February 18, 2011

Via electronic filing

Hon. Donald S. Clark
Federal Trade Commission
Office of the Secretary, Room H-135 (Annex P)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Phorm Inc's Comments on: Protecting Consumer Privacy in an Era of Rapid Change
A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS

Dear Secretary Clark,

Phorm is pleased to submit these comments regarding the FTC's proposed framework for Protecting Consumer Privacy in an Era of Rapid Change. As a company whose product is based on cutting edge technology and which has developed its offering from the ground up with privacy at the forefront, the questions raised by the Commission are ones to which we may provide considered input.

Although we have no current operations in the US, Phorm has started operations in Brazil with two of the country's leading Internet Service Providers, Oi and Telefonica. In cooperation with participating ISPs Phorm's, "PhormDiscover"offering provides consumers with a safer and more personalized Internet experience. This service is offered to consumers through their ISPs by means of unmissable notice and opt-in choice prior to any data collection or use. Consumers who use PhormDiscover will find both more relevant content and more relevant advertising on participating web sites. To use the content offering online publishers need merely accept a freely available PhormDiscover content widget which can be incorporated on their sites and which allows the publisher to surface content more relevant to participating consumers. Web sites may also, but do not have to, use Phorm's OIX (Open Internet Exchange) interest-based advertising product. This offers publishers and networks the ability to deliver relevant display advertising to the right user at the right time, thereby maximizing the effectiveness, yields and value of their inventory.

Phorm's technologies are revolutionary in their approach to consumer privacy. They utilize a level of unmissable notice and opt-in consent previously not seen in the online advertising industry. Owing to privacy by design, Phorm has built a commercial platform on a bare minimum of consumer data. Unlike other interest-based advertising systems, Phorm's OIX does not capture potentially personally identifying data such as IP address or browsing history including specific searches or page views. Alternatively, the OIX works by storing only: 1) an interest category, 2) an anonymous, randomly assigned marker/tag and 3) a time stamp to allow the purging of data after a maximum of six months.

The system works by recording membership in broader interest categories through the observation of more granular triggers but without recording these specific triggering events. By way of example, an anonymous marker may be associated with a "photography interest" channel through the consenting user's visit to any number of sites or pages dealing with "photography" without the need to store the specific site or page which lead to the broader categorization. The OIX provides further protections by placing certain channels or category types strictly off limits. For instance, among others, Phorm prohibits any channel the specific intent of which is to target children under the age of 13 or persons with sensitive medical conditions.

As a company which believes deeply that addressing consumer privacy issues is fundamental to the success of an advertising supported Internet publishing system, we recognize that the issues raised by the Commission come at a pivotal time for the online ecosystem. This ecosystem according to the Internet Advertising Bureau's latest full year report, http://www.iab.net/insights_research/947883/adrevenuereport, generated 22.7 billion dollars in the US. While this is an impressive revenue number for an early stage industry, and while growth in this sector has performed far better than in other areas of the economy, it should not be forgotten that these revenues need to finance a staggering array of online content and services relied on by consumers at low or no cost including: news, weather, entertainment, blogs, online video, mail, and social networking.

Additionally according to the same report, 89% of these revenues are controlled by the leading 50 companies with 71% controlled by only the top 10. It is clear that for this industry to continue to meet consumer expectations it must both increase overall revenues and diversify that revenue across the broader array of companies providing consumer benefit, including high speed access providers; and it must do this in a manner that meets the legitimate consumer privacy concerns addressed by this framework.

Phorm is dedicated to building a system which addresses consumer concerns on both sides of this debate. We have created technologies with unparalleled privacy protection while also allowing for the commercial viability of the ecosystem which can provide low or no cost access to highly demanded content and services. We applaud the Commission’s work in this area. We have attached our responses to some of the Commission's specific questions in Appendix A. We are also available for any follow up questions the Commission may have.

Sincerely,

J. Brooks Dobbs
Chief Privacy Officer
Phorm

Appendix A
Detailed Answers

Scope

Phorm agrees with the Commission in their understanding that in a dynamic and evolving environment it is prudent to expand some level of protection to all data which may reasonably be linked to a specific consumer, computer or other device. We do not believe, however, that the distinction between identified and non-identified data has been completely eroded. While in theory it is possible for any unique pseudonym to be made identified through connections of either other full identifiers or a series of attributes which reasonably allow identity to be triangulated, it is also possible through careful product design to build a system which disallows such linkages. Such systems, which work to the consumer's advantage, should not be disadvantaged relative to systems which collect granular data and allow such triangulation. Treating all players in the same manner without regard to the steps they take to retain anonymity would be a disincentive to adopting the the privacy by design philosophy the Commission correctly endorses.

By way of example, many online advertising systems today associate online activity both with granular event level data including IP address, unique cookie, browser information and the specific pages viewed or terms searched. In these cases, cookies who's values are randomly assigned may be misclassified as anonymous solely because their values do not directly contain personally identifying information (PII) such as name, email or government identifier. It is, however, often the case that the cookie's random value is associated with other identifiers such as customer_id, order_id, account_id or the like, which allows the cookie (and all activity associated with it) to be tied directly to a fully identified individual through programmatic data lookups.

In other situations the linkage of external PII is not direct, but it may still occur. For instance, where IP address and granular activity is linked to a cookie such linkage creates the problem that any future identification of the IP address immediately identifies all granular data connected to such an IP address and/or the cookie associated with that IP address. Even where such direct identification does not occur - where unrestricted association of browsing and search activity is mapped to a cookie or IP address - the ability to triangulate identity with event level data is often possible as has been demonstrated by the 2006 release of AOL search data.

Phorm has taken an alternative approach to the use of pseudonymous identifiers. We never allow external identifiers such as customer or order_id to be linked to our markers. Nor do we allow our cookies to be shared externally. We do not allow event level data like specific searches or pages views to be linked to a cookie. We do not log IP address, which may be able to externally referenced as PII. Additionally, we never share data (other than aggregate advertising performance statistics). We log only a marker as a pseudonymous cookie, a broad interest category triggered from multiple but unknown specific events and a time stamp so that data can be purged at a maximum of 6 months.

While Phorm believes that even such carefully limited data collection should be subject to commensurate protections, we do not believe that such irreversibly anonymized data should be treated in the same manner as data, which in the hands of its controller, could (or is) easily tied to an identified individual for reporting, targeting or other purposes.

Although definitional lines are not well drawn as to what data is anonymous, what data is linkable and

what data is designed to be linked, unless we recognize that distinctions may exist we will never be able to fully implement important standards such as accuracy, authentication, repudiation and notice of material change which are appropriate for identified data but which may be impossible or conceptually different for non-identified data. Phorm believes that there are a number of objective factors which may be considered in aiding in the determination as to if a given identifier is "PII". These include:

- Is the intent of such an identifier to link disparate systems where one system is anonymous and one is identified (order_ids, customer_ids, etc.)?
- Is such an identifier linked to other unknown identifiers?
- Is such an identifier linked to an IP address?
- Is such an identifier linked to event level page views or searches?
- Are there restrictions in place limiting what externally may be associated with such identifier?
- Is information linked to identifier shared with other parties who see data (e.g. IP address) from a different context?
- Are identifier and linked data transferred to third parties?
- How long is data stored both by initial collector and by other parties with whom it is shared?

While this may not fully categorize all data, it may serve to reclassify data which had previously been referred to as anonymous.

Companies should promote consumer privacy throughout their organizations and at every stage in the development of their products and services

Incorporate substantive privacy protections

Phorm supports the four principles enumerated in section V(B)(1): *1) companies that maintain information about consumers should employ reasonable safeguards – including physical, technical, and administrative safeguards – to protect that information, 2) companies should collect only the information needed to fulfill a specific, legitimate business need, 3) companies should implement reasonable and appropriate data retention periods and 4) companies should take reasonable steps to ensure the accuracy of the data they collect*.

Phorm appreciates the reasonable standard applied to principles 1, 3 and 4 and believes particularly that the degree to which data is or is not identifiable plays a crucial role in determining the levels of care required to meet these standards. By way of example, it is problematic to subject data which is not identifiable by the controller to the same accuracy standard as data which is fully identified. Provisions for access to non-identifiable data is challenging because, by definition, the controller cannot insure access is limited to the "identified" subject (as identity is unknown to the controller). Beyond this however, Phorm believes all data should be subject to reasonable safeguards, collection should be limited to that which is needed to achieve the specific business purpose communicated prior to collection and should only be stored for a reasonable retention period.

With respect to privacy enhancing technologies, we believe that the best privacy enhancement is privacy by design. It is far better to design a product which limits retention and collection than to retrofit anonymization and shorten retention periods for poorly designed systems.

Maintain comprehensive data management procedures

Phorm agrees with the Commission's concern that it has been difficult to bring together a full range of stakeholders to develop and deploy both privacy enhancing technologies and broadly scoped self-regulation. Phorm believes that a broadly designed privacy framework such as the one forwarded by the Commission is helpful in moving towards cross industry privacy protections. We further recommend that in a time of rapidly changing technology, it is in consumers' best interest not to differentiate protections based on the use of given technologies, but rather to provide guidance and requirements based on actual data practices.

Companies should simply consumer choice

Commonly Accepted Practices

Phorm agrees with various commentators who have expressed concerns regarding the ubiquity of data collection by parties unknown to consumers. In contrast to systems which provide no notice or which offer no or limited choice with respect to data collection, Phorm offers unavoidable notice and requires consent before any data collection or use. Phorm does share industry concerns however that creating a definitive list of what is or is not commonly accepted is a very difficult exercise. Rather, we would suggest that guidelines be established which would let data collectors better understand if their practice is or is not commonly accepted in the context in which it occurs.

With respect to data enhancement, Phorm is concerned that for an identifier in the online world to be linked to data in the off-line world there needs to exist a common identifier in both realms. Cookies and IP addresses don't exist in the off-line world where data is instead linked to true identity. It is for this reason we fear that often such enhancements of online data occur by linking off-line identity to an online cookie to allow off-line data to be brought online. Often this link is created through data points such as customer_ids or order_ids. Such ids, which may errantly be referred to as anonymous, directly link to individuals in the real world and are therefore ideal for mapping off-line data to online cookies. Although such a practice does not constitute online behavioral advertising (OBA) under current self-regulation, we believe such practices are not commonly accepted and should be subject to meaningful notice and choice.

Practices that require meaningful choice

Deep Packet Inspection

Phorm agrees with the Commission in their belief that, similar to other forms of OBA, the use of deep packet inspection for marketing purposes would fall outside of the scope of what is commonly anticipated by consumers. Phorm's DPI based OBA solution is presented to consumers with meaningful notice and opt-in consent prior to both data collection and use. We also concur with the Commission's concerns that choice is often not easily understood by the consumer. We note that many "opt-out" systems today are limited in a number of ways: 1) they are presented only after data collection; and 2) do not allow for true opt-out of data collection but rather only a limited opt out of behavioral targeting. We share concerns that this limited choice may allow data to be left identified for reporting or other non-OBA purposes. Phorm has built its choice mechanism to be presented prior to collection, to allow for complete opt-out of data collection and use, and to allow for persistent, non-cookie based, choice.

With respect to adding additional levels of consent for the use of deep packet inspection past other non-commonly accepted OBA practices, we are left to wonder what those might practically be. If it is considered that all non-commonly accepted practices should *offer consumers clear and prominently displayed choices* and that such choice should be *at a time and in a context in which the consumer is making a decision about his or her data,* it might be asked what standard lies beyond that? It is further worth asking if notice and choice should not be commensurate with actual data practices (granularity of data retained, identifiability of data retained, sharing, retention, etc.) rather than on a specific technology used to achieve those practices. Phorm believes strongly that consent is tied both to actual practice and the degree to which that practice is commonly understood to be occurring.

Sensitive Data Categories

With respect to sensitive data categories, Phorm believes there to be two potential classes of sensitive categories. While Phorm feels there are certain categories which should be universally off limits for the purpose of advertising, we also recognize that there is a second class of categories for which a more nuanced approach is required.

In the first instance there are categories, such as but not limited to, sexual preference, proclivity to adult content, minority status or interest in life impacting medical conditions, which Phorm universally considers sensitive. Because these categories are generally considered sensitive by all potential members, Phorm has decided to always prohibit their use. Phorm maintains a more extensive list of prohibited categories but looks to industry and regulators for a more formalized approach on determining what these categories ought to be and how in practice providers should evaluate a given category's membership in this exclusion list.

On the other hand, Phorm recognizes the existence of categories which may, to some populations be considered sensitive, but which to other populations may not be sensitive. Staff has previously cited "interest in balding remedies" as an example of a category which to one group, 40+ year old men, is not sensitive, but to another group, senior women, may be considered sensitive. In these cases were the potential for sensitivity is mixed, Phorm would recommend two criteria be applied prior in determining the sensitivity of such category: 1) the percentage of the likely membership who would find such categorization derogatory and 2) the degree to which membership in such category is or is not linked to identity. In the hypothetical "balding remedies interest" channel where the channel has been constructed in such a way that the vast majority of potential members are also 40+ year old men (for instance where membership is triggered by content consumption at a site targeting middle aged men), this would contribute to the channel being considered less sensitive. Also in cases like Phorm where no other data is linked to the membership marker this would further contribute to the category being less sensitive. Alternatively if the provider were to know more information about the category member such as IP address, specific URLs visited, customer or order_ids, or login information, this would increase the degree to which such categorization would be considered sensitive potentially adding to the argument that such category should be excluded.

Phorm has taken an industry leading approach to the treatment of potentially sensitive data categories both by maintaining a list of prohibited categories and by strictly minimizing data relating to all anonymous members of interest groups. We look forward to the Commission's further guidance on this matter.

Children's Data

Phorm prohibits the creation of any advertising channel with the specific intent to target children.

Special choice for online behavioral advertising: Do Not Track

Phorm shares the Commission's concerns that there have been significant failures with respect to notifying consumers about data collection and that much collection online occurs outside of what is commonly understood or accepted by consumers. Given these failures it has been difficult or, in some cases, impossible for consumers to exercise choice. We echo concerns of commentators who feel existing choice mechanisms are both fragile, often being unintentionally revoked, and imperfect in their ability to fully limit data collection for a wide range of uses by the collector.

Owing to these concerns we understand the desire to create a Do Not Track (DNT) mechanism, but we have strong concerns about how this process may unfold and the potential for unintended consequences to the detriment of consumers. Our first concern is that if a DNT mechanism evolves in a manner which significantly reduces the utility of online advertising, demand from advertisers will fall and accordingly so will publisher revenues. While this may seem like an industry problem, it quickly becomes a consumer problem given that many publishers are already exploring alternative means for content financing as they seek to operate profitably online. Should advertising revenues fall, many publishers and consumer service providers will have their hands forced into directly charging consumers for access to content or services.

We are also concerned that discussion of Do Not Track is occurring in the absence of a specific plan. Indeed there have been a number of proposals all of which seem to fall broadly under the same Do Not Track moniker, but which vary extensively in their potential for collateral damage. Two specific proposals, which have been discussed enough to comment on, are addressed below:

Tracking Protection List / Content Blocking

On or about December 7th, 2010, Microsoft announced that it would add Tracking Protection List (TPL) functionality to the upcoming release of its Internet Explorer browser, a browser which by most estimates still maintains over 50% market share. The Microsoft blog describing this release (HTTP://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx) demonstrates a method by which third party list provider could supply a list of *tracking domains* which will be excluded from the domains to which the browser will allow a connection in a 3rd party context.

While we applaud any attempt to empower users to exercise *considered choice.* We are concerned that such a tool, if widely adopted, might have implications beyond the understanding of most consumers implementing such functionality. Unlike other proposed mechanisms which may place limits on data collection – potentially *reducing* the value of online advertising – ad/content blocking will *remove* the value of online advertising potentially crippling an industry worth 23 billion dollar a year in the US alone. If widely adopted, this could dramatically upset today's ecosystem where most content and numerous services, through advertising support, are available to consumers at no direct monetary charge.

Additionally, this solution is a disincentive to individual industry actors to improve practices.

Even if a participant in the ecosystem adopts positive, consumer friendly data practices a failure at any part of the systems essentially punishes all members equally because so many parties are often involved in the chain of delivering online advertisements. As the vast majority of display advertising is delivered by only a handful of players, should even one of these players be placed on a popular TPL the entire ecosystem of ad supported content could be catastrophically impacted. While such a change may benefit the relatively few content providers seeking direct consumer payment, most ad supported sites will be negatively impacted, and it seems clear that consumers stand to lose on both counts.

Do Not Track Header

An alternative Do Not Track proposal calls for the addition of a new persistent HTTP request header which could be used to communicate user tracking preferences to all recipients of web communications. Critics of this proposal have pointed out that this method relies on the recipient to act on such instruction and does not itself prevent the communication of data, but, in contrast to other methods, this may offer significant advantages:

The first advantage is that ads may be delivered, albeit with potentially less value. This less draconian step does not immediately cut off all revenues but rather removes revenues based on practices which may particularly concern the consumer.

The second major advantage is the decision with respect to how to treat the choice can be made more granularly and contextually. For instance it may be possible that a given domain runs services on both opt-in and opt-out capacities. It may be reasonable to assume that a global statement of "Do Not Track" should apply to all non-commonly accepted opt-out practices but should not apply to services to which consumers have expressly consented or requested.

Do Not Track is a tempting alternative owing to the prevalence of non-commonly accepted data practices, but it is one that should be considered judiciously as serious unintended consequences to the detriment of consumers are possible or even likely. Given the relatively small number of browser manufacturers, it would also be worth the Commission's consideration to examine the market impacts and who is advantaged by proposed changes where consumers are potentially disadvantaged.

Companies should increase the transparency for their data practices

Improved privacy notices

Web site privacy policies have been criticized for being overly complex, dense and beyond the grasp of the average consumer. Phorm agrees with the Commission that consumers should be made aware of and presented with choice for non-commonly accepted practices. However, the difficulty raised by one of the web's underpinning technologies, HTML, is both the sheer number of players that can be seamlessly involved in the creation/delivery of a page and the inability for any given player (including the first party) to speak for the other parties. Phorm has addressed this concern by providing unmissable notice and gaining consent prior to data collection and use. We share the concerns of commentators who note that there may be tens of discreet data collectors on a given ad supported page who are both unknown to the consumer and may, as well, be equally unknown to the publisher/1st party.

As a practical matter the architecture of the web has led to extreme specialization with very little

marginal cost to integrate multiple, dynamic players into the same page. So long as these efficiencies are taken advantage of, it will be extremely difficult to build a system where one party is responsible for providing notice for the practices of other, potentially unknown, participants . Improvements, however, are possible in three areas:

1) *Limiting the number of players per page*. While specialization always has a role, there is an opportunity to reduce the number of players. Where technologies within ads like pixel tags (which allow data collection by third and fourth parties) make communicating practices difficult, those pixels' ability to dynamically call numerous other pixels make the explanation of practices by publisher practically impossible.
2) *Change the party responsible for notice and gaining consent to the party whose practices are at issue*. If a data collector wishes to collect data in a manner not transparent to either the first party or the consumer, that data collector should be responsible for presenting consumers with clear and prominently disclosed choice.
3) *Greater adoption of machine readable technologies*. A recent legislative draft proposal called for 15 specific pieces of notice to be given for every broadly defined covered entity collecting data on a specific URL. To better understand the implications of this seemingly innocuous request, and by way of example, on January 17th, 2011 the home page of a top 20 website showed 20 discreet covered entities (other ad supported sites were similarly positioned). If each covered entity were to make their required 15 disclosures hypothetically averaging 2 sentences in length, each viewer would need to read 600 sentences of privacy disclosure to understand the practices of the home page alone! While limiting the number of players may help, better uses of technologies like P3P which could be used to automatically compare practices with user preferences could play an important role in reconciling this problem.

Reasonable access to consumer data

Access to data has long been a fundamental part of fair information practices, but to date such access has always assumed the ability to protect such data through repudiation. In other words, it has always been assumed that the controller of data and the subject of data could agree on the fact that the data related to that given subject; and that the controller and subject could agree on a credentialing system to allow the subject to access such data while others could not. As we look to expand protections of information to all data even data, which in the hands of the controller, does not allow said controller to accurately know to whom such data relates, we necessarily run into an inability for the controller and subject to agree on a credentialing system. Today's profile viewers (often referred to as ad preference managers), when used as intended, can provide consumers with a view as to what information a given controller has associated with a particular cookie, but such systems are only as secure as the subjects' computer. For example, it is fairly trivial for spouse 1 to gain access to spouse 2's profile by simply accessing the profile viewer from their computer. *Authentication* here is not possible as the controller does not know which viewer, spouse 1 or spouse 2, is the legitimate subject of the data.

Beyond this question of repudiation of non-identified data, a further question of data ownership presents itself. For many of the most popular ad serving systems, the data relating to the ad serving cookie is owned and controlled not by the provider of service but rather by the end publisher, advertiser or agency. As a practical matter there may be hundreds of discreet entities all of whom control data related to a single service provider cookie. These parties do not necessarily share their practices (or the practices of *their* partners) with the initial service provider. Many of these players, according to the service providers' own statements, have practices not covered by those of the service provider. This

begs the question of how a single profile viewer can accurately make transparent the practices of potentially hundreds of discreet parties all with different relationships to the data.

Given these concerns, Phorm asks the Commission for clarification as to how access requirements should balance data security and subject access rights for non-identified data.

Material changes

Phorm believes that data should be collected and used in a manner consistent either with what is commonly accepted by the consumer given the circumstance or in a manner consistent with the prominently given choice presented before the start of such practice(s). Where data is collected under one expectation (either by notice or accepted practice) and a controller wishes to use such data in a materially different manner, such as to share it with an unaffiliated third party or to make it identifiable, such a practice should be considered non-commonly accepted and the party wishing to engage in the changed practice should first seek the consent of the affected party. Where such practices deal in data which is not reasonably identified by the controller (and where such change does not seek to allow data to be identified) a lesser standard of consent should be required than where data is known to pertain to an identified subject.

Consumer education

As commentators have noted, there is tremendous opportunity for improving consumer education. Proposals for addressing choice with respect to non-commonly accepted practices will undoubtedly make a dramatic difference in consumer understanding of how data is being used by business. It will be equally important for business, industry associations, government and consumer groups alike to make clear the other side of the equation. The commercial use of data funds the majority of web based sites and services which today require no direct financial payment by the consumer. In a world where consumers are presented with only notice about how their data is used by others, absent the knowledge of how this use provides direct and indirect benefit, we risk undermining the potential for systems, like Phorm's which yield consumer value in a manner respectful of consumer preference.

-Ends-