80/20 Thinking Ltd

First Stage (Interim) Privacy Impact Assessment

For

Phorm Inc.

February 10, 2008

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 document serves as an Interim (first stage) report that will lead to the publication of a full PIA in March 2008.

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.
- Working collaboratively to develop a sustainable privacy framework within the organisation.
- Conducting privacy training to all *Phorm* staff.
- Auditing the privacy policies.
- Developing an outreach and stakeholder engagement process.
- Creating a rapid response privacy reporting & response regime.
- Follow-up for nine months, involving meetings with the executive team.

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, if not all, of the 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, 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 Interim report will provide a foundation for a robust and ongoing privacy infrastructure for *Phorm* by setting out and examining key criteria. The aim of the final report will be to recommend a specific and sustainable programme to achieve this aim.

This PIA takes into account the May 2007 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.

Table of Contents

EXECUTIVE SUMMARY

- In our view, *Phorm* has successfully implemented privacy as a key design component in the development of its *Phorm* Technology system. In contrast to the design of other targeting systems, careful choices have been made to ensure that privacy is preserved to the greatest possible extent. In particular, *Phorm* has quite consciously avoided the processing of personally identifiable information.

- However, despite our positive findings regarding Phorm's approach to privacy protection we are disappointed that 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.

- We broadly agree with the positive findings of the 2007 Ernst & Young privacy examination, but remain concerned that the scope of that report was based almost exclusively on conditions applying to the US privacy environment. Public sensitivities, regulatory conditions and other factors vary substantially according to geographical location.

- We are encouraged by the spirit of openness shown by *Phorm's* executive team. A clear willingness to engage with and respond to this examination has, in our view, provided a strong foundation for development of a strong and sustainable privacy commitment by the organisation.

- Based on the information and documentation we have reviewed, 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). However the technology may prompt wider (albeit often perception based) privacy and intrusion concerns.

- This initial assessment has not had the opportunity to examine the privacy practices of *Phorm's* partner organisations, but our understanding of the technical elements of *Phorm* Technology leads us to the view that there are sufficient design protections in place to maintain fundamental user privacy regardless of potential adverse technology adopted by third parties and partners.

- We believe that *Phorm* Technology offers a high standard of privacy and data protection. However, there is a serious risk that the product will be perceived as invasive. This risk arises because of the plethora of invasive products and programmes currently being deployed across the Internet and elsewhere. The *fact* of having one's Web activity analysed will, in the minds of some, be an intrusive act, regardless of legal analysis.

- 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.
- In our view, *Phorm* should ensure that ISPs clearly communicate with their users about the issues involved in *Phorm* Technology surveillance, and actively and regularly pursue users' consent. We believe this approach may be crucial to mitigating potential concerns about surveillance.
- 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'. Considering how legal protections vary by country, far more information is required for users to ensure their confidence in the data processing.

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. PIA's are also designed to help embed responsible privacy practice and to promote fully informed policy, program and system design choices.

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

INITIAL RISK ASSESSMENT

Phorm's technology (hereafter referred to as '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 ensure that privacy is

preserved. In particular, Phorm has quite consciously avoided the processing of personally identifiable information.

These design choices still give rise to some concerns regarding the protection of privacy. We outline these concerns below. Of course it is possible that many of these can be mitigated through careful design and implementation.

Without adequate openness and transparency, however, consumers, partners, the media and the general public may have a vastly different interpretation of the privacy-friendly nature of Phorm's system. We therefore identify these risks for Phorm to resolve in clear language and training materials for users and clients, and to reconsider in future design iterations.

The documentation of these risks and the methods of risk mitigation in this report are a key component of a privacy impact assessment and will be included in such an analysis in the near future. 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.

The Perception of Selecting Traffic for Sensing

Phorm is careful to note that only a small component of Internet usage is actually being processed. However there is immense public concern regarding the monitoring of Internet usage, and if poorly explained and managed, this current wave of concern could seriously damage trust in Phorm's system and in the ISPs who choose to implement Phorm's technology.

Media attention will likely jump immediately to this dynamic and may warn users that their ISPs are monitoring all their online activities. Even if more educated coverage notes that only web-browsing is covered this will not resolve immediate responses from audiences that the system is 'spying' on their activities online to the profit of ISPs.

Purpose Re-specification and Communications Surveillance

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.

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.

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.

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

Does the system ignore more 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. Regardless, it 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. Similarly, as profiles are developed 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.

Ideally some form of black-list of sites should be included, or a white-list with clear exclusion processing. For instance, even though Phorm's system excludes forms, and therefore would exclude content from sites where an individual is drafting an email, and also excludes https traffic which therefore excludes many webmail service providers, users would need strong assurance that the process through which they read emails (on less-secure platforms) is not also being monitored.

Can user-sensitive URLs be excluded?

While Phorm is careful to note that HTTPs pages are processed this is perhaps more a matter of an inability to gain access to the content of these pages because they are encrypted. Are https-requests not logged at all? That is, 1080-requests tend to be from servers where users have an existing relationship, e.g. their banks, travel agents, mail providers, and places where the user shops. If this information was to be logged by an ISP this would make users feel spied upon because their ISP would know which services he or she makes use of. Phorm must ensure that it is not using information about these sites in any way, e.g. URL data.

We are aware that only widely-viewed pages will be used, possibly to limit profiling to highly specific user data. This is certainly a positive development. Phorm must communicate this fact to end-users.

Similarly, 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, is in itself personal or sensitive information. For instance, if a channel is able to discern that a user banks online, uses a non-online insurance company, this could be seen as personal information particularly where the user's bank and insurance company could be known to the profiler. Therefore clearer information is required about how the profile is developed and how this information is combined with the channels.

Consent and Participation

To adhere to the highest principles of data protection, any system that processes personal information must require consent on an opt-in basis. As Phorm's system involves a form of communications surveillance then optimal protections would involve opting-in.

The market default for cookie-based consent systems is opt-out however. Phorm's chosen implementation matches market practices. Phorm goes some way to mitigate this concern by creating a website for opting-out and encourages partners to remind users about opt-out rights.

We would 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.

If the advertisements themselves include information about opting out, 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-add basis how to manage their privacy preferences.

Further challenges exist and clarifications are required.

- 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. That is, if there is no cookie present does the traffic still get processed? It is 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.

- If a user regularly deletes cookies then this would result in that user being monitored again. Ideally a user would 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. Is such an implementation possible?

- With limited information about the channels and profiles, a user may be concerned about seeing which 'channel' they have been linked to and the means through which this decision was made. Phorm must develop educational materials for users to understand this process. Similarly, Phorm must explain how many possible channels there are in case users are worried about being segmented in great detail.

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. We are unsure if users can fully opt-out of this service and in fact users should be asked to opt-in to any service that regulates, in any way, what sites they may or may not access. Failure to provide an opt-in process could raise significant public attention even if the guiding purpose is beneficent.

Identity, Traceability, and Security

Phorm is very careful in the design of its system and in its public information avoid processing 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.

Concerns remain, however:

- Can cookies lead back to users in any way? Of course it is merely a unique identifier but a unique identifier can still be linked to individuals. Can an external attacker gain access to the required information to re-link the individual and the UID? Even if this was possible, what potential gain could there be for an attacker?

- Phorm's privacy policy responsibly notes that Phorm may disclose information to third parties under 'legal requirements'. Considering how legal protections vary by country, far more information is required for users to ensure their confidence in the data processing. We would be interested to know 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 the profile nor the advertising information

not linkable to the individual then of what use would such data serve to third parties such as law enforcement authorities?

- Linked to the above two point, 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 persona data about the user, the types of advertisements served, and the user's IP address?

Although the security statement in the privacy policy is a responsible statement, Phorm's security policy and security processes should be audited regularly.