February 17, 2011

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Secretary Clark:

PrivaCeed Inc., a recently-launched company dedicated to bridging the gap between commercial interests and consumer privacy in the online ecosystem, appreciates the opportunity to comment on the Federal Trade Commission's preliminary report addressing the complex topic of consumer data collection. We support the Commission's ongoing efforts to protect consumers, both online and offline, and applaud the Commission's attempt to strike the correct balance between commercial innovation and privacy protection.

PrivaCeed was founded with the goal of striking that balance as well. One of our core objectives is to enable buyers and sellers of online advertising to maximize their ability to utilize data through solutions that protect user anonymity and enhance consumer privacy. It is in the context of that mission that we submit our comments on the Preliminary Staff Report, and we respectfully request that the Commission consider these comments as it evaluates its proposed framework.

Our comments focus primarily on three of the topics for which the Commission requested responses – the scope of the proposed framework, privacy by design and consumer education. Although we are addressing these topics individually in this response, we believe that they are interconnected and should not be examined in isolation.

Scope of the Proposed Framework and the Continued Relevance of Identity

PrivaCeed believes that the principles embraced by the Staff Report can and should apply to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, but we do not believe that such data linkage should represent the sole distinction drawn by the Commission's framework. Certain fundamental principles underlying the PII/non-PII distinction – in particular, the context in which data is held – remain and will continue to remain relevant and significant, and need to be addressed.

The very notion of PII speaks to information that can identify a person or is otherwise related to an identified person. Seemingly innocuous bits of information, in the right (or wrong) context, can be personally identifiable. What may appear to be a random string of letters and numbers may in fact be a frequent flyer number in the hands of an airline or a customer ID in the hands of a health insurance provider, in which case that apparently random string is in fact PII to those parties (as a proxy for the actual personal data they hold). Further, such data as, for example, gender, birthday, and college alma

mater could enable the identification of an actual individual by a party that has the capacity to combine and associate those three data points. While there may be significant differences of opinion with respect to the potential effects of information that can be linked to a specific computer or device, it should be undisputed that information linked to specific identifiable person has the greatest potential to cause harm, regardless of how expansive the concept of harm is constructed.

PrivaCeed agrees that the analysis should not be limited merely to determining whether particular data is, by itself, personally-identifiable information. Rather, the appropriate inquiry should examine not only whether certain data is PII per se, but also the context in which data is held – in other words, the ability of parties either to determine identity through accretion of discrete pieces of data or to link discrete pieces of data to the identity of a particular individual, whether directly or indirectly. Eliminating that ability has proven problematic for technological "de-identification" methods, as noted by the Staff Report, but the shortcomings of currently utilized methods do not and should not erode the distinction between PII and Non-PII. Rather than attempting to de-identify data, PrivaCeed's solutions have been designed to *decontextualize* data, thus eliminating the ability of any party to identify an individual.

PrivaCeed's patent-pending data analysis engine creates a wall between online advertisers and the granular pieces of data derived from their advertising activities. Advertisers maintain the ability to measure the effectiveness of their advertising and to deliver relevant ads, but they lose the ability to link that advertising data with other data in their possession or available to them. Consequently, online advertising data is rendered anonymous, as it will no longer able to be linked to a particular individual (or to any computer or other device) by the advertiser or any third party, and commercial practices are aligned with consumer expectations.

Unlike de-identification technology, a decontextualization solution cannot be reverse engineered.

Privacy by Design and the Incorporation of Substantive Privacy Protections

PrivaCeed embraces the tenets of "privacy by design" and challenges the conventional wisdom that an individual needs to be identified in order for an advertiser to reap the unique measurement and targeting capabilities afforded by the online medium. We contend that commercial utility is not predicated on identifying any particular individual, computer or device; highly effective measurement and targeting outcomes can be achieved by identifying aggregated groups associated with particular attributes or actions (including purchases) rather than the individuals within those groups. Highlighting the efficacy of solutions that utilize such data minimization practices is crucial to getting those practices incorporated in a self-regulatory framework and, by extension, gaining widespread industry adoption.

As the provider of a solution that operates as an "identity protector" within online systems and demonstrates that commercial effectiveness can be achieved through decontextualization and anonymization, PrivaCeed strongly supports both the privacy by design initiative proposed in the Staff Report and the privacy-enhancing technologies model to which privacy by design is closely related. We believe that the incorporation of substantive privacy protections and the development and deployment of privacy-enhancing technologies will be crucial to a healthy and transparent online environment. Incorporating privacy protections into commercial offerings, and cleansing unnecessary identity linkages from the data collected through such offerings, will align online data collection and usage with consumer expectations and eliminate not only the potential for tangible harm to consumers, but also much of the chilling effect referenced in the Staff Report.

In the area of online data collection and usage, there are few, if any, practices more dangerous than false or misleading statements about identity and anonymity. To eliminate these practices, the Commission should exercise its existing authority under Section 5 of the FTC Act and impose significant disincentives for material misstatements relating to identity or anonymity. We urge the Commission to utilize that

authority to ensure that the disincentives for such deceptive practices are at least as great as any commercial incentives for those practices.

Stakeholders should also recognize that there are not only significant legal and brand consequences for bad practices, but also benefits to privacy-enhancing solutions. Data collection and usage and consumer privacy are not necessarily mutually exclusive; stakeholders must work together to shatter the false choice perceived as existing between the two. The Staff Report wisely encourages competition on privacy, and emphasizing consumer interest in the matter should serve to facilitate progress. The incorporation of privacy enhancements should be publicized, and companies that undertake such efforts should benefit due to the increased brand value associated with the consumer trust built as a result.

In addition, we must accentuate the fact that responsible privacy practices do not necessarily represent an impediment to commercial gain. This theme was central to the report that initially endorsed the concept of privacy-enhancing technologies. That report raised the fundamental question, "Is it possible to minimize the amount of identifiable data presently collected and stored in information systems, but still meet the needs of those collecting the information?" PrivaCeed joins the Commission in its dedication to answering that question in the affirmative, and supports the Staff Report's recommendation of reasonable data collection limits.

PrivaCeed believes that the insertion of a "data intermediary" into the online advertising economy could provide one of the cornerstones of privacy by design. Such a trusted third party would serve the crucial purpose of altering the context of data elements collected in the online advertising process, as described above in greater detail. The reduction of data usable by the commercial stakeholders and the cleansing of identity from such data would engender consumer confidence in industry while preserving value for those stakeholders. However, in order for such developments to occur, both the incentives for deployment and the disincentives for deceptive practices need to be apparent.

Increased Transparency – Consumer Education and Privacy Statements

Most consumers do not understand the value proposition of the Internet – Internet users are paying for the content they think is free, and the currency they are using to pay for that content is the data they are passively providing through their interactions with the sites they visit and the search queries they enter. However, no one has explained this value exchange to consumers effectively. Many consumers therefore believe that the payments they make to their Internet service providers entitle them to online content and that the collection of data is an unjustified, gratuitous event. In fact, fees collected by ISPs merely entitle consumers to enter the carnival; they have to pay – usually with data – to ride the rides.

Industry has hinted at the online value exchange in certain contexts. For example, some sites offer users the choice between viewing online content for free if advertisements are interspersed with the content and viewing the content without advertisements but for a fee. The value exchange, however, has rarely been made explicit, and it certainly has not been widely communicated to consumers.

Extensive efforts need to be taken to educate the general public about the data collection and usage ecosystem, both offline and online. Lack of consumer understanding about such data practices is one of the primary causes of the problems the Commission and other stakeholders are seeking to solve. Rapid growth and evolution in this space has only magnified that knowledge gap. Icons and other notice and choice tools, when appropriately implemented, provide a valuable first step in educating online consumers about the parties collecting data and for what purposes, but they address the issue only at the level of the individual advertisement. They do not clarify for users that they are paying for content with the currency of data.

No single constituent is at fault. As the companies utilizing the consumer data generally rely on service providers to collect that data, the concept of "data collection practices" is not central to their consumer messaging. On the other side of the coin, data collecting service providers are generally business-to-business solutions that are not consumer-facing, making it difficult to serve any practical educational function.

PrivaCeed aims to be consumer-facing even though we will not collect or independently utilize consumer data. As a trusted third party whose services will be relied upon by companies seeking to publicize their responsible privacy practices, we hope our clients will display our logo as a means of disclosing those practices. That logo will direct consumers to the PrivaCeed site, which will contain explanations not just of PrivaCeed's services but also of the role of data collection in the online economy.

PrivaCeed also applauds the Commission for emphasizing the fact that privacy policies have become too lengthy and incomprehensible to consumers. Through our offerings, we intend to enable both our clients and other commercial participants in the online value exchange to make more concise statements in their privacy policies. Our solutions are designed to modify the myriad of current data collection and usage practices that already may be causing site owners, often unwittingly, to make false or misleading statements in their privacy policies about the activities occurring on their sites.

An opaque or obscured statement in a privacy policy certainly makes it difficult to communicate the value exchange; however, a false or misleading statement may induce consumers to participate in the value exchange when they otherwise would not. PrivaCeed's services are designed to align data collection and use practices not only with consumer expectations but also with the expectations of site owners, thereby enabling them to make clear and accurate statements to consumers.

Conclusion

PrivaCeed thanks the Commission for its consideration of our comments and for its ongoing efforts to protect the privacy of consumers. We share that commitment, and look forward to working with the Commission to develop holistic solutions to the issues at the core of this complex industry.

Should you wish to contact us regarding our comments, please do not hesitate to contact Matthew Haies, PrivaCeed's Chief Executive Officer, by email at matt@privaceed.com or by phone at 917.721.9249.

PrivaCeed Inc.

Matthew Haies, Chief Executive Officer
Greg Tagaris, Acting Chief Technology Officer