~~Draft 2~~
February 18, 2010

~~Mr. Christopher Olsen~~Federal Trade Commission
~~Bureau of Consumer Protection~~Office of the Secretary
~~Federal Trade Commission~~
600 Pennsylvania Ave NW
Room H-135 (Annex P)
Washington DC 20580

Re: Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers

~~Dear Mr. Olsen and Members of the Federal Trade Commission:~~
Ladies and Gentlemen,

~~On behalf of SAS, I~~SAS appreciates this opportunity to provide comments on the Preliminary FTC Staff Report on Protecting Consumer Privacy. Similarly, SAS appreciates the recognition within the staff report about the need to balance consumer protection with ~~providing enterprises (both for-profit and non-profit)~~continuing ~~with the~~ incentives and flexibility for businesses to enable them to ~~continue to~~ innovate. While SAS believes there is much that is positive about the proposed framework, we do offer observations~~We offer comments~~ on several aspects of the preliminary report:

- Scope of coverage
- Privacy by design implications—specifically relating to service providers and commercially acceptable practices not requiring consent
  - ~~First party marketing~~
- Implications relating to social media
- Requirements relating to access, particularly ~~relating to~~ for non-consumer facing enterprises

Formatted: Indent: Left: 0.54", No bullets or numbering

~~I.~~ *Introduction and Background*

A bit of background about SAS may be helpful to understanding our comments.

SAS provides data integration, business analytics[1] and information reporting software to business, government, educational, and non-profit users. SAS does not sell to consumers, nor does it directly interface with consumers. This is a fancy way of saying that ~~we help our~~SAS helps its business and government customers unlock the power of the data that they collect so that they can make better decisions relative to their own products, services, customers, business operations, etc. By way of example, ~~we~~SAS helps ~~our~~ financial services customers understand potential fraud within their credit, debit, and online transactions. ~~We~~ SAS helps ~~our~~ manufacturing clients understand potential

[1] By business analytics, we mean the full range of statistical analytical capabilities, including predictive analytics and data mining, data visualization, forecasting and econometrics, model management and deployment, operations research, quality improvements, statistics, and text analytics.

safety issues in their manufacturing and supply chain processes by evaluating information received through warranty cards and customer call centers. ~~We~~SAS helps ~~our~~ pharmaceutical customers assess the effectiveness and efficacy of drugs in clinical research trials. ~~We~~ SAS helps ~~our~~ health care provider customers assess data—both structured and unstructured~~,--~~ to better understand how and why potential errors may be made, to help them improve the safety of health care delivery. ~~as a means of improving health care safety.~~ - SAS~~We~~ helps law enforcement clients understand potential money laundering and other suspicious ~~fraud~~ activities, to improve our safety domestically and from a national security standpoint. ~~Our~~SAS software products are used by retail customers like grocery stores and department stores , to ensure that each store in the chain carries products appropriate for its customer base. In this capacity, SAS enables, through data analysis, more customized marketing offers (such as the ~~provide customized offerings to their clients, which may include t~~the generation of coupons or special offers at the point purchase or recommendations about other products), as well as tailored markdown strategies. ~~. They~~SAS analytics are used by our customers to survey social media networks, to assess what is being said about their products—as a means of understanding potential issues relating to product and reputation. And, ~~They are~~SAS analytics are used by our business customers to assess how their customers are maneuvering through their webpages and responding to their own targeted product offerings.

This is by no means an exhaustive listing of the problems that our customers are trying to solve by using SAS' powerful software. But these illustrations are important for several reasons. First, while SAS historically was a software product that was downloaded or otherwise installed on our customers' hardware, increasingly our customers are demanding a hosted version. ~~of our software.~~ SAS has established a line of business which provides software-as-a-service and enterprise-hosting solutions, as SAS Solutions OnDemand. While the hosting can take a number of forms, this does mean that in some instances personal data is transmitted by or on behalf of SAS customers to SAS servers. Data that is~~i~~ sensitive is encrypted when transmitted to or from SAS, and protected while stored at SAS. But, it is the evolving way in which analysis is being conducted that gives rise to many of the concerns that we have about the FTC's proposed framework.

Second, SAS Solutions OnDemand only collects the information that our customers provide to us or direct us to collect. ~~**Brian, can you elaborate on this – under what circumstances, and is this "public record" data?**~~ ~~Similarly, we do~~SAS does not further share the data that ~~we~~is received; the results of the analysis are transmitted back to our client, and only to our client~~.~~[2] ~~-~~. Likewise, we are not using the data that we receive to market our own products to consumers, or in any other way to enhance our business. We are~~,~~ merely acting as a service provider to our enterprise users. The service ~~that we are providing~~ is tantamount to being another "back office" function such as data processing, which is very different from what an information broker does, and ~~very d~~ thus should raise very different ~~in terms of~~ consumer expectations. Indeed, we would submit that most consumers would understand that data processing is occurring and that most would implicitly consent to such functionality~~. As a service provider, SAS is already regulated by a plethora of requirements to ensure privacy and security. If our services are not secure, the company's reputation would suffer irreparable damage and it would not remain in business for long. (The company celebrates its 35th anniversary so has a lengthy history of achievement in this area.)~~
. SAS notes that there is already much on the books in terms of sectoral privacy requirements that govern such service providers. And, if the statutory and case law were insufficient to discipline our conduct, maintaining our

[2] ~~There are some instances in which the data does not come directly from our client, but potentially through an unaffiliated third party. These instances are extremely rare. Some clinical trials may be conducted by unaffiliated third parties, with the results sent by that entity to SAS for analysis. In the education setting, some states deploy unaffiliated third parties to collect and process testing results, with SAS used as the analytical engine.~~

brand and reputation—and remaining as a viable business—provides perhaps the most robust discipline to ensure that SAS protects privacy and provides security.

Third, SAS Solutions OnDemand typically does not access the identities of the individuals captured within the data sets. In fact, from an analytics perspective, knowing the identities of~~, nor do we actually care about the identities of~~ specific individuals is not central to the services that we offer. For example, it is not important for either us or our clients to know who is communicating on social media sites; it is important, however, to know what is being said. Similarly, while it is not important to know that "Betty Smith" participated in ABC clinical trial, it is important to know that the clinical trial involved a number of different demographic groups, and the reactions of each of those demographic groups to what was being tested.

~~*II. Specific Comments on the Proposed Framework*~~

As ~~we said~~noted at the outset, SAS appreciates that the report is both preliminary~~,~~ and flexible. We also value the comment in the executive summary that recognizes that the analysis of data has led to substantial consumer benefits, given that the "acquisition, exchange, and use of consumer data not only helps to fund a variety of personalized content and services, but also allows businesses to innovate and develop new products and services that offer consumers convenience and cost savings." Equally, we support the notion that any framework must be "delivery neutral"—ie applicable to both online and offline commercial entities. That said, we share a number of concerns and observations.

~~*i. Scope of framework.*~~ ~~We do have a number of concerns with the framework.~~ Our first concern involves what we believe the framework implicitly assumes: that all companies are collecting data only to build customer profiles to better target advertising. Clearly, this is happening, both on the first party and third party basis. While ~~we~~SAS expresses no opinion about third-party marketing, we ~~would sugges~~submit~~t~~ that having customized marketing is a consumer benefit. More to the point, though, there ~~might be~~are any number of other reasons to create "profiles" that have nothing to do with advertising. For example, to understand whether a particular transaction is an outlier (and thus potentially fraudulent), for any specific banking customer, it might be helpful to have a clear idea of that customer's purchasing habits. That picture is also a "profile" of sorts; not being able to develop a comprehensive view in this circumstance would be harmful to that customer because the outliers become indistinguishable from any other transaction. Similarly, with the delivery of health care becoming much more personalized (meaning specific treatments are recommended based on a genetic map—or, as importantly, not being recommended), being able to fully understand individual patient characteristics becomes critical. We raise this point because we are concerned that all these activities are being unreasonably characterized as "advertising" or marketing, which raise some negative and unfavorable connotations.

Similarly, we believe that the report is not particularly precise when it describes third party actors. In some segments of the report, all third parties are synonomous with "information brokers" or data aggregators. ~~Similarly, the report suggests that a~~Other parts of the framework suggest that all data processors are information brokers, again ~~-~~without providing support. ~~In other parts, the draft recognizes that there is a concept~~The report is also inconsistent in that it seems to understand that there are ~~of~~ "service provider", and that some "service providers may provide benefits that are deemed more legitimate than others." In short, there are many different types of actors in this ecosystem. Some of these actors—and activities~~---~~ raise more concerns than others, but the broadbrush effort to depict all as potentially ~~harmful of consumer privacy,~~ intrusive to privacy ~~which~~ is neither warranted nor helpful. We would ask the FTC to

Formatted: Font: Italic

carefully think through what it intends and to use a great deal more specificity when articulating both the actors and the harms that it is seeking to capture and avoid, respectively, within its framework.

With that ~~overal~~general~~l~~ background, we raise an issue about the broad applicability of the framework. The framework, in its preliminary version, would apply to any commercial entity "that collects, maintains, shares or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device, regardless of whether such entities interact directly with consumers." The ambiguity in the phrases "maintains…or otherwise use" and "reasonably linked to a specific consumer regardless of whether such entit[y] interact[s] directly with consumers", ~~for raise concerns for u~~ concerns us for several reasons. Is receiving data and keeping it secure considered to be maintaining data? Similarly, what is a "reasonable linkage", particularly if the nexus between the entity and the consumer should not be considered? ~~i~~If SAS does not have the means to decrypt or unscramble individual identities, would that be sufficient to fall outside the phrase "reasonably linked to a specific consumer", even if someone else might be able to unlock the identities? More important, while we are analyzing data for someone else and not our own benefit, does that constitute "use" of the data? We would submit ~~since the purposes of the analysis are not f~~that the usage relates back to our business customers such that any requirement about privacy etc. should fall on that entity, not us.~~or our own product-oriented or marketing purposes?~~ Our client's choice of analytical platform should not dictate the privacy regime that applies to us, particularly when the benefits for enhanced ~~to the~~ consumer ~~of~~ understanding from understanding our role seem limited at best. Conversely, the fact that our business customer has chosen a hosted model should not alleviate their obligation to ensure privacy and security, which is a potential outcome of having platform dictate compliance requirements.~~.~~ In short, if the purpose of the ~~requirement~~framework is to enhance a consumer's understanding of what kind of data is collected or the scope of data that is being connected, we would submit that a more active and direct interaction ~~intention~~ be the minimum requisite before the framework applied, as well as more precise definitions and illustrations relating to collection, maintenance and use of data. In the absence of direct interaction or a clear showing that broader regulation greatly enhances consumer regulation, we would also submit that having the full framework apply to service-oriented enterprises is simply not warranted. ~~At a minimum, then, SAS offers that there should be a closer nexus between the consumer and the corporation before the framework is said to apply.~~

Formatted: Underline

~~*We note that the report's drafters seem to recognize that there are circumstances under which not all aspects of the framework should be applicable to all enterprises. For example, while consumer choice is a central premise of the framework, choice is implicitly granted in certain "commonly accepted business practices", which would include when such business practices are undertaken by service providers. Indeed, in most instances, requiring the application of the framework to service providers does not appreciably enhance consumer protection where the actions being undertaken are only to provide support and service. Consequently, we would urge the drafters to more narrowly tailor the scope of the framework to ensure that unintended entities are not captured by the full scope. Instead, we would urge to specify compliance obligations only in those circumstances in which requiring compliance by a service provider would enhance consumer protection.*[3]~~

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

~~*ii.* *Privacy by Design*~~

SAS notes its general support of many of the concepts incorporated within the privacy by design effort outlined in the framework. That said, we do raise a number of issues. The first relates to the comment that "companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services." The opening "companies should…" suggests that **all** companies should comply with the directive, irrespective of whether that companies directly interacts with consumers. This is part of the problem of having a framework of such broad application, as already noted.~~which is part of the problem that is created by having the scope of the framework as breathtakingly broad as in the discussion draft~~ . As stated above, where the "company" only interacts only in the B2B or B2G space, such a privacy by design mandate does nothing to enhance consumer privacy. Thus, the statement should be limited to those companies that clearly collect and interface with consumers. That said, to the extent that these B2B and B2G enterprises might receive consumer data, then there is an obligation to ensure security for such data and that it is not further shared beyond the consent. ~~That is much narrower presentation that what is reflected in the framework's statements.~~

SAS' ~~S~~second~~, we have concerns related~~ comment relates to data collection and retention ~~issues~~[4]~~.~~suggestions within this section. Specifically, the requirement that~~ We raise concerns about the suggestion that~~ companies should only collect the information needed to fulfill a "specific, legitimate business purpose" may be too confining. ~~."~~ While ~~we~~ SAS ~~appreciate~~acknowledges the concern that consumers ~~do~~may not know what data is being collected or that data is being used for purposes not envisioned by that consumer, the framework's requirement ~~this~~ raises real practical questions. For example, fraud takes many forms, but because one does not know at the outset what might be fraudulent (including the use of an identity), what data would be "specific" to "only" detecting fraud? As the fraud evolves, or grows into a concerted effort by more than one individual, how would a company that specializes in fraud detection distill only the data that relates to fraud, and nothing more? (We can raise similar concern relating to product improvement and brand protection, and the myriad of other legitimate uses for which companies are collecting data.) In short, more guidance about what is envisioned by this parameter, and what is not envisioned would be helpful and that the FTC be cautious about becoming overly prescriptive.

~~*iii.* *Consumer Choice*~~

Formatted: Font: Italic

~~[3] For example, because service providers might "handle" consumer data, it would enhance consumer protection to require service providers to ensure at least minimum levels of security commensurate with the type of data, scope of the enterprise and potential risk. A more surgical approach provides greater clarity, and greater certainty for service providers. To the extent that service providers do more with the data than simply provider service on behalf of another company, the framework should apply to those extracurricular activities.~~

Like other aspects of the preliminary framework, SAS is supportive of the FTC's efforts to balance privacy choices, foster clearer expectations for consumers, and its recognition that there are some "commonly accepted practices" for which consent is implicit. One of these areas where consent is implicit relates to understanding data. Assuming that the consumer understands data is being collected, that same consumer understands that the collection is not occurring in a vacuum. The collecting organization ~~will~~ undertakes to evaluate and understand that data~~,~~ to be able to continue to innovate (~~both~~ in terms of product offering, product safety and marketing issues.) Thus, because we believe the analysis of data is implicitly understood, we would suggest that that FTC add a general category to its list of commonly accepted practices relating to "first party data analytics". Whether the analysis is undertaken directly by the collecting organization, or as an outsourced activity is irrelevant~~.~~ ~~(~~ provided the outsourcer only provides analytical support and makes no further use of the data~~)~~. (As noted, there may be genuine debate about what the consumer understands with respect to data collection. The burden of ensuring that the consumer knows data is being collected should fall on the collecting organization before it is collected. Our comments relate to what happens after the data has been collected.)

With the addition of ~~that~~an "exception" for first party data analytics~~, category,~~ SAS ~~would~~ suggests several other clarifications to the list of commonly accepted practices that do not require consent.~~.~~ While the section clarifies towards the end that consent is not necessary relative to service providers, in the absence of clearer direction about the scope of the framework, this is an important exception that should not be buried within the text of the section but should be clearly articulated up front.

We also offer that several of these categories should be expanded, and commentary that the examples are for illustration purposes only and are not exhaustive. ~~For example, t~~The category of "fraud prevention," for example, should be expanded to include "fraud detection" (which, we note, is the phrase that is used within the categorical description.) Clearly, fraud that cannot be detected cannot be prevented, and the issue now is that those intent on committing fraud change their practices once they believe their old methods have ~~been detected~~become "public". To stay current and ahead of evolving fraud patterns, both online and offline enterprises are moving to increasingly sophisticated, and varied approaches to detect and prevent fraud. These include ~~incorporating~~the use of static business rules, but also analytical methods that statistically link behaviors and patterns together. By limiting the description of the category and the terminology for the exception, one might limit the usefulness of this consent exception. (Indeed, one can envision those intent on committing fraud "opting out" of data collection and analysis if they had a choice. It is not hard to depict how incomplete data sets would skew both the analysis and the results.[5]) Similarly, the category related to product and service fulfillment should be expanded to include analytical efforts to understand warranty or product problems. Moreover, many of the illustrations provided are not particularly robust or representative of the kinds of activities or the kinds of technologies that are increasingly being deployed. Thus, it would be ~~very~~ helpful for the FTC to note that the illustrations are for explanatory purposes only and are not meant to exhaust the types of activities that would fall within the commonly accepted practices.

~~iv.~~ *Choice and Social Media Applications*

Formatted: Font: Italic

SAS appreciates both the novelty of social media, and the growing popularity of social media outlets as a means of communication. Given that appreciation, we do not necessarily express an opinion about how or when consumer choice options should be conveyed about "consumer information." That said, the comment that "if consumer

[5] ~~Because fraud detection necessarily considers financial information, we would also assert that requiring affirmative express consent, as suggest later in the framework, could severely frustrate this critical function. Thus we would also assert that where sensitive information might be necessary for these commonly understood processes, that the draft clarify that express consent not be required. See, for example, page 61 of the preliminary draft.~~

information will be conveyed to a third-party application developer, the notice-and –choice mechanism should appear at the time the consumer is deciding whether to use the application, and in any event, before the application obtains the consumer's information" ~~does raise some concern~~is problematic. Specifically, the lack of a definition for the phrase "consumer information", and the clear intent to move away from traditional notions of "personally identifiable information" raise~~s~~ significant questions as to who must give notice and under what circumstances ~~should~~must notice be given. For instance, if a company is monitoring a social media site to understand what is being said by consumers about its products, does that constitute the collection of "consumer information"? We would submit that such monitoring is not collecting consumer information because the intent is not to identify ~~what~~ individual~~s~~ consumers – and thus to target that consumer for additional information. It is to detect trends and patterns that may reflect issues relating to brand, reputation, or product, which are legitimate concerns of any enterprise. ~~may be doing or to share that data with other enterprises.~~ In fact, ~~this~~the ability to monitor social websites in this manner ~~would~~ both enhances consumer protection and is expected by consumers as part of the company's warranty and product development/product fulfillment responsibilities. Consequently, we would ask the FTC to provide more definitive guidance as to what it means ~~in this circumstance~~with respect to social media and ~~about~~ the collection of consumer information and to ensure that the commonly accepted practice exceptions are sufficiently broad to apply irrespective of developing technologies or communication media.[6]

~~v.~~ *Increased Transparency: Access to Data*

Formatted: Font: Italic

The preliminary report raises important questions about the ability of a consumer to access data collected, including asking how consumers might discover which entities possess information about them to seek access. We would submit that a "one size fits all approach" to third parties would not appreciably enhance transparency. ~~, and i~~In some circumstances, permitting consumers to access data could ~~engender more important~~create other issues. As we have stated, not all third parties are in the business of collecting data, and not all third parties who have access to such data are using that data for their own unaffiliated purposes. Most of the data that is shared is obscured, so that the service provider cannot identify specific individuals. Thus, to place a burden on non-consumer facing service providers to give access to data by consumers creates completely different privacy issues ~~raises other privacy issues~~ that are not addressed in the report. We think in this circumstance that if the consumer is concerned about the accuracy of the data, his or her recourse should be limited to the enterprise that collected it in the first place with no suggestion about recourse to the non-consumer facing service provider.

Similarly, there are circumstances, particularly involving law enforcement and investigation, in which maintaining a data set that has not been "cleansed" may actually be more important that ensuring "pure" data in all circumstances. These usages ~~For example, some fraud investigations rely on the ability to see how data evolves over time. Let's take the following example. Jane Smith lives at 123 Main Street. She has a bank account at Bank of America, and credit cards with Wells Fargo. In terms of fraud detection, though, Wells Fargo sends its account data to XYZ analytics processing. XYZ searches for Jane Smith at 123 Main St;, Jayne Smith at 123 Main Street, Jane Smyth at 123 Main St. etc. All of these accounts are statistically linked and can be identified as the same person. Under the FTC's proposal, Jane Smith would be permitted to access XYZ's files and tell them to standardize on Jane Smith at 123~~

[6] ~~The FTC asks specifically about what kind of notice and choice should be required for "the many companies that collect and use data without directly interacting with consumers. Information brokers, for instance, may acquire consumer data from a variety of sources and use it for purposes never intended." Although the report notes that choice in these contexts is difficult, we raise objection with the implication that every company that is "using" data is somehow an information broker. Indeed, one can argue that a service provider is "using" data, but that the usage is envisioned within the construct of the underlying consumer/collector relationship. As we said at the outset, we would strongly encourage the FTC to articulate what it means by using data to more clearly understand when there is or should be an obligation to give notice and obtain consent.~~

~~Main Street. Assuming that this happens, once this happens, XYZ would lose any visibility into what might be happening with any of these other variations on "Jane Smith", which means that it may well not detect other activity that is linked to Jane Smith that could raise identity or authentication issues. Because of the potential interference with important social objectives, as well as the direct privacy issues that the access and correction issue raises, we would strongly encourage the FTC to move very deliberately in this area.~~ depend on being able to see how pieces of data evolve over time. If the data were "cleansed", and the investigator able only to look at certain instances of the data, or certain usages of data, potentially whole areas of investigation become closed or limited. Just think, for example, if TSA or intel analysts could only look at data sets that spelled the Christmas Day bomber's name as "Omar Abdullmatulab". If all pieces of data within the set were cleansed so that they only considered "Omar", new pieces of data that might come to light spelling his name as "Umar" (or any other variation) would necessarily be excluded. Certainly, the analysts would never be able to "connect the dots" in this scenario, and thus unable to detect threat, much less a concerted threat. All of us are hurt by this, and we believe that this social hurt outweighs any benefit that allowing access and cleansing in all circumstances might afford. Obviously, this is a fairly extreme example, but does reflect concerns that relate to all sorts of different types of investigations. Our point in raising this is that while there may be individualized harms that could occur when certain types of collection agencies have inaccurate data, the framework's proposal to standardize and cleanse raises serious unintended consequences.

~~vi.~~ *Conclusion*

We appreciate the opportunity to provide perspective on the preliminary framework and welcome the opportunity to work with the FTC as it refines and further considers its propos~~ed framework~~als.

Sincerely,

Katherine Hahn
Director, Federal Government Relations

Formatted: Font: Italic