

The Internet Threat: Who needs privacy when we can have relevant ads?

Online Privacy and the Interception of Internet Communications

Wednesday 11th March 2009, Committee Room 20

Funding the Internet

The Internet is funded in several ways. The public and business pay for broadband and other services. Companies, government, other organisations and individuals pay to provide content. Content on the Internet may include web pages, but may also include services like email, video streams, software, audio streams, voice, file transfers, instant messaging, and online games.

Website content may be funded by sales of products and services, government, charities, altruism, and user subscription. Some is funded by advertising. That advertising may be simply related to the content of the web page you are viewing. Or it may be related to the content of several or many of the web pages you have recently viewed – behaviourally targeted advertising.

Behaviourally Targeted Advertising

Behaviourally targeted advertising works by tracking which web pages you have visited. In its most simple form, a single website – such as Amazon.com – will keep a record of which pages you visit and show you advertisements relevant to those.

Privacy issues arise when websites share information about your web activity. Many news and social networking sites are part of advertising networks. What you do on one website in the network may be used to decide which advertisements you see on any other website in the network.

Web search engines such as Google use information about what you have searched for to choose which advertisements to show you. Concerns have been raised about the dangers and privacy implications of having a centrally-located, widely popular data store of millions of Internet users' searches, the length of time this data is retained, and about the processing of email message content by Google's Gmail service.

Behavioural Targeting by Interception

Advertising networks use only information collected on websites you have chosen to visit. Last year a new form of behaviourally targeted advertising emerged. This works by intercepting your web activity at your Internet Service Provider and recording information about the websites you visit and what you see when you are there. Nearly everything you do on the web could be used to choose which advertisements to show you. In the US, the main company promoting this was NebuAd. In the UK it is Phorm. BT is one of three major UK Internet Service Providers who have agreements with Phorm. BT has run three trials of Phorm on their broadband service, and this has raised controversy amongst privacy activists and amongst consumers.

Core Issues

Should Internet Service Providers be allowed to read their customers' online activity so as to select advertisements for them? Or should they be expected to operate like the Royal Mail and the telephone companies, who simply convey messages between communicating parties? Can websites expect that their communications with their visitors and customers won't be intercepted or read, or should network providers have the final say over who gets to see and use pages served to users?

What are the dangers to future development of the World Wide Web if such systems are deployed? How does it affect the privacy, security and integrity of personal and commercial communications? How does it affect the ability of the Web to accommodate new ideas, new protocols and new devices?

Why is the UK Government not enforcing laws which appear to preclude systems like Phorm?

The Regulation of Investigatory Powers Act 2000 (RIPA) prohibits unauthorised interception of communications. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) controls how data is used. The Copyright, Designs and Patents Act 1988 prohibits making copies of work (in this case web pages) if they have an independent economic significance.

Current Status

Plans for interception-based advertising deployment in the UK: Following secret UK trials of Phorm's technology in 2006 and 2007, and public trials in Autumn 2008, BT has not given a definite date for when it will deploy Phorm. However, as recently as 10th February 2009, *The Register* reported BT Group chief press officer Adam Liversage as stating that BT still intends to proceed to full rollout.

BT's trials of interception-based advertising in 2006 and 2007: since November 2008 the Crown Prosecution Service Complex Casework Centre has been reviewing whether a prosecution should be brought. A decision is still awaited.

BT's trial of interception-based advertising in 2008: All BT home broadband traffic from customers who were candidates for the trial would have passed through the Webwise/Phorm systems. The trial used a cookie/redirect-based design. During the trial problems were reported with web browsing, mobile device web functionality, and the trial invitation page being presented to a user who wasn't even on BT Broadband. In late November, BT banned all discussion of Webwise and Phorm from its support forums.

UK Information Commissioner's position: On 9th April 2008 the ICO advised that interception-based advertising should be opt-in, not opt-out. At the end of May the ICO stated that it believed that Regulation 6 of PECR would be likely to apply to BT's 2007 trial. However, it did not intend to pursue the issue further with BT as it believed that the trials had not resulted in significant detriment to the individuals involved.

EU position: The Director General of the EU's Information Society and Media Directorate wrote to the UK Government on 30th June 2008 asking for information about their response to the BT 2006 and 2007 trials and possible deployment of Phorm's technology. Correspondence has continued since then, with the EU's lawyers apparently taking a strong position. Following recent discussions with UK government minister Lord Carter the Commissioner has stated that legal questions around Phorm are set to be answered.

US position: On 17th July 2008 Congressman Ed Markey held congressional hearings about NebuAd, whose business model was similar to Phorm's. On 4th August Congress widened its enquiries to thirty major US Internet Service Providers. All plans for interception-based advertising in the US have now been halted.

UK ISPs' position: In October and November 2008 senior or executives or spokespeople for Sky, Tiscali and Orange publicly distanced themselves from Phorm in separate statements. Even the CEO of Virgin Media (an original Phorm partner) stated at a Virgin investors' meeting in New York that "*Our next initiative probably won't be with the Phorms of the world.*"

The Future of the UK rollout? Phorm still believes it has a firm place in the new media and economic landscape. BT appear to be reluctant partners and have declined their invitation to this event, but yet have said they still intend to proceed to full rollout. The UK Government – in the form of the Home Office, OFCOM and the Department of Business Enterprise and Regulatory Reform – appear to regard interception-based advertising as acceptable if certain conditions are met, and appear willing to ask the EU to agree to a potential deployment.

Government involvement: In 2008 Baroness Miller of Chilthorne Domer asked a series of questions about the relationship between the UK Government, BT and Phorm [HL4801-6 and HL4872]. Home Office minister Lord West revealed that they had received a number of requests between June and December 2007 for information concerning targeted online advertising and had met one targeted online advertising company. Responses to Freedom of Information requests suggest that the Home Office were engaged in a dialogue with BT and Phorm as early as November 2006.

What next?

This section sets out a number of policy options for Parliamentarians to consider:

1. Existing laws should be enforced. Future deployment of interception-based advertising should be stopped – as it has been in the US – and a prosecution brought against those responsible for trials in 2006-07. Statements by the Home Office and the Information Commissioner claiming that interception-based advertising systems can operate lawfully must be withdrawn.
2. There must be effective penalties for malicious commercial violation of the Data Protection Act and the Privacy and Electronic Communications Regulations. At present no significant action can be taken if the malicious misconduct has already ceased.
3. The Government should review whether Ofcom can combine the roles of regulating communications, regulating content and encouraging the funding of infrastructure without unacceptable conflicts of interest arising. The Government should consider whether Ofcom should be split into a telecommunication regulator and a media regulator.
4. Telecommunication companies should be encouraged to develop a voluntary code of conduct, including the commitment to refrain from certain conflicting business pursuits, particularly those involving media and advertising interests.
5. The Information Commissioner's Office must employ qualified IT expertise, and demonstrate a capability to conduct independent critical regulation of the IT industry. We understand that currently among 200 staff, there is no one in the ICO with an IT graduate qualification.
6. Recognising the advent of mobile communications, the privacy of data concerning the location of the parties to a communication should be protected.
7. The Government should prohibit trading in personal data without explicit consent of the data subject.

Trustworthy telecommunication services are a key enabler of a modern economy, and vital to protect human rights, so must be robustly protected for the UK community as a whole.