PHORM – PRIVACY IMPACT OF NEW INTERNET ADVERTISING MECHANISMS

1. INTRODUCTION

1.1. Online advertising company Phorm has caused a stir in the Internet community because of its profile-driven service. Phorm has trialled this service with BT, and signed further contracts with Virgin Media and TalkTalk. However, critics claim that the service breaches the Regulation of Investigatory Powers Act (2000), and that Phorm's approach is contrary to users' privacy wishes.

1.2. The BCS believes that the solution to this debate rests in self-regulation of online advertising: companies must establish and enforce a code of conduct; be completely transparent about their practices; resist sharing data with third parties; and submit to ongoing oversight from an independent third party organisation.

2. THE BATTLE FOR THE INTERNET

2.1. The massive market for online advertising is one that affects every Internet user: many search engines and websites depend upon advertising revenues for funding, and some ISPs use advertising to subsidise subscription costs. In the absence of those funding sources they would either have to pass on additional operating costs to users, or cease trading altogether.

2.2. The battle for control of Internet advertising had, until recently, been confined to a small number of (rapidly consolidating) players including the likes of Microsoft, Google, Yahoo! and DoubleClick. These well-established companies have built their offerings over many years and believed themselves to control the market, with little threat from new companies.

2.3. However, a new breed of online advertising company has recently appeared. The likes of NebuAd and Phorm are using behavioural profiling mechanisms to deliver targeted advertising to individual users. As a result they claim that they can justify charging higher fees because of the increased effectiveness of the advertising they provide.

2.4. Their approach has shaken the existing providers, who recognise a legitimate threat to the market share, and end users, who are concerned about the potential for privacy invasion. These worries are catalysed by the sheer scale of the market, estimated to be worth US$41bn.[1] The new entrants have adopted a 'nothing to lose' approach to their business plans, much in the spirit of the original dot-coms, and this aggressive, flexible attitude has jarred with some of their competitors' and end-users' expectations.

3. PHORM

3.1. Phorm[2] offers two key services: the *Open Internet Exchange (OIX)* collects anonymised browsing data (port 80) from participating ISPs' users and builds behavioural profiles of those users with that data. The *Webwise* service then serves targeted advertisements on participating websites based on that data.

3.2. Phorm has announced contracts with three leading Internet Service Providers – BT, TalkTalk and VirginMedia – to embed its OIX and Webwise advertising tools. TalkTalk has stated that it will adopt an 'opt-in' approach to the service whereby users are asked to participate, whereas *the other ISPs will use an 'opt-out' approach.*

[1] **http://www.bloomberg.com/apps/news?pid=20601103&sid=atoBdaCePaBo&refer=us**
[2] **http://www.phorm.com**

4. LEGALITY OF TARGETED ADVERTISING

4.1. Privacy activists claim that Phorm's approach breaches the Data Protection Act 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000. Having been invited to review the system by Phorm, Dr Richard Clayton of Cambridge University and a trustee of the Foundation for Information Policy Research (FIPR), declared the approach to be illegal.[3] Clayton said "the [Phorm] system performs illegal interception" according to the definition found in Section 1 of the Regulation of Investigatory Powers Act, as its profiling mechanism 'intercepts' the user's Internet data.

4.2. It should be noted that if the approach is illegal, then the criminal party here is not only Phorm (by virtue of breaches of RIPA) but also the participating ISPs (by virtue of breaches of the DPA). In this context, we believe that Phorm is acting as a Data Processor with the ISPs as Data Controllers, and that the responsibility to prove data protection compliance therefore rests with the ISPs.

4.3. The public's primary protection of the privacy of their communications is Part 1, Chapter 1 of the Regulation of Investigatory Powers Act (RIPA) (which replaced the Interception of Communications Act). RIPA prevents monitoring of communications traffic unless that monitoring is necessary in order to pass on the communication, or both communicating parties have consented to the monitoring[4].

4.4. The Information Commissioner's Office has taken a close interest in the case since receiving complaints[5]. The ICO's statements on the subject do not focus in great detail on the RIPA issues as this is outside of their remit and competence. They also do not address the question of the legality of earlier trials by BT conducted without the consent or awareness of their subscribers. However, they do state that the matter will be kept under review to assess whether indeed Phorm's activities are in compliance with both the Data Protection Act (DPA) and the Privacy and Electronic Communications Regulations (PECR).

4.5. This is an area of legal compliance that is very complex, not least because: it straddles international jurisdictions, is evolving quickly and is likely to be tested in the courts in several countries in the near future.

5. THE IMPORTANCE OF TRUST

5.1. It is essential to build trust in electronic services, to ensure that all those who hold and process personal information on individuals follow both the letter of the law as outlined in the Data Protection Act and the spirit of the law as articulated in the Act's underlying principles. This includes getting the informed consent of individuals to use their personal data for purposes other than that for which it was originally collected. It is this point that has been the focus for debate about Phorm, which has been characterised by considerable misinformation and personal attacks that have obfuscated the real issues. Many commentators have misunderstood or disregarded the documentation published by Phorm in efforts to reassure its customers. Part of the concern about Phorm arises from the company's history. In its previous guise as 121Media, it was accused of distributing 'spyware' and 'rootkits,' approaches now considered unacceptable for legitimate online advertisers, and blocked by security systems.

5.2. Those who support Phorm's approach argue that this is little different from existing cookie-based approaches to targeted advertising, and that users will in fact benefit from seeing relevant advertisements rather than random (and possibly even offensive) advertising material.

---

[3] **http://www.lightbluetouchpaper.org/2008/04/04/the-phorm-webwise-system/**

[4] However, since RIPA requires consent from both communicating parties, an ISP gaining 'opt-in' consent from an individual is not necessarily going to help as they don't know *a priori* who you may be communicating with.

[5] **http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/phorm_webwise_and_oie.aspx**

5.3. Phorm has stirred additional media attention through what some claim to be heavy-handed use of Public Relations; for example, Phorm has admitted to 'over-zealous' editing of its Wikipedia entry.[6] However, Phorm has also made some very positive moves, most notably hosting a 'town hall' meeting to discuss critics' concerns, and appointing a Chief Privacy Officer to oversee privacy issues.

6. TECHNOLOGY

6.1. Phorm has released information about its technology to FIPR, but there is still uncertainty about the effectiveness of OIX in distinguishing between 'public' materials distributed over port 80, and 'private' materials that use SSL/HTTPS. Phorm's assumption that all private traffic is automatically encrypted using SSL is not valid, since there are numerous webmail services and member forums that do not apply encryption.

6.2. The effectiveness of the 'opt-out' mechanism is uncertain, and it appears that the OIX will still have to intercept traffic from users who have opted out in order to determine this to be the case. For this reason, if no other, we believe that the service should operate on an 'opt-in' approach.[7]

7. RECOMMENDATIONS

7.1. The British Computer Society broadly supports the findings of reviews conducted by the Open Rights Group (ORG) and FIPR.

7.2. In the short term, we recommend that all targeted Internet advertising companies and their partners should adopt an 'opt-in' approach to their services, whereby valid consent is obtained from each user prior to collection of data or delivery of advertisements. Users should be able to revoke this consent as easily as they give it. Furthermore, where traffic is transmitted on port 80 but there is a reasonable expectation of privacy by the user – for example, when using webmail or accessing a members-only forum that is not protected by SSL – then this traffic should be exempt from profiling, although how that is to be achieved is not yet clear.

7.3. In the longer term, if targeted Internet advertising is to be acceptable from a legal, ethical and technological perspective, then this emerging industry requires effective regulation. Since most industries prefer self-regulation to external control, the onus is upon Phorm and others to propose and enforce their own regulatory controls. These controls should include:

a) preparation of a Code of Conduct for organisations collecting or delivering information for targeted online advertising (including ISPs), and the establishment of a management body to independently review and manage that Code. The management body should incorporate an ethics committee of stakeholders to review and advise on changes to the Code. We would expect the management body to be owned and funded by its Members, but overseen by an independent third party, thus creating a self-regulatory approach.

b) an unequivocal statement of participation in targeted advertising by both ISPs and websites, to ensure that users are aware of the possibility of collection, retention and usage. A logo for these partners, linked to further information about the services, opt-out mechanisms, and consumer education materials, will provide transparency of operation.

c) a firm commitment to compliance with all aspects of the law, and in particular that data will not be shared with third parties except where subject to a relevant warrant or court order.

[6] **http://en.wikipedia.org/wiki/Phorm**

[7] http://www.phorm.com/user_privacy/Phorm_PIA_interim.pdf)

d) an invitation to a trusted independent third party body to review the effectiveness of regulation. Participating organisations could fund the likes of the Foundation for Information Policy Research (FIPR) to review their services on an ongoing basis to confirm compliance with the Code of Conduct. The third party may also be funded to review services provided by non-participating organisations operating in this space, and publish comparisons of their operation against the Code of Conduct in order to apply pressure to those organisations to comply.

7.4. Over time, Internet users themselves will determine whether targeted advertising is acceptable to them. Those that object can switch to non-participating (and possibly, therefore, more expensive) ISPs, and choose to exclude participating websites from their browsing habits. Other users, of course, may have no objection, and even welcome reduced ISP costs or more relevant advertisements.

7.5. As aside, the complicated split of responsibility for oversight of compliance issues that this case raises is not helpful for individuals of for industry, particularly where DPA and PECR is covered by the ICO, whilst RIPA compliance is the responsibility of the Home Office and The Interception of Communications Commissioner who keeps under review the work of all organisations involved in the acquisition of communications data. This is a separate issue from industry "self regulation" and best practice and needs separate attention.

Contact:

Andrea Simmons, MBCS CITP, CISSP, CISM, IISP, BA
Consultant Security Forum Manager

For and on behalf of
BCS Security Forum Strategic Panel, chaired by Louise Bennett

British Computer Society
Landline: 01905 356268 / Mobile: 07961 508775
Email: **andrea.simmons@bcs.org.uk**
Web: **www.bcs.org/security**