Enclosure to Victor Nichols' Letter dated February 17, 2011

Comments on the Preliminary FTC Staff Report
on Protecting Consumer Privacy in an Era of Rapid Change

Experian appreciates this opportunity to provide comments on the Federal Trade Commission's ("FTC" or "Commission") *Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* ("Staff Report").[1] As a company, we work very hard to provide information products and services that benefit consumers and businesses alike, and part of that work involves placing a premium on consumer privacy.

This letter contains a detailed explanation of our comments, along with some background information about our company that we hope you will find helpful. Our key points are as follows:

We agree with the Commission on the following matters:

- The assessment that"[t]echnological and business ingenuity have spawned a whole new online culture and vocabulary … that consumers have come to expect and enjoy"[2] is absolutely correct. We believe this presents our company with both an opportunity and a responsibility to ensure that we meet evolving consumer needs while providing exemplary consumer protection.

- We commend the Commission's continued recognition that in today's digital marketplace, self-regulation provides the ability to quickly adapt to new trends and technologies and offers effective protection for consumers.

- We also agree that the scope of the Staff Report should cover information collected in all media. (However, we presume that the Staff Report does not intend to cover data collected under existing sector-specific legal regimes, which could create inconsistent or redundant obligations.)

- The "privacy by design" framework endorsed in the Staff Report could potentially serve as a useful tool for evaluating companies' privacy and data security policies, but is not comprehensively explained. We would welcome the opportunity to work with you and others to further define this concept.

- Like the Commission, Experian believes data should be collected and retained only for a legitimate business need. Here as well, we would welcome the opportunity to work together to advance our shared goals of consumer protection and privacy.

---

[1] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report (Dec. 1, 2010) (*hereinafter* "Staff Report").
[2] Press Release, FTC Staff Issues Privacy Report Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010).

- We also agree with the positions that choice is not necessary for certain data practices; that the collection and use of consumer data for first-party marketing purposes does not require choice; and that this exclusion is appropriate irrespective of the channel in which the marketing occurs.

- Experian supports efforts to increase the transparency of corporate data policies whenever feasible. We appreciate the acknowledgment in the Staff Report that the associated costs can sometimes be prohibitive and that the costs to consumers could outweigh the benefits.

- Accordingly, we agree with the Staff Report's suggestion of a sliding scale approach to providing consumers with access to their personal data and the opportunity to correct the information they find.

- Finally, Experian fully supports efforts to anonymize and de-identify data when appropriate. We agree that corporations – no matter the industry, scope or size – should understand the sensitivity of the data they collect, use and transfer, regardless of whether the data is personally identifiable.

However, we were disappointed in the following elements of the report:

- Regrettably, it fails to recognize the value of third-party data, which provides significant benefits to consumers. We feel so strongly about its value both to our services and to consumers that we've shared several examples in the following pages. In our view, public policy must carefully balance any restrictions on the collection and sharing of third-party information with consumers' best interests.

- We have deep reservations regarding new requirements that would impose mandatory accuracy or data access and correction standards. This is because current consumer protections, combined with the nature of marketing information in general, render new requirements unnecessary.

- We also have concerns with recommendations that would require inflexible data collection standards. Such standards are unworkable and could undermine innovation and the development of new technologies, services and even consumer protection processes.

- In this regard, the Commission's Final Staff Report should be accompanied by an economic analysis of the impact any substantive recommendation contained in the Final Staff Report might have. It is critical that any legal changes in the collection and treatment of personal data be accompanied by an analysis that represents a thoughtful approach to understanding how our frail economy may be impacted by the Commission's recommendations.

- On the matter of consumer choice, the Staff Report's approach falls short of the goal of alleviating the burden on consumers and businesses, and perhaps most important, the Commission's approach to identifying practices that do not require choice is far too narrow.

- The Staff Report does not provide sufficient detail around what constitutes a "commonly accepted practice" in this arena, nor does it define the criteria so as to include other practices as consumer preferences evolve.

- Further, the Staff Report appears to consider any data sharing with a third party for marketing purposes to be outside a commonly accepted practice, but fails to provide a basis for making a distinction. This approach does not reflect the complexity of today's business practices.

- The proposal to require choice prior to the collection of information or a "real-time" notice goes too far and could interfere with evolving technologies. Additionally, we are concerned that the report includes no analysis of the proposed costs and impact of changes associated with such notice and choice procedures.

- Though we agree with the principles of "privacy by design," we believe that the creation of rigid new standards could be counterproductive and have significant inadvertent economic consequences that have not been adequately explored in the proposed framework.

- Finally, while we support efforts to anonymize and de-identify data when appropriate, we suggest that the Commission should not adopt guidelines that would weaken incentives to use this data, thus reducing the demand for it. Specifically, with respect to this issue, we are very concerned with the report's suggestion that IP addresses should be considered personally identifiable.

Experian appreciates the opportunity to further engage in a dialogue with the Commission staff on these important matters.

***

I. Background on Experian Products and Services

Experian is a leading global information services company, providing analytical and marketing services to organizations and consumers to help manage the risk and reward of commercial and financial decisions. Experian is comprised of a family of companies that are tied together by a focus on consumer data. We partner with organizations around the world and operate in more than 90 countries. Experian maintains its North American headquarters in Costa Mesa, California.

We combine our unique information tools and deep understanding of individuals, markets, and economies to help commercial, non-profit and government entities establish and strengthen consumer and customer relationships. Experian provides information services in all

sectors of the economy, including e-commerce, financial services, retail and catalog, telecommunications, utilities, media, insurance, automotive, leisure, manufacturing, property, and government.

For more than 50 years, Experian has also compiled consumer data and used the information to help facilitate more targeted direct marketing, historically through the U.S. mail. Especially in recent years, there have been many changes in technology and the manner in which organizations communicate with and advertise to their current and prospective members or customers. Experian now uses its compiled databases to facilitate multi-channel marketing and advertising through the mail, telephone, and email to help advertisers reach a more receptive audience.

The emergence of Experian's Digital Advertising Services brings the same compiled marketing information and direct marketing principles to television, online, and mobile advertising. As an example, and in response to consumer, media and policy concerns about tracking across Websites, new technologies are being introduced in the marketplace that result in targeted ads that do not require collection of website browsing behavior across unaffiliated third-party websites. These technologies deliver anonymous (or de-identified) and encrypted household demographic information, that is linked to cookies acquired from qualified websites where clear notice is provided and consumers are given the choice to opt-out. These cookies are not used to collect online information, such as websites visited, in order to target advertisements. These new technologies result in advertisements with sound privacy and security features that are not only relevant to consumers but also bring a higher return on investment for advertisers.

Experian serves large and small corporations, government entities, and non-profit organizations around the world. In our work, Experian has adopted five global information values that guide our use of marketing and other data. These values—balance, accuracy, security, integrity, and communication—align with the fair information practices and principles ("FIPPs") embraced by the Commission, as well as the Commission's international colleagues in the Organization for Economic Cooperation & Development, the European Union, and the Asia-Pacific Economic Cooperation organization. These information values, combined with sectoral laws where applicable, put into practice our belief that the use of information must benefit both businesses and individuals, while simultaneously meeting the privacy expectations of consumers.

Experian applies these information values according to the laws, customs, and consumer expectations of the nations and regions in which we operate. In turn, information policies, built upon our corporate values, more specifically define how information may be used. For example, our privacy and compliance team works closely with Experian's business units to perform a proactive information values assessment prior to all data sourcing and product development launches. This self-regulatory audit incorporates subject matter experts from every relevant functional area of the company, including product development, technology, legal, compliance, information security, risk management, and data acquisition. Based on our understanding of the Staff Report's concept of "Privacy by Design," Experian believes that our assessment process represents a real-world application of this concept.

In addition, Experian provides consumers with notice, choice, and education about the use of personal information through our collateral materials and information available on each of our public-facing websites. We also allow consumers easily to make their preferences known with respect to the use of their personal information. Experian provides consumers with multiple ways to opt out of having their personal information used for marketing. Furthermore, we provide our clients with the ability to utilize available suppression files.

Experian has played and continues to play a key role in the development and implementation of industry self-regulatory systems such as the Direct Marketing Association's *Guidelines for Ethical Business Practices* and the advertising coalition's emerging *Self-Regulatory Principles for Online Behavioral Advertising.* We believe that these self-regulatory systems, when combined with existing sectoral laws and the FTC's authority to enforce current law against unfair and deceptive practices, provide a workable and flexible means to address issues regarding transparency and choice. These self-regulatory efforts will continue to evolve alongside the digital marketplace in order to address consumer issues that emerge in the future.

As the steward of some of the largest consumer information databases in the world—all regulated by applicable laws, regulations and industry self-regulatory standards—Experian has unique insight into not only how third-party data is collected and shared, but also how it is used by commercial, non-profit, and government entities. In addition, Experian also provides services for improving consumer financial literacy directly to millions of Americans who are our direct customers. As such, we are familiar with the marketing challenges facing commercial organizations from both a third-party and first-party perspective.

Informed by this diverse background, well versed in the responsible use of consumer data, and as a long-standing member of both the Direct Marketing Association ("DMA") and the Consumer Data Industry Association ("CDIA") and supportive of the comments filed by the these organizations.

II. Third-Party Sharing of Data Provides Significant Benefits to Consumers

Regrettably, the Staff Report fails to recognize the value of third-party data, and presents a framework that incorporates disincentives to third-party collection and sharing of consumer data. The use of third-party data by institutions provides significant benefits to consumers. In particular, we are concerned about the following Staff Report recommendations:

- Excluding all collection and use of data by third parties from the Commission's listing of "commonly accepted practices" and therefore subjecting them to a choice mechanism;
- Requiring companies to provide consumers with "reasonable access" to the data maintained about them;
- Requiring first parties to provide an opt-out mechanism when enhancing customer data with third-party information;
- Requiring merchants to take extraordinary and unworkable steps at the point of sale to gain consent for third party sharing; and
- Including a "real-time" pop-up notice for data collection that might be shared with third parties.

The collection and sharing of third-party consumer data, whether online or offline, provides numerous significant benefits to consumers. For instance, the use of third-party data lowers prices, fosters competition by providing small entities with access to consumer data that larger companies already maintain, creates consumer convenience, provides consumers and businesses with information that allows them to compare competing offers and services, facilitates access to consumer and business credit, and reduces fraud.

Third-party data also enhances the relevance of first-party marketing efforts, especially for small businesses and start-ups, which rely heavily on marketing to attract prospective customers but do not have the capacity to collect or maintain data for this purpose. In today's economy, the availability of third-party data significantly reduces barriers to new firms entering the marketplace. Even large, first-party marketers with extensive customer databases rely on third-party data to provide better services and more relevant marketing offers to existing or new customers. Marketers cannot rely solely on their own transactional and experience data to make offers that are tailored to specific individual or households, because such data probably does not include basic segmentation factors for effective marketing, such as gender, age range, type of dwelling and the like. Thus, for example, imagine how ineffective for the company, and frustrating for recipients, a marketing campaign would be if advertisements for lawn mowers are sent to those who live in apartments and condominiums.

In addition to increasing the relevance of advertising, third-party data helps marketers (1) identify the best branch or retail locations; (2) conduct consumer and market research; (3) increase innovation in product development; (4) increase innovation in advertisement placement; (5) determine media placement strategies for advertising (newspaper, magazines, Internet, email, billboard, telemarketing, direct mail, etc.); (6) reduce irrelevant marketing communications; and, (7) obtain analytics to determine which websites offer the most relevant venue for placing both behavioral and contextual advertising. Third-party data is also crucial to providing services that consumers value and use, such as price comparison shopping websites.

Moreover, many different types of organizations rely upon third-party sources to ensure the accuracy of consumer databases that are used to allocate resources and serve the needs of people. For example, over 40 million Americans will move this year. Organizations that serve the public, including non-profits and government agencies providing critical social services or securing public health and safety, therefore routinely undertake "data hygiene" processes to ensure that addresses in their records are up-to-date. These organizations also use third-party data to understand and serve the needs of the citizens in their charge. Politicians at every level, as well as the major political parties, use third-party information to enhance voter records and communicate with voters. In a free society that relies upon information, third-party information is the lifeblood that fuels countless services that people depend upon and expect.

As a national framework for privacy evolves, it is essential that the final Staff Report acknowledge the important role third-party data plays in our society and economy. The Commission should be cautious in proposing any new restrictions on the collection and sharing of third-party information in light of the significant benefits that such information provides to consumers. We are concerned that the proposed framework, which recommends disincentives and restrictions that affect third-party data use, would have negative effects for consumers and businesses.

III. Data Collection and Retention Limits Are Best Practices, but Should Not Be Regulatory Requirements

The "privacy by design" framework endorsed in the Staff Report potentially offers a useful tool for evaluating companies' privacy and data security practices at various stages of the development of their products and services. Indeed, we believe that the substantive principles of "privacy by design" are all incorporated into Experian's information values self-audit process to enhance our ability to identify potential vulnerabilities in our privacy practices. These principles include provision of notice and consumer choice where appropriate, data security, reasonable data collection limits, sound retention practices, data accuracy, access and correction where appropriate, and compliance with sectoral laws and self-regulatory regimes. We firmly believe that the promulgation of rigid standards or the imposition of onerous obligations would not improve upon the system we have developed and, in fact, could be counterproductive. Experian therefore welcomes the opportunity to work with the Commission and other stakeholders to further define this concept in a manner that is flexible and responsive to businesses' unique missions.

Experian communicates directly with tens of millions of consumers each year, providing us with a detailed understanding of consumers' expectations about how data is used and shared by commercial entities to provide products, services, and benefits. We also gain feedback from the thousands of companies, non-profits and government agencies we serve. Finally, we receive regular guidance from a consumer advisory council we have established and meet with regularly. The insight we gain from these interactions is fed back into our internal audit process to predict how consumers will react to new product offerings. For example, Experian has a corporate process for determining how to handle sensitive information relating to children, health and ethnicity – a nuanced issue that has been proven difficult to codify in law or regulation.

Given our experience, we have particular concerns with the Staff Report recommendation that would require inflexible data collection standards. Such standards are unworkable as legislative, regulatory, or self-regulatory requirements, and we believe they could undermine the development of new technologies, services and even consumer protection processes. The data collection standard proposed in the Staff Report would limit the collection of data to "information needed to fulfill a specific, legitimate business need." This proposal does not reflect practical business models or operations, nor does it recognize that consumers already have multiple options for controlling the collection of online behavioral data through browser settings.

Companies may collect a single piece of data that can be used for important multiple purposes that may not be known at the time of collection. For instance, IP addresses are regularly collected and are absolutely essential in online fraud detection and prevention systems. If collection limitations had been adopted previously in accordance with past legislative and public policy proposals, IP addresses may not have emerged as one of the most important tools for detecting and preventing online fraud. This is only one clear and compelling reason that data protection standards should focus on uses of data, and not the collection of data. A focus on data use is the means by which data has historically been controlled in the United States. Fundamentally changing this focus to one of controlling data collection could impede future beneficial uses of data that was previously collected, and thereby have significant inadvertent

consequences for our economy, which have not been adequately explored by the Commission, economists, policy leaders, business or consumers in general.

Experian likewise has concerns with the Commission's proposals in the area of data retention. Experian supports the premise that data should be retained only for as long as there is a legitimate business need or required by law, but opposes the imposition of specific time limits. Instead, data retention should be viewed as an aspect of data security. Notably, of the 48 states and two other jurisdictions (Puerto Rico and the District of Columbia) that have enacted data security and maintenance laws, none imposes specific time limits. Experian further recommends that any guidance on data retention should recognize that data retention needs vary according to data type and use.

IV. Choice Is Unnecessary for Many Data Practices beyond Those Identified in the Staff Report

Experian agrees with the Commission's position that choice is not necessary for certain data practices. This concept is already embodied in Section 502(e) of the Gramm-Leach-Bliley Act governing the sharing of financial data with third parties. We further agree that the collection and use of consumer data for first-party marketing purposes does not require choice, and that this exclusion remains appropriate irrespective of the channel in which the marketing occurs (whether by postal mail, telephone, email or online, with the exception of online behavioral advertising). Notwithstanding these areas of agreement, the Staff Report's approach to simplified choice falls short of Commission's stated goal of alleviating the burden on consumers and businesses.

First, the Staff Report does not provide sufficient detail for an organization to clearly determine what would constitute a "commonly accepted practice" beyond the list provided in the Report. For instance, the Staff Report identifies "first-party marketing," or the "collection of data from a consumer with whom the company interacts directly for purposes of marketing to that consumer," as a commonly accepted practice. Once that data is shared with a third party, however, the Staff Report would no longer consider this information within the realm of a commonly accepted practice. The Staff Report fails to provide any basis for making this distinction, which fails to capture the complexity of current widespread data uses. As one example, it is both very common and widely accepted for first parties to use third-party data in order to carry out the first party's own marketing goals, and such data matching usually requires some limited data sharing. These practices have been occurring for decades, benefiting businesses, consumers and the economy, with no demonstrable harm that would justify any change in such long-accepted and well-entrenched practices. In this and other respects, the Staff Report does not provide sufficiently detailed guidance to industry.

Second, and most importantly, if the list set out in the Staff Report is intended to be exhaustive, the Commission's approach for identifying practices that do not require choice is too narrow. The definition of first-party marketing should extend to the sharing of consumer data among corporate affiliates and divisions. It has long been recognized that companies may transfer data among affiliates, even in highly regulated areas such as financial data under the Gramm-Leach-Bliley Act, with certain exceptions. Similarly, data enhancement is a common practice that is essential to effective first-party marketing practices, and should be considered

within the ambit of first-party marketing. Because choice already is provided to consumers for the transfer of third-party marketing data under the DMA's Ethical Guidelines, data used for enhancement should not be subject to additional choice. Finally, if the Commission continues to promote the concept of "commonly accepted practices," it should extend the exclusion from choice to cover all relevant exceptions under Section 502(e) of the Gramm-Leach-Bliley Act.

While Experian believes that choice, when appropriate, should be easily available to consumers, it should not interfere with the consumer experience. Experian supports the right for consumers to be able to opt out of having information shared with third parties for such third parties' own marketing purposes. Such rights are already embedded in sector-specific laws, such as the Gramm-Leach-Bliley Act, and in industry self-regulatory standards, such as the DMA's Ethical Guidelines. However, the Commission goes too far in proposing to require choice prior to the collection of information or a "real-time" pop-up notice if information is intended to be shared with third parties. Such a change in current practice would deter and limit first-party marketing and third-party information sharing, along with all the corresponding consumer benefits. It could also interfere with evolving technologies used to improve the detection and prevention of online fraud and the targeting of online advertising.

Finally, the Commission offers no evidence or analysis on the proposed costs and other impact of its proposed changes in notice and choice procedures, including the impact on the consumer experience. For example, it would be costly and burdensome, as well as inconvenient and unfair for consumers, to require consumers to make a decision about whether information should be shared with third parties at a retail point of sale, as the Staff Report suggests, because there is not enough time for clerks to state all the benefits and presumptive costs of such a decision. Training sales clerks to deliver such notices would be unproductive and costly. This is also true of pop-up notices about third party sharing when information is collected in the online, social media and mobile environments. Instead, a consumer's ability to exercise choice should be easily available from the website from which the information is collected, but does not always need to be presented on the page or at the point where the consumer enters his personal information. Nonetheless, it could be helpful for the Commission to explore whether a real-time, pop-up notice might be justified for the transfer to non-affiliated third parties of certain sensitive information, such as financial account numbers or Social Security numbers, for marketing purposes.

V. Current Means of Providing Consumer Access and Correction to Personal Data Sufficiently Protect Consumers

We support the Commission's proposal to increase the transparency of corporate data policies. We further agree with the Staff Report's endorsement of a sliding scale approach for providing consumer access and correction rights for personal data. While certain data uses command a robust access and correction regime, other data uses, such as for marketing or consumer authentication purposes, do not. For this reason, we have deep reservations regarding any legislative or regulatory effort to impose new mandatory accuracy or data access and correction standards on data files. As the Staff Report recognizes, the costs of implementing access and correction for marketing databases would be prohibitive. For the reasons stated below, we believe the costs of allowing consumers to access and correct data in most other cases would also outweigh the benefits.

First, companies that maintain consumer information, such as Experian, already provide broad access to many data practices. Existing laws, including the Fair Credit Reporting Act ("FCRA"), the Fair Debt Collection Practices Act, the Fair Billing Act, the Health Insurance Portability and Accountability Act ("HIPAA"), and the Wall Street Reform and Consumer Protection Act, provide consumers with considerable access to and ability to correct the types of data covered by these laws. Experian's data access and correction standards therefore reflect both applicable laws and our own corporate values, and we believe that they strike the appropriate policy balance.

Second, the Staff Report has not provided evidence of any need for new requirements for accuracy and data access and correction for data used for consumer authentication. The Staff Report states that erroneous data used for consumer authentication could lead to consumer harm, in ways not addressed by the FCRA, but does not support the claim that such harms are occurring.[3] In fact, expanded access to data used for identity verification and fraud prevention could prove detrimental. Allowing consumer rights to access and correct data files designed to prevent fraudulent behavior could significantly reduce the efficacy of these data files because such measures also make it easier for fraudsters to gain access to files. Such a reduction would have a substantial affect on the effectiveness of the Commission's own Identity Theft Red Flag Guidelines, as will as on the Obama Administration's National Strategy for Trusted Identities in Cyberspace. In addition, data files used for consumer authentication may purposely contain information that is not necessarily correct in the eyes of the consumer. Such data might be names or other information from those who have attempted or perpetrated an identity evasion, which is maintained because it is necessary to prevent future attempts. These information tools have helped reduce the incidence of financial identity theft, once the fastest-growing white collar crime in America. Undermining the value of these tools will increase business risk, which could ultimately impede consumer access to credit and other benefits.

While the risks of providing increased consumer access to data used for authentication are quite high, the corresponding benefits are low. The only result from failing an authentication test is that the consumer is asked to provide additional information or documentation. Given these costs and benefits, Experian believes that the Staff Report's proposal to allow consumers access and correction rights with respect to the actual data used for authentication is both unfounded and unwise.

Finally, in the area of marketing data specifically, the nature of this information makes it irrelevant and unnecessary to impose any new requirements for accuracy, access and correction. Providing enhanced standards for accuracy, access and correction would not only be expensive to implement but also would raise additional privacy and data security concerns.

As discussed in Experian's Privacy Roundtable Comments, filed with the Commission on January 22, 2010, marketing data are largely benign. Marketing databases are not designed for individual "look-up." Accordingly, marketing databases are typically compiled at the geographic or household level, rather than at the personal level, and marketing data are estimated or presented in ranges. Compiled databases also contain inferred information obtained from

[3] Staff Report at 74.

models or demographic overlays of Census information. While marketing databases maintain information about individuals, marketers typically seek to understand the general characteristics and broad trends of the individuals or households to which they are marketing.

Moreover, marketing information is not used to assess eligibility for credit, insurance, employment or any other substantive decision covered by the Fair Credit Reporting Act. If information is inaccurate in a marketing database, there is no harm to the consumer aside from receiving a potentially irrelevant advertisement. To address this issue, Experian provides consumers, upon request, with an explanation of the categories of consumer data we possess and provides a suppression right that allows consumers to request that their name not be used by Experian for marketing purposes. Experian supports this type of notice and opt-out mechanism for marketing data, and encourages the Commission staff, in its final report, to continue to recognize that this mechanism is sufficient.[4]

Expanded access would raise significant privacy, data security, and cost considerations because sensitive identifying information would actually need to be added to marketing databases in order to ensure proper authentication of a consumer's request for access. As noted, marketing databases often are maintained without reference to individual identification. Additionally, providing access would also require the integration of multiple, separate consumer databases, which would raise additional privacy and data security concerns. Allowing access unquestionably would make the data less secure and would increase the risk of potentially harmful data breaches or other unauthorized access.

Some commercial entities are experimenting with various regimes that would allow consumers to view and change certain marketing profiles that are used to target advertisements on the Internet. Experian applauds such efforts, and is carefully monitoring their success. We believe that access and correction relating to marketing data will be driven as consumer demand and technology intersect. At this time, there is little evidence that consumers are interested in access to marketing data, beyond being able to opt out.

VI. Incentives to Anonymize or De-Identify Data Should Be Encouraged

Experian submits that the Commission should support efforts to anonymize and de-identify data, and therefore should avoid recommending guidelines that would create disincentives to these efforts. We have seen that as technology advances and consumers express their expectations about data privacy and security, companies are increasingly beginning to use de-identified and anonymized data whenever possible. Processes used under HIPAA, FCRA, and by the U.S. Census Bureau are good examples of such advancements in technology. Accordingly, expanding the scope of privacy restrictions to apply to non-personally identifiable data, as suggested in the Staff Report, would reduce existing incentives to use anonymized and de-identified data, thus reducing the demand for such technology.

In addition, industry self-regulation already allows consumers to opt out of using anonymized data to track them for online behavioral advertising purposes. Anonymized data

[4] *Id.* (indicating that a "sliding scale" approach might include this type of access and correction regime for marketing data).

used for purposes other than behavioral advertising is not personally identifiable, nor can it generally be re-identified, and thus it should not be subject to consumer privacy limitations, with the exception of information security policies.

Specifically, we are greatly concerned with the notion expressed in the Staff Report that IP addresses should categorically be considered personally identifiable. In reality, unless they are combined with personally-identifiable information, an IP address reveals no personally-identifiable information. While it is true that Internet users connected through a DSL connection may have a static IP address that does not change, the rise of cable modems and cell phone connections, which use dynamic IP addresses that may change multiple times in one day or not at all for several weeks, have made it difficult to tie an IP address to a single location. Moreover, while an Internet Service Provider has the ability to link static IP addresses to a household (but not to an individual user where computers are shared), most entities do not have this ability unless the consumer has specifically offered information to make this link. Indeed, IP addresses and even static IP addresses change so frequently that they cannot be reliably linked to personally-identifiable information ("PII") unless the consumer has specifically offered information to make this link. Importantly, most Internet marketing models do not and need not make this link between IP addresses and personally identifiable information.

It is critical, therefore, that the Commission's final report recognizes that IP addresses are not inherently personally identifiable. To find otherwise could seriously disrupt the manner in which the Internet has be configured and how it operates. For example, one way that companies fight spam is by linking spam emails to the IP address from which they were sent. If restrictions are put in place that limit what companies can do with IP addresses, companies would not be able to analyze their data in order to look for patterns used by spammers. In addition, millions of web servers, by default, log IP address on any user page visit but do not log PII. If IP addresses are re-defined as PII, data security and retention policies around this data would require substantial revision for no real consumer benefit.

We agree that businesses should fully understand the sensitivity of all data they collect, use, and transfer, regardless of whether or not the data is personally identifiable. Such an approach is useful to companies in identifying potential privacy issues, like data security and storage. However, such a process should not be established through legislation, regulation or even self-regulation. Requiring choice, access, and other principles to apply to non-personally-identifiable data does not meet any public policy purpose and, as discussed above, could have the perverse effects of discouraging the use of de-identified or anonymous data and inhibiting technological innovation.

* * *

Again, Experian thanks you for the opportunity to engage in a dialogue with the Commission on these important matters. Should you have any questions, please do not hesitate to contact Tony Hadley, Experian's representative in Washington, DC.