Privacy Impact Assessment

INTRODUCTION

Phorm Inc has engaged 80/20 Thinking Ltd to deliver a Privacy Impact Assessment (PIA) as an integrated component of product development and deployment of its technology. This final document follows publication of an Interim (first stage) report completed in February 2008. Both documents will be made available on the Phorm website in their entirety.

The commissioned work involves the following elements:

- Scoping the technology and engineering elements to assess privacy functionality.
- Assessment of due diligence and compliance aspects.
- Conducting a full risk assessment of presentational and other elements of the product launch and deployment.
- Auditing the privacy policies.

Going forward, 80/20 Thinking will:

- Work collaboratively with Phorm to develop a sustainable privacy framework within the organisation.
- Conduct privacy training for Phorm staff.
- Create a rapid response privacy reporting & response regime.

80/20 had originally envisioned a final PIA by March 2008, however ongoing public engagement and a rolling series of technology and organisational changes have necessitated a delay. We believe this delay has allowed the creation of a more comprehensive and relevant PIA.

Background to the PIA

Although Privacy Impact Assessments have been adopted for some years in such countries as the US and New Zealand, the process is relatively unknown in the UK. The UK Information Commissioner’s Office executed the Privacy Impact Assessment “launch campaign” only five weeks prior to our engagement with Phorm. Phorm is one of the first companies in the UK to undergo such a process.

As this assessment is being conducted relatively late in the lifecycle of Phorm’s product deployment, 80/20 Thinking has developed a “late stage implementation” PIA model that aims to satisfy most of the key criteria of a “full product cycle” PIA. This model is specifically designed to assist the implementation of a risk mitigation strategy for the implementation and lifecycle of IT projects that either involve personal data or which deploy potentially complex or controversial technologies and techniques.

This model adopts and adapts the best PIA practices from around the world, including those from Australia, Canada, the United Kingdom and the United States. The methodology used for this report incorporates PIA guidance provided by the UK Information Commissioner's Office, the US Office of Management and Budget, and the privacy regulators of Canada and Australia. However, from the perspective of risk mitigation, this PIA is particularly relevant to the UK environment.

One key feature of the "late stage" 80/20 model is the creation of a comprehensive PIA integration throughout the latter phase of product deployment. The publication of this report will provide a foundation for a robust and ongoing privacy infrastructure for Phorm by setting out and examining key criteria. Its aim is to recommend a specific and sustainable programme to achieve this aim.

This PIA takes into account the January 2008 audit performed by Ernst & Young. While broadly agreeing with Ernst & Young's findings, the 80/20 assessment provides a broader geographical context, a wider focus across a more universal privacy environment and a more risk-based approach in its methodology. The Late Stage model also seeks to locate each company's performance in the context of prevailing industry behaviour.

It is important to stress that the PIA is not a comprehensive legal analysis, nor is it a thought-piece on underlying principles and values. The document is a fact-based analysis of the core components of the Phorm system, and an evaluation of its likely implications.

Table of Contents

EXECUTIVE SUMMARY

General

We reiterate the view expressed in our Interim Report that Phorm has successfully implemented privacy as a key design component in the development of its technology system. In contrast to the design of other online targeting systems, careful choices have been made to ensure that the collection of personal data in the Phorm system itself is eliminated. In particular, Phorm has quite consciously avoided the storage of personally identifiable information. This view is reinforced by the Information Commissioner's v.1.3 statement of 18th April 2008. It would thus appear that the UK Data Protection Act, relating to the processing of information by Phorm, does not apply to the Phorm systems.

However, despite our positive findings regarding Phorm's approach to privacy protection, unfortunately the company has not benefited from an earlier implementation of a PIA. While we are encouraged that Ernst & Young were engaged to perform a privacy examination, the full scope and influence of an "early intervention" PIA has not been possible. At this late stage of product development it will not be possible to fully exploit the value of a PIA. In making this observation, we do not mean to imply any criticism at Phorm. PIAs in the UK private sector are rarely undertaken. In this respect and others Phorm has demonstrated a level of engagement and public responsiveness rarely seen in the UK IT sector. Furthermore, in our view, the company has shown a level of commitment to privacy protection rarely demonstrated by online targeting companies. Finally, Phorm has shown a strong commitment to reconsider its designs and plans even at this late stage, showing that even a late stage PIA can result in the integration of privacy protections identified at this point in time.

We broadly agree with the positive findings of the January 2008 Ernst & Young privacy examination that covered Phorm's privacy policy, controls and procedures, Phorm's compliance with its stated privacy policy, Phorm employees' privacy policy training and compliance and Phorm's data retention, integrity and security policies and procedures, but remain concerned that the report was based almost exclusively on conditions applying to the US privacy environment. Public debate, regulatory conditions and other factors vary significantly according to geographical location.

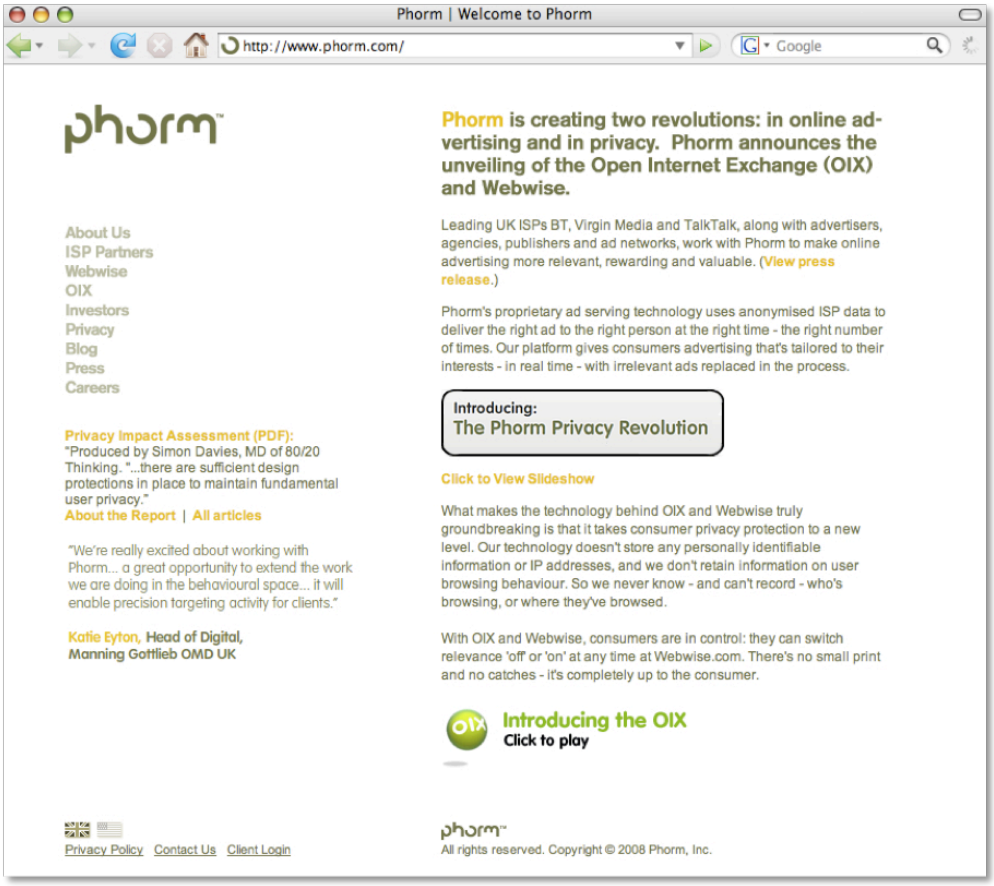
We are encouraged by the openness demonstrated by Phorm's executive team. In addition to what one could call the "Privacy by design" element of the technology, Phorm's clear willingness to engage with stakeholders and to respond to this examination has, in our view, provided a strong foundation for the continuation of a strong and sustainable privacy commitment by the organisation.

Developments since the Interim PIA

Since the publication of our Interim report, Phorm has completed a number of important processes in line with good privacy practice. It has appointed a Chief Privacy Officer, agreed to independent assessment, undergone a security audit of its data capture software, published extensive documentation and directly engaged the public via a variety of channels including a public meeting, press, blogs and forums.

Phorm has proposed the creation of an ongoing independent process of assessment, an initiative that we believe carries considerable merit and, significantly, would be a key safeguard against “mission creep”. It should be noted that since setting this public challenge to the privacy and technology communities, Phorm’s offer has not yet been taken up. This may be an indication that these communities are unaccustomed to this level of access to corporations or it may simply be that these groups are resource poor. At Phorm’s “Town Hall” meeting on April 15th 2008 there was some discussion of Phorm creating and funding, together with others in the industry, an oversight body to keep a check on private sector companies and their privacy protections. We would welcome the furtherance of this initiative on the condition that its operation remained independent.

As an organisation, Phorm has met a number of key privacy tests. The organisation is transparent about the data it collects, its privacy policies are accessible and visible on their website from every page. One reservation is that we believe that the size of the link could be increased to set an industry best practice in this domain. Phorm has affirmed to us that it will consider doing so soon. The company has also created a Privacy and Security Committee (PSC), and has deployed an employee Information Risk, Security and Privacy Policy (IRSPP).



Phorm is creating two revolutions: in online advertising and in privacy. Phorm announces the unveiling of the Open Internet Exchange (OIX) and Webwise.

Leading UK ISPs BT, Virgin Media and TalkTalk, along with advertisers, agencies, publishers and ad networks, work with Phorm to make online advertising more relevant, rewarding and valuable. (View press release.)

Phorm's proprietary ad serving technology uses anonymised ISP data to deliver the right ad to the right person at the right time - the right number of times. Our platform gives consumers advertising that's tailored to their interests - in real time - with irrelevant ads replaced in the process.

What makes the technology behind OIX and Webwise truly groundbreaking is that it takes consumer privacy protection to a new level. Our technology doesn't store any personally identifiable information or IP addresses, and we don't retain information on user browsing behaviour. So we never know - and can't record - who's browsing, or where they've browsed.

With OIX and Webwise, consumers are in control: they can switch relevance 'off' or 'on' at any time at Webwise.com. There's no small print and no catches - it's completely up to the consumer.

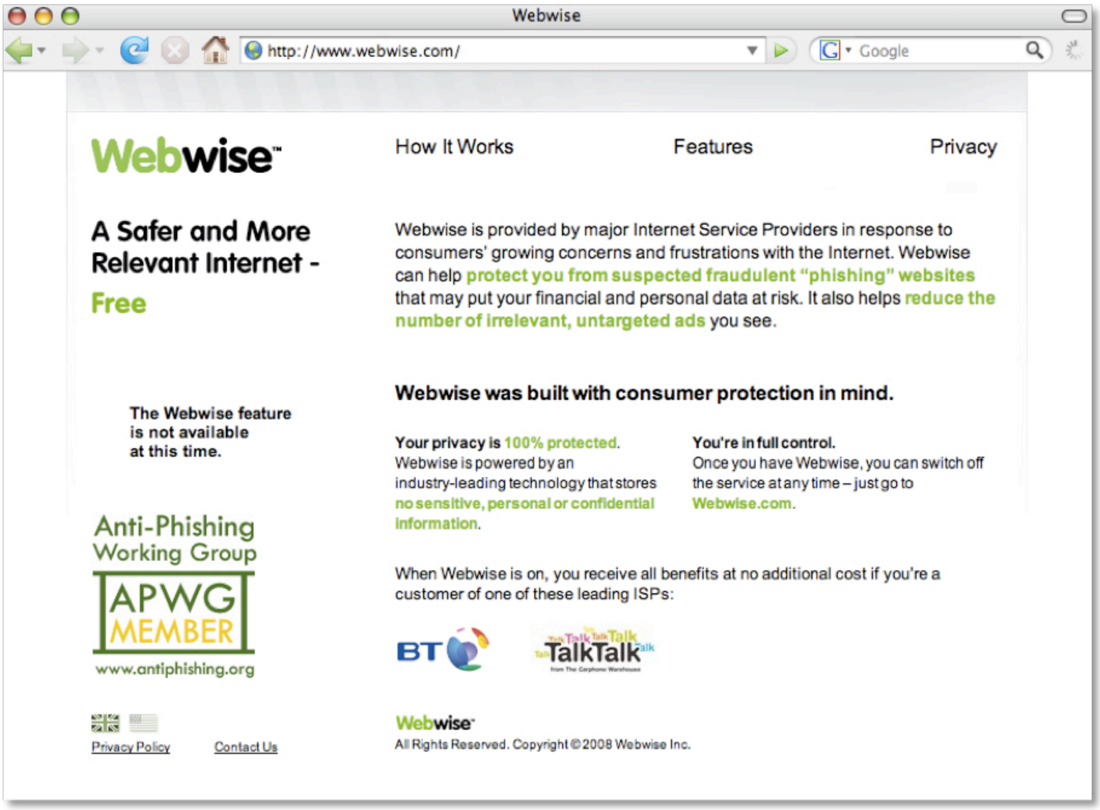
Privacy Impact Assessment (PDF):
"Produced by Simon Davies, MD of 80/20 Thinking. "...there are sufficient design protections in place to maintain fundamental user privacy."
About the Report | All articles

"We're really excited about working with Phorm... a great opportunity to extend the work we are doing in the behavioural space... it will enable precision targeting activity for clients."

Katie Eyton, Head of Digital,
Manning Gottlieb OMD UK

All rights reserved. Copyright © 2008 Phorm, Inc.

Figure 1 - Phorm's website front page. Note the privacy policy appears on the left-hand bottom corner.



A Safer and More Relevant Internet - Free

Webwise is provided by major Internet Service Providers in response to consumers' growing concerns and frustrations with the Internet. Webwise can help protect you from suspected fraudulent "phishing" websites that may put your financial and personal data at risk. It also helps reduce the number of irrelevant, untargeted ads you see.

The Webwise feature is not available at this time.

Webwise was built with consumer protection in mind.

Your privacy is 100% protected. Webwise is powered by an industry-leading technology that stores no sensitive, personal or confidential information.

You're in full control. Once you have Webwise, you can switch off the service at any time – just go to Webwise.com.

When Webwise is on, you receive all benefits at no additional cost if you're a customer of one of these leading ISPs:

All Rights Reserved. Copyright ©2008 Webwise Inc.

Figure 2 - Webwise front page again has a link to the privacy policy, as does every other page.

Phorm has established itself as a key player in the privacy marketplace, particularly when mapped against the following criteria:

- Corporate administrative details (appointment of CPO and creation of PSC),
- Corporate leadership (Phorm has played a strong public role in promoting privacy in the marketplace and has been participating in a number of key public meetings and conferences),
- Data Collection and processing (no storing of personally identifiable information, including IP addresses),
- Data Retention (minimal data retained for minimised time periods),
- Openness and Transparency (numerous examples of public engagement), Responsiveness (highly responsive to media and public comments and attention),
- Customer and user control (Phorm has provided transparent notice and the ability for consumers to exercise choice over participation, though further and stronger leadership is still required for dealing with ISPs).

Importantly, Phorm has responded to criticism by creating key reforms to its functionality. An example of this change is the company's webmail exclusion list. When it became clear that Phorm's critics were uncomfortable with only the largest 25 webmail sites being excluded from Phorm's analysis, Phorm increased this exclusion to over a thousand sites. We also understand that Phorm has created functionality that allows users to submit webmail sites for exclusion as desired.

Phorm and data protection

Based on the information and documentation we have reviewed, including the April statement by the Office of the Information Commissioner, we believe that Phorm Technology does not make use of personal data as defined in the UK Data Protection Act (though not necessarily the data protection or privacy Acts of all countries).

We warned in our Interim report that regardless of legal compliance, "the technology may prompt wider (albeit often perception based) privacy and intrusion concerns". Given the controversy generated in the period since our first report it is clear that regardless of its privacy practices or any safeguards built into its technology, Phorm is engaged in a war of perceptions based on conflicting core beliefs.

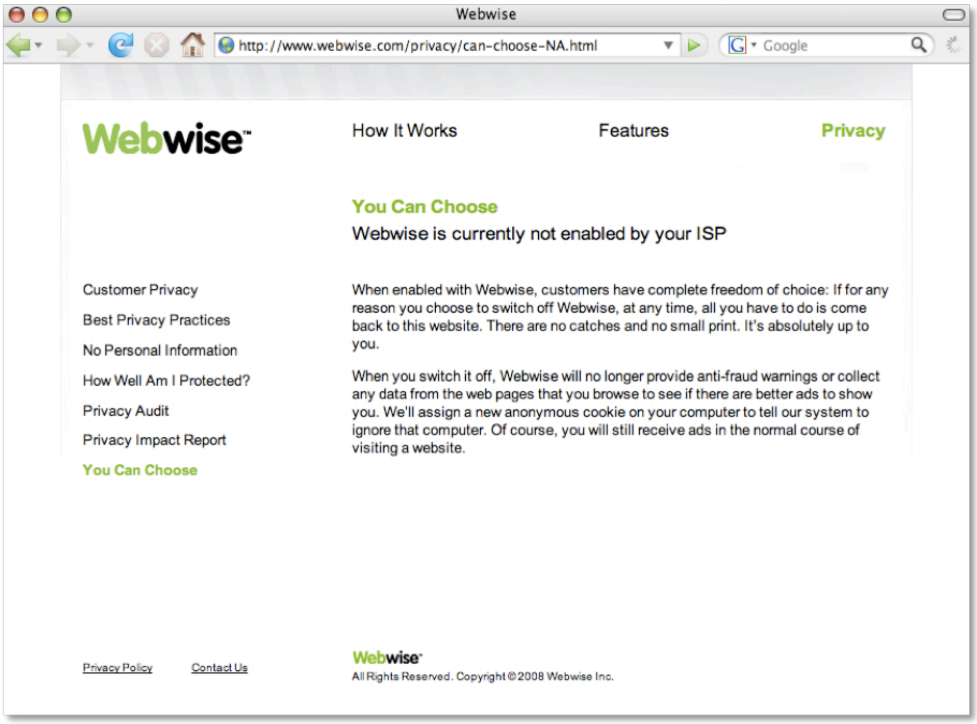
While acknowledging the existence of these contrasting views of the inherent nature of targeted advertising, the PIA is an evidence based process that seeks to assess the specific elements of a system, rather than a discussion of the varying perceptions and social values that are involved. These are matters that will create a commercial impact and are thus more appropriate to market analysis.

The controversy since Phorm's February 2008 announcement has indeed highlighted this dynamic and should sound a warning to other companies that legal compliance with data protection will not necessarily provide immunity from fear of privacy violation and intrusion. However we should also emphasise that claims by opponents of any system must be well-founded or companies may decide to "retreat into the bunker" rather than pursue constructive engagement along the more transparent route that Phorm has chosen. Participants in these public debates must also require similar openness from other companies operating in this marketplace so that fair comparisons can be developed.

Default opt-in versus Choice in opt-out

At a functional level and at a level of principle, the division of opinion about Phorm centres largely on the opt-in/opt-out question. That is, whether the Phorm system should be, by default, switched on, leaving customers with the option of opting out, or whether by default the system should be switched off, leaving customers to opt in. Best privacy practice would normally be the latter, though we are mindful that the Phorm opt-out system, when fully developed, could be one of the best we have yet seen in the online environment.

The choice of one model over the other will be a decision carrying market and trust implications relating to a proportion of users. We urge that where the default is not opt-in, the mechanism adopted should centre on simplicity of use, clear and ongoing notification and minimal disruption.



You Can Choose

Webwise is currently not enabled by your ISP

When enabled with Webwise, customers have complete freedom of choice: If for any reason you choose to switch off Webwise, at any time, all you have to do is come back to this website. There are no catches and no small print. It's absolutely up to you.

When you switch it off, Webwise will no longer provide anti-fraud warnings or collect any data from the web pages that you browse to see if there are better ads to show you. We'll assign a new anonymous cookie on your computer to tell our system to ignore that computer. Of course, you will still receive ads in the normal course of visiting a website.

Webwise™
All Rights Reserved. Copyright © 2008 Webwise Inc.

Figure 3 - Webwise Notification and Opt-out page

As we observed in the Interim report, we maintain that “Phorm Technology offers a high standard of privacy and data protection”. However, there continues to be a serious risk that the product will be perceived as invasive. This risk arises from three key phenomena: the plethora of invasive products and programmes currently being deployed across the Internet, the belief that the “fact” of online tracking is inherently invasive, and the lack of knowledge the majority of people have about online tracking. The fact of having one’s Web activity analysed will, in the minds of some, be an intrusive act, regardless of legal analysis. This is a perception Phorm should take seriously.

Whether or not the view prevails that Phorm is intrusive will largely depend on the framework for notice and consent offered by Phorm’s partner ISPs and the extent to which consumers understand not only what Phorm’s technology does, but the current state of online tracking. One key challenge for Phorm is to educate the public and key stakeholders not only about its own practices, but also about the industry in which it operates.

The ISP element

Neither the Interim assessment nor the work leading to the final PIA has been able to fully examine the privacy practices or intentions of Phorm’s partner ISP’s. However, we understand that Phorm’s ISP partners are under pressure to adhere to a high standard of privacy practice to ensure the maintenance of consumer trust.

We stated in our Interim report that our initial understanding of the technical elements of Phorm Technology led us to the view that there are sufficient design protections in place to maintain fundamental user privacy regardless of potential adverse processes adopted by third parties and partners. BT, Carphone Warehouse, and Virgin Media have provided statements to us, intended to inform the PIA, and these documents tend to support our initial assessment. Nevertheless, we urge all ISPs involved in the technology to independently conduct PIAs to ensure that there exists a consistent methodology for privacy evaluation.

Recommendations

We believe it will be crucial to devise a system based on both transparency and embedded technological safeguards to provide assurance that Phorm Technology does not fall victim to the level of function creep evident in other technologies. Continuing engagement with Phorm, involving independent technology specialists, will help ensure that these safeguards are fully developed and exploited.

In our view, Phorm should ensure that ISPs using its system clearly communicate with their users about the issues involved in Phorm Technology surveillance, and actively and regularly pursue users' consent. Phorm promotes the view that its model is predicated on ensuring consumers are aware of the system and are always able to exercise choice as to their participation. In the absence of a default opt-in we believe this approach may be crucial to mitigating potential concerns about behavioural targeting. There are strong indications that future trials by the majority of ISP partners will involve appropriate use of notice and consent, though it remains unclear how each ISP will choose to offer their customers the service.

We encourage Phorm to work closely with Partners to ensure that privacy practices are pushed to the highest level possible. Communications surveillance laws at the very least require consent to be re-affirmed at regular intervals, particularly as multiple users may make use of a single Internet connection and machine.

Phorm's privacy policy responsibly notes that Phorm may disclose information to third parties under 'legal requirements'. The general public needs to be made aware of the type of information collected by Webwise, ISPs, and Phorm as well as the security processes in place to ensure against abuse. The reality is that Phorm collects very little that may be of value to other parties.

This assessment does not embrace the scope or the mandate to comment on the compliance situation with regard to the Regulation of Investigatory Powers Act (RIPA) or the Privacy and Electronic Communications Regulations 2003 (PECR). Although we note that the House of Commons Home Affairs Select Committee observed in its recent report A Surveillance Society? that “In April 2008 the Information Commissioner took the view that Phorm could operate Webwise and Open Internet Exchange (OIX) in a way which is in compliance with the Data Protection Act and Privacy and Electronic Communications Regulations but must be sensitive to the concerns of users;” we do not feel we have competence with regard to this assessment to take the matter further.

THE PURPOSE OF THE PIA

Privacy Impact Assessments provide a framework to help ensure that privacy is considered throughout the design or re-design of programs or services. The PIA assessment is a resource to clarify the risks and effects of collecting, maintaining and disseminating information, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. PIAs are also designed to help embed responsible privacy practice and to promote fully informed policy, program and system design choices.

The PIA process may invoke a range of sentiments. When a PIA is applied to potentially intrusive or controversial technologies it can attract criticism for “aiding” or legitimising the client company. However, 80/20 Thinking believes that applied properly and with genuine respect for consumer interests, a PIA satisfies the best interests of both the company and stakeholders.

The PIA process, with regard to potentially intrusive technologies, might be equated in the environmental arena to engagement with motor vehicle manufacturers. This is a question that confronted environmental campaigners more than twenty years ago. On the one hand it can be argued that any engagement with such sectors is inherently counterproductive. That is, many advocates take the view that all internal combustion engines are hostile to the environment and no amount of engagement with industry will change that situation. On the other hand there is a view that engagement is more beneficial than non-engagement. This view asserts that there are advantages to engagement that outweigh the polemic.

The PIA process assumes that the latter option is most desirable. Margins for improvement can be discovered, even for an inherently privacy hostile technology. Safeguards can be designed, user options adopted, data minimised and limitations placed on information flows. One view, additionally, is that the PIA process means that a company cannot claim ignorance about the impact of its proposals.

We conditionally agree with the June 2008 House of Commons Home Affairs Select Committee report which observed when looking at surveillance in the public and private sectors: “In the case of the private sector, several of our witnesses saw a direct link between trust and profit, which created a commercial imperative to protect personal information and privacy: losing the trust of customers would result in loss of revenue. The Information Commissioner’s Office has stated that “in the private sector there are pressures to get it right which do not necessarily exist in the public sector”.” This assessment has merit when, in the case of online tracking, privacy is becoming a market differentiator.

At its core, the PIA is principally a form of risk management. It enables mitigation of such project risks as:

- Loss of public trust and credibility as a result of perceived harm to privacy or a failure to meet expectations with regard to the protection of personal information;
- Retrospective imposition of regulatory conditions as a response to public concerns, with the inevitable cost that this entails;
- Low adoption rates (or poor participation in the implemented scheme) due to a perception of the scheme as a whole, or particular features of its design, as being inappropriate;
- The need for system re-design or feature retrofit, late in the development stage, and at considerable expense;
- Collapse of the project, or even of the completed system, as a result of adverse publicity and/or withdrawal of support by the organisation or one or more key participating organisations, or
- Compliance failure, through breach of the letter or the spirit of privacy or data protection law (with attendant legal consequences).

When planning a PIA, the responsible executive within the organisation should ensure that all of these possibilities have been considered, and that the organisation seeks an appropriate set of outcomes from the investment.

At an executive level, the objectives for a PIA are:

- Ensure effective management of the privacy impacts arising from the project
- Ensure effective management of the project risks arising from the project's privacy impacts
- Avoid expensive re-work and retro-fitting of features, by discovering issues early, devising solutions at an early stage in the project life-cycle, and ensuring that they are implemented.

In order to achieve those objectives, the following are taken into account as operational aims for a PIA.

- Clearly define the organisation's business needs.
- Clearly define the design, including technical elements, the relevant data flows and the relevant business processes
- Identify the features of the design that have potential privacy impacts and implications.
- Understand the rationale underlying those features.
- Consider the business case that justifies (a) the design as a whole, and (b) the design features with potential privacy impacts and implications.
- Identify (a) the project's first-order privacy impacts (i.e. Those that are direct and immediate) and (b) the project's second-order privacy implications (i.e. Those that are indirect, deferred, contingent or speculative). An example that is easily over-looked is 'function creep', which refers to the application of personal data to additional purposes that were not originally envisaged.
- Identify the stakeholder groups, including all segments of the population that may be affected by the project and what it delivers.
- Identify and involve representative and advocacy organisations for the relevant stakeholder groups.
- Enable the representative and advocacy organisations to (a) Achieve an understanding of the project, (b) Assess it from their own perspectives, (c) Have their perspectives understood by other stakeholders, (d) Understand the perspectives of other stakeholders (e) Have their

perspectives reflected in the project design and (f) Assure all stakeholder groups that their perspectives have been taken into account.

- Enable the design to work towards maximisation of the positive impacts and implications of the project.
- Enable negative impacts and implications of the project to be avoided, or at least reduced.
- Avoid the emergence of new requirements at a late stage in the design process (or, worse still, during construction, deployment, or even operation), when modifications are much more expensive, slower and risk-prone.
- Be publicly credible, in order to support public confidence in the project, and minimise the risk of the project encountering difficulties with public acceptance.
- Achieve awareness-raising and education for (a) Executives, managers and operational staff of the organisation and other participating organisations (b) Representatives and advocates of stakeholders and (c) Relevant segments of the public.
- Pre-empt any possible misinformation campaigns.
- Commit stakeholder representatives and advocates to support the project, in order to avoid the emergence of opposition at a late and expensive stage in the design process.

Privacy Audit vs. PIA

Privacy Impact Assessment is defined as a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a search is undertaken for ways to avoid or minimise privacy concerns. In the case of Phorm, we define “stakeholder” to include all members of the public using the Internet. An audit is undertaken on a project that has already been implemented. An audit is valuable in that it either confirms that privacy undertakings and/or privacy law are being complied with, or highlights problems that need to be addressed.

Although the PIA process takes the Data Protection Act and other relevant laws into account, it does not focus exclusively on them. A complementary audit process is needed to ensure that the project is legally compliant. That process can begin early, but cannot be finalised until late in the project lifecycle, when the design (and usually implementation) is complete.

STAKEHOLDER ENGAGEMENT

Stakeholder engagement is one of the key ingredients of a transparent and responsible approach to privacy compliance. The process assists the evolution of implementation, operation and the development of trust. The specific elements of the PIA that apply are:

- Identify the stakeholder groups, including all segments of the population that may be affected by the project and what it delivers.
- Identify and involve representative and advocacy organisations for the relevant stakeholder groups.
- Enable the representative and advocacy organisations to (a) Achieve an understanding of the project, (b) Assess it from their own perspectives, (c) Have their perspectives understood by other stakeholders, (d) Understand the perspectives of other stakeholders (e) Have their perspectives reflected in the project design and (f) Assure all stakeholder groups that their perspectives have been taken into account.
- Achieve awareness-raising and education for (a) Executives, managers and operational staff of the organisation and other participating organisations (b) Representatives and advocates of stakeholders and (c) Relevant segments of the public.

Phorm has undertaken an unprecedented exercise in public engagement. It has sought to engage fully with key stakeholders from parliamentarians to privacy advocates, to the general public. It is noteworthy that Phorm's CEO has directly engaged media and the public on numerous occasions. Of particular note is the "Town Hall" public meeting held on April 15th in London, which created an ideal environment for stakeholders to directly interact with Phorm. The meeting was criticised on grounds of accessibility to all (it was held at relatively short notice in London), but in our view Phorm's willingness to invite two of Phorm's most prominent critics as speakers established the level of positive engagement that we wished all companies and government agencies would adopt. Phorm's effort to directly engage key advocates throughout the past four months is also a valuable contribution to the engagement process.

Prior to the town hall meeting, Phorm agreed to a full inspection by a computer security specialist, a person who was also a prominent Phorm critic. This process went beyond the expectations of a PIA, and helped clarify a number of key issues. More detail of this assessment is set out below.

Our assessment is that Phorm has complied with, and exceeded, all requirements of the PIA with regard to stakeholder engagement. In fact, we would go so far as to say Phorm's approach can be viewed as a model for stakeholder engagement.

RISK ASSESSMENT

Phorm's technology ('the system') performs analyses on a user's Internet traffic through a partnership agreement with the user's Internet service provider (ISP). These analyses result in targeted advertising.

Phorm appears to have considered privacy as a key design component in the development of its system. In contrast to the design of other targeting systems, careful choices have been made to maximize privacy protection. In particular, Phorm has quite consciously avoided the storage of personally identifiable information.

However, despite Phorm's openness and transparency, its offer is a complicated one and it needs careful explanation. In the absence of proper understanding, consumers, partners, the media and the general public may have a vastly different interpretation of the nature of Phorm's system. The amount of attention this technology has generated is not a surprise as the general public and interested parties should naturally be concerned when a product or a system offers 'deep packet inspection'. DPI is, after all, the type of technique that is used in highly invasive surveillance and censorship practices. But Phorm goes through extensive measures to avoid the data protection risks in this technique. However, we need to be assured that a simple redesign or rewriting of code could not enable some more invasive form of processing.[1] Even though we are assured that the packet inspection technology is solely operated by ISPs (and so Phorm would not likely benefit from changing the code), legitimate concerns remain. Yet the risk of modifications that enhance surveillance is low as it is likely that alternative measures would be sought if ISPs or others wanted to conduct more extensive surveillance. Despite this, there needs to be an oversight process for any relevant changes to the design and implementation of Webwise to ensure against any abuse.

The documentation of these risks and the methods of risk mitigation in this report are a key component of a privacy impact assessment. With our experience in Internet and privacy policy we are able to identify what are the likely issues to give rise to concern to consumers, policy-makers, civil society, media and other stakeholders. We consulted with external experts and with Phorm employees to clarify our initial concerns, as outlined in the interim assessment, to elaborate on Phorm's techniques below.

The Perception of Selecting Traffic for Sensing

Phorm is careful to note that only a small component of Internet traffic information is actually being processed. However there is significant public concern regarding the monitoring of Internet usage,

[1] This point was raised by the analysis from the Foundation for Information Policy Research, entitled 'The Phorm "Webwise" System - a Legal Analysis', April 23, 2008, particularly in paragraph 5.

and if poorly explained and managed, this current wave of concern could seriously damage trust in Phorm's system and in the ISPs which choose to implement Phorm's technology.

Media attention has already focused on this dynamic and has warned users that their ISPs will monitor all online activities. Even if more educated coverage notes that only web-browsing (and even then a specific subset) is covered this will not resolve immediate responses from audiences that the system is 'spying' on their activities online to the profit of ISPs. In essence this is the difference between ‘privacy’ and ‘data protection’ concerns. In most ways, Phorm manages its own data protection problems within Webwise with great care by ensuring it processes the least amount of personal information as possible.

Purpose Re-specification, Communications Surveillance, and Consent

Users of ISPs are accustomed to the current contract that an ISP is merely a conduit and the ISP itself does not use the data shared with the ISP by the user, i.e. routing information, for any purpose, except for perhaps network engineering. Any change to this relationship is likely to have an impact on users' confidence. It is therefore essential that Phorm be as transparent as possible, particularly since it has acted in such a pro-active manner, to preserve and arguably enhance users' privacy. We would also hope that in the future Phorm would dictate some terms to its ISP partners to ensure that they uphold the highest standards of data protection.

In essence, ISPs are changing the purpose of data processing activities. Whether they adopt Phorm's services is at the discretion of the ISP, and therefore the responsibility to negotiate with the users lies with the ISP. Concerns may mount that ISPs are now conducting communications surveillance for their own financial benefit. But this means that Phorm will have to play a proactive role in educating policy makers and the media to explain how their service does not herald a ‘slippery slope’ towards surveillance of other forms. While we accept that Webwise is very limited in what it can do, we worry that policy makers will use the argument that because our traffic is inspected for advertising purposes, adding new devices to networks to monitor for suspect key words is merely an evolutionary step. We expect that Phorm will play a leadership role in such debates to ensure that such a confusion does not arise.

Phorm liaised with the Home Office to assess whether its system could infringe the UK law that regulates communications surveillance. The Home Office concluded that Phorm's system is consistent with the Regulation of Investigatory Powers Act and does not intercept communications. While this conclusion is a fair interpretation of Phorm and the system's capabilities, communications monitoring still takes place. Even if the Home Office's conclusions were appropriate and relevant, it would mean that if an ISP or any government wished to conduct similar monitoring of communications for segmentation purposes, albeit with consent of the user, then they may indeed do so and yet still be compliant with UK law. This could indeed give rise to a worrying situation as users can be compelled or convinced to consent to monitoring that would be seen as being necessary (e.g. monitoring cybercrime activity or any access to controversial resources) and would face a reduction in their expectation of privacy. Consent is merely one step to provide protections and safeguards, while independent authorisation and oversight is also necessary.[2]

In its assessment, the Home Office compares targeted online advertising with email/spam filtering. This was a similar line of argument pursued by Google in its Gmail advertising service: the content of messages are already being processed by ISPs to assess whether they are spam, therefore – the argument goes - analysing content for advertising purposes is no different. The key difference, as argued by many privacy experts, is that processing communications to remove inconveniences (e.g. spam) is not invasive because it is intentionally not passing judgment on the user. Processing communications to categorise individuals, or to pass judgment on the consumer, is a privacy interference.

Phorm must endeavour to ensure that ISPs clearly communicate with their users the issues involved in this targeting, and actively and regularly pursue users' consent. This is the only way to mitigate concerns.

While we were only asked to do a PIA for Phorm, conducting an informed PIA requires understanding how third parties, and in this case, essential third parties, intend to apply the techniques in question. In light of this, we are somewhat disappointed by the lack of responsiveness from ISPs. Although the three key ISPs did respond, there were few substantive comments. One ISP informed us that they had conducted legal reviews, user focus groups and surveys.

BT was more open about the planned trial of Webwise. It noted that the trial would only involve a subset of invited customers who can then ‘switch on’ Webwise. They promise that their own policies and terms of service will be amended accordingly. But BT notes that their change in ToS is for the purpose of notifying customers that they are responsible for ensuring that all users in the household are aware of the Webwise service and how to switch it on and off.

The issue of notification thus becomes essential. Without adequate notification of their options to be advertised to, users will not be able to exercise any of their rights. As with any value added service run by any operator, we are worried about the scenario where ISPs start adding customers without actively inviting them to participate. In turn, unless every user within a local network (e.g. home or business subscriber enables a local network using routers) is notified by the ISP of the terms of service that they must appropriately opt-out or manage their cookies accordingly, then they are unwittingly included in the Webwise system. As a result, we we would like to reiterate that that ISPs should always give the subscriber the right to decide whether to participate.

Moreover, we are concerned, however, that this should not be the only mechanism by which users of the system will be aware of the existence and operation of an advertising system. According to Phorm, there is both the possibility of 'unavoidable' notice delivered to each individual user and the

[2] Although the 'reasonable expectation' test is a North American legal concept, it helps to understand some of the possible risks here. This point was raised in the dissenting opinion by Justice Marshall in *Smith v. Maryland* (442 U. S. 735 (1979)) where he said that you could reduce the public's expectation of privacy in communications data by just informing them that all communications are monitored, and thus 'conditioning' them. This would permit unfettered monitoring.

continued showing of 'status reminders' within the ad slots shown to the users, which will indicate that webwise is switched on or off.

While Phorm promises that they are also responsible for notifying individuals that Webwise is in use, it is disappointing that a single subscriber can subject all users of a network to browsing-profiling. We would like to reiterate that ISPs should always give the subscriber the right to decide whether to participate, as BT is doing in the trial. That is, the form of consent in participating in the upcoming trial should become the norm. We have been informed that at least one ISP is looking into options to develop a mechanism to capture non-consent to the service without any cookie-related procedures. We hope that other ISPs follow this example.

At a minimum, we expect that Phorm and the ISPs would establish a form of consent that would sustain the assessment of the Information Commissioner's Office. That is, in its statement, the ICO stated

> "from the information available at this point it appears that users will be presented with an unavoidable statement about the product and asked to exercise a choice about whether or not to be involved on that basis. In addition we are told that users will be able to easily access information on how to change their mind at any point and are free to opt into or out of the scheme at any point thereafter which should involve the same degree of transparency and choice."[3]

This is a problem for ISPs to manage, and therefore this is in one sense a matter beyond the scope of this PIA, as we are informing the practices of Phorm and Webwise. However we look forward to seeing how Phorm continues to manage its relationships with the ISPs and establishes and hopefully requires best practices to manage consent. For instance, Phorm has stated that they are working with the ISPs to develop a network-level opt-out. We would like this to become the default. According to one analysis and commentary, Phorm believes that whether an ISP implements a network-level consent mechanism should be up to the ISP, as their ability to do this depends on their infrastructure and support systems.[4] While we understand the need for flexibility, we expect Phorm in turn to expect best practices from its partners.

There are many other legal concerns regarding interception of communications involving only one-party consenting (and not the webserver, for instance). These are best articulated in the detailed analysis provided by Dr Richard Clayton[5] and the Foundation for Information Policy Research. Dr Clayton notes that websites may opt-out of this form of processing by amending their *robots.txt* file but the manner of managing this form of consent is problematic. This potentially raises serious problems particularly for websites that contain substantial amounts of personal information such as social networking sites, personal web pages, private webpages and others. Admittedly some of these are already beyond access by search engines and thus will be beyond access to Phorm, and

[3] Phorm – Webwise and Open Internet Exchange, Statement from the Information Commissioner's Office, April 19, 2008, available at http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/phorm_webwise_and_oie.aspx

[4] 'The Law of Phorm', Outlaw editorial from Outlaw News, by Struan Robertson, May 1, 2008.

[5] 'The Phorm "Webwise" System', Richard Clayton, version revised May 18, 2008.

we understand that that the Phorm system is effectively 'blind' to any data that is not contained in one of its advertising categories, so that personal or sensitive information, which is excluded from these categories, will not matched and cannot therefore form the basis of a stored behaviour. We are also assured that Phorm will continue to update its list of email websites, and allows for individuals to notify Phorm of such services. We believe that Phorm should also allow for website owners to opt-out, though this introduces difficulties in ascertaining the identity of the 'owner' of a website. Rather, Phorm should develop additional criteria for assessing, upon receiving a complaint, whether a page should or should not be analysed.

How the system deals with sensitive data

Under data protection law 'sensitive information' would involve data regarding the racial or ethnic origin of the data subject, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

As data is processed by Phorm's system without collecting personally identifiable information it is then likely that this will be compliant with data protection law. We previously advised Phorm to develop black-lists or white-lists of sites and types of data that will not be processed. Measures such as these would enhance user confidence to know that this type of information is never processed at all. Therefore information from websites and queries regarding sexual content, political preferences, medical health, racial origin should be blocked from processing. We were originally concerned in our interim PIA that Phorm should communicate openly whether profiles and channels will match information of this type, e.g. matching pharmaceuticals with web activity that searches for anti-depressants.

Phorm has assured us that they have established exclusion categories to limit the risk of this form of data processing. The system ignores sensitive data because the only data that it registers is that which match advertiser-related channels, whose content is controlled to exclude any sensitive triggers e.g. medical conditions. We look forward to a regular review and audit of these channels to ensure that this practice continues.

Additionally, Phorm's system excludes forms, or any site that uses standard HTTP 'Basic' authentication. This should therefore exclude content from sites where an individual is drafting an email. Webwise also excludes 'secure' web traffic (see below). Phorm also maintains a blacklist of over 1000 webmail sites whose content will not be analyzed.   Finally, Webwise excludes email addresses and has developed a technique that attempts to exclude names from processing.

How sensitive sites are excluded

While Phorm is careful to note that 'secure pages', i.e. those delivered under the HTTPs protocol over port 443, we are reassured that https-requests are not logged at all. That is, HTTPS requests occur on port 443 and are not seen by the system at all. Even if an HTTPS request were directed to port 80, it would be encrypted and therefore could not be analyzed.

The reason we raised this concern is that such ‘secure’ requests tend to be from servers where users have an existing relationship, e.g. their banks, travel agents and mail providers. If this information is logged by an ISP this process would make users feel spied upon because their ISP would know which services he or she makes use of. Webwise does not process this information in this manner. In fact, URLs are not kept beyond the period of essential processing. That is, the channel match associations that are stored consist of only the advertising category, a random number, and a timestamp. The URLs are thrown away when the match is made.

Additionally, the channel must have a minimum number of match terms so that the fact of a channel match cannot be used to deduce where the user browsed. There is also a requirement for a minimum match volume so that a channel cannot identify an individual or small group.

Users need to be informed explicitly about the constitution of channel information. If not carefully explained, users may worry that channel information, depending on the level of data granularity, in itself constitutes personal or sensitive information. We are assured that channels are vetted to ensure that they contain no personally identifiable information, and there are no ‘sensitive’ match terms e.g. keywords relating to pornography, medical, gambling, tobacco or alcohol.

Consent and Participation

To adhere to the highest principles of data protection, any system that processes personal information must require informed consent. Users must be fully aware of the system in which they are participating and should be given adequate notice of the operation of that system. Ideally individuals would consent to this participation by opting-in, as we have noted above. Phorm’s assurances that users will be given proper notice, plus reminders of their participation in the form of banner advertisements, are a welcome development in an industry that is not known for consumer notice or ongoing consumer notification.

Indeed, the market default for cookie-based consent systems is opt-out. Phorm's implementation matches market practices – albeit with additional consumer choice and notice elements: As one example, Phorm has created a website for exercising participation choice and encourages partners to remind users about opt-out rights. We hope that they will endeavour to be included in the more popular ‘opt-out’ resources online.[6]

We would still like to hear more about this form of 'encouragement' to clarify the role of Partners in ensuring privacy practices are pushed to the highest level possible. Communications surveillance laws at the very least require consent to be re-affirmed at regular intervals particularly as multiple users may make use of a single Internet connection and machine.

[6] For instance, consumers can use http://www.worldprivacyforum.org/cookieoptout.html or http://www.networkadvertising.org/managing/opt_out.asp

If the advertisements themselves were to include information about participation in the system and the ability to switch the service off or on, this would be a strong step forward. Industry practice is moving in this direction as companies with stronger privacy practices are notifying customers on a per-ad basis how to manage their privacy preferences.

We previously raised a number of issues relating to this issue in our interim assessment. Phorm has subsequently responded.

- If a user blocks all cookies (or manages cookies on an opt-in basis), these users will have to be informed about how their traffic is managed by the Phorm system. We asked: if there is no cookie present does the traffic still get processed? The reason we posed this question was because we felt it was important to be clear to users that if they choose not to participate in the system at all then their traffic is not being processed. We are now confident that users who block all cookies are detected and handled as if opted out. The traffic is still processed by the ISP (as the opt-out status has to be determined) but it is not analyzed by Phorm. Moreover, if the opt-out is detected, then the IP address is blacklisted, temporarily, so that no further Webwise processing takes place.
- A user regularly deletes cookies -- could this lead to re-enrolment?. We are now assured that if a user blocks cookies from the webwise.net domain, then they are essentially opted-out.
- A network-level opt-out. That is, a user should be able to notify his or her ISP that he or she is uninterested in participating in the advertising scheme altogether and this would result in a permanent non-processing of Internet traffic. As we covered above, Phorm is currently working with its ISP partners on developing such a scheme. We would expect this issue to be resolved prior to deployment.

One of the additional benefits of Phorm's technology is its anti-phishing service. This is a very interesting and potentially privacy-enhancing technology but only when properly implemented. Internet-service blocking is highly controversial and has faced extensive public scrutiny and criticism. We are optimistic that users can still choose to access a site that is 'blocked' and that future visits are not regulated. Furthermore, Phorm has assured us that opting out of their system also allows users to opt out of phishing protection – should they wish to do so. The ISP can configure the period for which that choice persists.

Identity, Traceability, and Security

Phorm is very careful in the design of its system and in its public information avoid processing or storing personally identifiable information. Phorm's system itself does not process IP addresses and promises that it does not link back to ISP's subscriber databases.

Moreover, while each user is assigned a unique ID, the UID is a random number that in itself contains no additional information about the user. This number is only used by the browser and the Phorm system, and is not made available to advertisers, publishers, or any other party.

There is a natural concern that if an external attacker gain access to the required information to re-link the individual and the UID. In such a situation, however, such an attacker would have to also gain access to the data in the ISP’s channel server, have decoded the data and filtered by the reference in the UID. In this attack, the information that the attackers could gather would be limited to a list of timestamps and advertising categories which are guaranteed not to be in sensitive subjects and to be impossible to reverse-engineer to discover the original websites browsed or keywords encountered. In short it is very hard to see what gain there might be. Others have commented that an attacker could request an advert using a Phorm identifier of another user. Upon inspecting the advertisements the attacker would learn about the advertisement interests of a user. But this is probably true of any system that profiles users based on their transaction history. This does not excuse this situation, however, and Phorm should conduct a security analysis of these types of risks and consider the use of encryption when appropriate.

On a related matter, Phorm's privacy policy responsibly notes that Phorm may disclose information to third parties under 'legal requirements'. We enquired as to what kind of information Phorm and its system actually holds that may be of interest to third parties. This of course refers back to the linkability issue: if neither the profile nor the advertising information is linkable to the individual then of what use would such data serve to third parties such as law enforcement authorities? Phorm confirmed this point. After all, the disclosure notice would be addressed to an ISP, and it would be far more useful for that ISP to disclose the clickstream or log data rather than the channel association information held in the Webwise server. Additionally, because of the unlinkability of the UID, law enforcement agencies would first require access to the user’s computer to obtain the UID, which again means that the authorities would have access to far more information than the Webwise server could disclose.

Linked to the above two points, however, a further security scenario arises: we asked if there was a malicious insider, with complete access to all the traffic and transactions, could re-identification take place? Or could any level of traffic analysis generate personal data about the user, the types of advertisements served, and the user's IP address? Phorm promises that all Phorm staff undergo privacy training and the company has a security policy in place. If a malicious Phorm insider could gain access to the stored channel:UID:timestamp triples and to data to and from the channel server, the stored data would give no access to personal data, and could not reveal the advertisements served historically, nor procure the user's IP address. The traffic data would give only the data digests used for channel matching (containing a URL and page keywords) and the ads that were served, but no IP address. It is therefore unlikely that this could be used to identify the user or obtain personal data.

For general security assuredness, Phorm has undergone a review by IBM to confirm the security of its data capture software. Furthermore, and importantly, Phorm has publicly and repeatedly offered to be independently reviewed by security specialists or privacy advocates.