specifically concerning behavioural advertising. Some key players including Microsoft, AOL, Google, Yahoo and Phorm have signed this code. The IAB code is designed to ensure that the behavioural advertising industry protects and educates consumers on their rights and choices. The code agrees on three key principles that set out minimum standards to ensure any company collecting or using data for behavioural advertising must:

- inform a consumer that information is being collected for this purpose;
- provide a mechanism for consumers to withdraw consent; and
- provide clear and simple information about the how information will be used and how to withdraw consent.

I trust that this information is helpful. As I said at the ICO conference, I am aware that your concerns about Phorm are more widely shared and I understand them. I shall continue to take a personal interest in the issues surrounding it as they develop in the months ahead.

MICHAEL WILLS MP