February 18, 2011

SUBMITTED ELECTRONICALLY

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

Dear Secretary Clark:

The National Business Coalition on E-Commerce and Privacy (the "Coalition")very much appreciates the Federal Trade Commission ("FTC")'s inquiry into the appropriate national consumer privacy framework, as well as the opportunity to submit our comments on the Preliminary Staff Report, entitled "Protecting Consumer Privacy in an Era of Rapid Change" (the "Draft Report"). The Coalition represents sixteen name-brand corporations engaged in both the offline and online collection, disclosure and use of personal information. The Coalition's membership is diverse, ranging from major financial institutions to equally well-known retailers. Most of our members are global enterprises, with multiple and varied compliance obligations throughout the world. All have the same goal: to contribute meaningfully to the public policy debate in such a way as to help assure that policymakers undertake changes in law and regulation that are both commercially and economically prudent and workable, as well as beneficial to consumers generally and our customers in particular.

We understand that the FTC plans to digest the comments that we and others submit before eventually releasing a final report. The Coalition welcomes the opportunity to contribute to this process, and we hope that the Commission will find our comments useful. As our letter will demonstrate, we have some significant concerns with the assumptions underlying the Draft Report, as well as some of its conclusions, and we hope our comments, combined with those of others similarly concerned, will contribute to the Commission's deliberations and the form and substance of the final report.

At the outset, we believe that the system of information sharing that has developed in the United States to date both protects and benefits consumers and is a critical component in the success and innovation of our economy. We also are, of course, mindful that privacy expectations of American consumers are evolving but we believe these can be accommodated within the existing system. Information exchanges

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

among affiliated organizations, third parties and consumers fuel new product development, innovation and productivity. We need only to look to the way in which the Internet has developed in the United States, compared to other nations, or to the innovation in the financial services industry to see this at work.

This innovation comes, in part, from the flexible and adaptive regulatory system that has developed in the U.S., a system which stresses the enforcement of multiple sectoral laws and ensuing regulations, robust and evolving self-regulation, and enforcement by multiple agencies and at multiple government levels against unfair and deceptive commercial practices.

This flexible system inherently fosters a practical approach that recognizes that consumer privacy is but one lens through which to view the larger issue of information sharing and data protection. The other and equally important lenses include how consumers benefit from and are protected by information sharing, how businesses use information in a responsible manner to innovate and increase productivity, and how the economy in general benefits and can compete in a global marketplace. The views through each of these lenses must be balanced when considering a new framework, or even individual practices and policies.

Therefore, we urge FTC to defend the existing system of information sharing domestically and promote the system internationally as a legitimate and adequate regime for ensuring consumer privacy. While the Coalition has not seen any evidence yet that new laws on the subject are necessary, we are very much interested in a better understanding of precisely where self-regulatory standards and guidelines can be enhanced to ensure the proper balance of consumer privacy and economic innovation.

The FTC's final report should be much clearer in indentifying specific areas in which self-regulation can be improved, with recommendations that include consideration of consumer privacy, consumer protection, the need to encourage business innovation, and our national ability to compete effectively in a global marketplace full of different enforcement regimes. The Draft Report appears too much like a "laundry list" of *perceived* concerns, with little or no record of harm that might form the basis for the proposed guidelines. In addition, the Report does not appear to make any attempt to balance the costs or benefits that would be inevitably inherent in their adoption or application.

I.) Additional Legislation/Regulation is Not Needed to Protect Consumers

First, we commend the Commission's continued recognition that self-regulation is the most effective way to protect consumers in this rapidly evolving digital economy. In a dynamic marketplace, such as today's "information economy", the ability of

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

businesses to quickly adapt to new trends and technologies through self-regulation has proven over time to provide the most appropriate protection for consumers. Effective self-regulation will and should always be an essential component of offline and online consumer privacy protection, as laws and regulations are often too rigid and can quickly become obsolete.

The current multi-tiered enforcement environment, composed of a combination of sectoral law, federal and state regulations, FTC enforcement and industry self-regulation, provides an ample menu of enforcement tools to be arrayed against "bad actors" and companies that fail in their responsibility to protect consumer privacy.

To our Coalition members, protecting the privacy of their customers is a foremost priority and, to advance that policy, our members have put robust consumer privacy protections in place. "Privacy by design," as proposed in the Draft Report, is consistent with both the practices and the philosophies that our members have embraced in order to respond more effectively to the expressed needs of their customers. We welcome the opportunity to work with the FTC to further develop this concept.

Any FTC privacy framework, even if characterized as "self-regulatory," should not be structured so that it risks preventing the development of innovative privacy protections that are integral to economic growth and customer satisfaction. A framework that inevitably increases consumer costs, such as that which is proposed in the Draft Report, is the cause of great concern by businesses and consumers alike, especially in this stressed economic environment. The Draft Report presents no support whatsoever that consumers are willing to pay higher prices, as has been suggested, for goods and services in order to avoid targeted marketing.

II.) A Harms-Based Approach Must Be a Critical Part of Any Sensible Privacy Policy Including the Proposed Self-Regulatory Framework

There is a recognition that the privacy framework within the United States needs continued and evolving development. One such area of key development is the concept of a consequence, or a harms-based policy standard, especially in the context of new and evolving privacy issues in the increasingly important world of electronic data and commerce. Under a harms-based approach, the costs and benefits of data use and misuse need to be the foremost factors in deciding when and how to address issues regarding the use of personal information about consumers. This principle has relevance whether the approach is legislative, regulatory, self-regulatory, or even the product of free market activity. It focuses the debate and our efforts on what information matters most to consumers and which rules are appropriately tailored or too strict to be justified. It also critically focuses the debate on the overall effects of

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

privacy policy on consumer benefits—net effects, but also outliers or extreme and unusual examples.

Targeted marketing reflects the refined evolution of advertising focused on the expressed interests and needs of consumers, and if there were no such marketing, consumers would be buffeted by a range of imprecise advertisements without relevance to their expressed need. The Draft Report does not define any "harm" associated with targeted marketing, nor does it identify shortcomings in the current blend of legal and regulatory obligations that, when combined with self-regulation, might justify a stricter framework. It is our view that targeted marketing is essential to continued economic growth and to suggest, as the Draft Report does, that it is somehow "harmful" to consumers is to take the view that consumers are incapable of making unilateral purchasing decisions and that government must provide protection from accurate and relevant marketing.

This harms-based approach is by no means antithetical to the concept of Fair Information Practice Principles (FIPPs), which we believe should serve a legitimate role as a foundation, not to be applied in a rote manner, but rather to serve as guidance for self-regulatory practices. In sum, a harms-based approach is the necessary approach required in an already diverse regulatory and statutory compliance landscape, including the FTC, that incorporates robust self-regulatory codes of conduct to ensure that businesses meet the reasonable expectations and protect the legitimate interests of consumers.

A. Privacy Policy Should Focus on Concrete and Objective Harms

A sensible application of a harms-based standard should recognize that "consequences" can be positioned on a sliding scale of importance. Not all consequences matter equally. Starting with the simple idea that the consequences of data use (or misuse) should be ranked in some simple order of importance, one can begin to establish what types of data use are worthy of the most rigorous policy focus. Traditionally, there are three relatively well-recognized sets of privacy interests that have been identified and addressed through policies and law, and they can be ranked in decreasing order of importance. The foremost is financial data. Its unauthorized release to the public clearly jeopardizes the privacy interests of consumers and puts them at risk of demonstrable economic harm. Consequently, financial data is subject to a successful regulatory framework that protects consumers' interests.

Reputational harm is also a well-recognized privacy interest, though this concept is often indirectly tied to economic harm. Unauthorized disclosure of private, personal information that affects a person's livelihood, relationships, or community standing can be classified as an objective harm. Finally, unwanted intrusions can also

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

be classified as concrete harm—that is, unwanted intrusions into a consumer's life, at the very least, wastes his or her time. Notably, each of these types of consequences is objective, measurable, and concrete, and each has an established basis in common law.

Much of the current debate over privacy regulation, however, has become divorced from these simple concepts of concrete and objective harm. Rather than focusing on harm, many advocates of increased privacy regulation complain that companies are taking different data sets, joining them together, and making sophisticated predictions about future consumer behavior. This misdirected focus fails to recognize that consumers are also voluntarily sharing information about themselves at an increasing rate, as demonstrated by the rapid and continuous expansion of online commerce (which requires some consumer identification) and the exponential increase in the use of social networking. It is not at all clear that there is any groundswell of concern about privacy interests generated by consumers themselves.

In contrast to the harm that would follow if someone with a malicious intent obtained information about a particular consumer's location, a targeted promotion sent to a consenting Starbucks coffee drinker when near one of their locations would offer benefits to that consumer and not harm him or her in any way. In short, a belief that the collection and use of consumer information for targeted marketing purposes, with appropriate notice and choice, is somehow injurious is unsubstantiated and presents a weak basis for further domestic or global restrictions on commercial data use.

B. A harms-based policy focus allows application of cost-benefit analysis

The importance of focusing upon concrete, objective and ultimately quantifiable harm cannot be overstated. Data misuse, of course, has costs—even potentially subjective costs regarding how some consumers may feel about the use of personal information that pertains to them. But restrictions on the use of personal data, especially data that are created through two-sided commercial transactions, have very real and objective direct and indirect costs. Simply put, there is no question that putting any restrictions upon the collection, use, and dissemination of commercial information will increase the cost of doing business and providing goods and services. It will also reduce innovation, and ultimately force the abandonment of otherwise acceptable business practices, at considerable cost to consumers.

A harms-based approach forces policymakers to grapple with both the short- and long-term trade-offs of restricting data use. It protects the benefits of data use by examining the overall effects. As reflected in recent reports issued by the FTC and the Department of Commerce, data use, essentially for advertising and marketing purposes, increases the value of goods and services to consumers. Through effective advertising, businesses pay for new or additional services, attract and provide value to consumers

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

(e.g., the use of discount coupons), or give consumers information that has real value to them. We now live in a society fueled by the availability of information and a primary incentive for creating and disseminating information is the value that can be created through advertising. Take the "information" out of the "information economy" and the economic consequences will be dire.

A harms-based approach is equally applicable to the online and offline worlds—if that distinction even remains important in the long term. Moreover, the online world is also an environment ideally suited to collecting electronic data. Whether done explicitly, for example through a notice and choice system, particular transactions, or behind-the-scenes through tracking cookies or other technology, an online presence creates information. It was inevitable, however, that the online world would become tied, at least for informational purposes, with the so-called offline environment. Trends are already developing in which point-of-sale information in physical locations is being tied to online accounts. This linking of data from different sales channels is beneficial to consumers, for example, who may wish to return or exchange goods purchased online to a local retail store rather than making such returns or exchanges via a longer and more cumbersome courier process. In addition, mobile telephones and even televisions have become interactive, and direct mail and telemarketing efforts can and are being improved (and targeted) using information collected through multiple channels.

If data are not available to be used to refine the offers provided to consumers, they will be overrun with irrelevant information, which wastes their time and excludes them from offers that may actually be of greater interest to them. The resulting mass, unsolicited marketing in the digital world has been decried as "spam" (in e-mail form) and the subject of numerous laws and regulatory enforcement actions. Individualized advertising therefore has a recognizable benefit to consumers and advertisers. Without it, consumers will face greater mass-marketing and the cost of doing business will surely rise, resulting in added costs or decreased value to consumers. In the absence of a thorough economic analysis on the part of the FTC that realistically balances the perceived harms and relative benefits of targeted advertising, over-regulation presents real, concrete risks and will impose distinct economic costs on consumers.

C. Current law reflects a pragmatic harms-based approach

While a harms-based approach may be relatively new as an expressed principle, it is actually well reflected in the current U.S. privacy framework. Unlike the European Union, which has a broad-based privacy approach, the United States has a set of discrete laws that address specific types of privacy issues. That is not a weakness; it is a strength of our system. Our relatively narrow privacy statutes address financial harms, highly sensitive personal data (e.g., health), discrete classes of "vulnerable"

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

consumers (e.g., children), or particular types of intrusions.

Indeed, even the broadest applicable "privacy" statute, Section 5 of the FTC Act, has been used sparingly and through careful case development. No FTC actions have attacked behavioral advertising simply because it is behavioral advertising. Further, the United States has rightly resisted the temptation to enact a one-size-fits-all privacy law. Thus, our legal system reflects the reality that law makers and regulators have cautiously restricted data use when concrete consumer harms have been identified, studied, and understood.

Our laws are perhaps not perfectly aligned with "quantifiable" harms, but the existing statutes were passed to address objective and identifiable problems – an important political dimension to privacy regulation. This focus on consumer harms on an issue–by–issue basis has allowed political consensus to form for each issue, enabling not only the passage of our discrete privacy laws but also their continued and effective enforcement. Notably, such consensus also fosters an effective self-regulatory environment.

Likewise, common law, for similar reasons, has resisted creating privacy rights not directly related to economic or physical harm. The common law traditionally has been our key means of developing legal rules that balance individual costs against society-wide benefits. This dynamic demonstrates the long-term recognition of the limitations and the dangers of not grounding privacy policy on consumer harms.

D. The Push to Legislate Broadly Based Upon a Subjective and Amorphous Standard is Dangerous

The application of a harms-based approach cautions against sweeping legislation without further study and analysis. Given how much of the current debate is being driven by subjective perceptions (or arguments about consumer perceptions) regarding the use of consumer information, we need to keep in mind that subjective valuation of privacy for the sake of privacy is a very limited measurement. It simply is hard to measure and use without a realistic cost-benefit analysis.

Perceptions can and do change, and what is unexpected or surprising to consumers today may be considered perfectly normal or obvious in the future. Not long ago, companies like Amazon.com began experimenting with providing product "recommendations" based upon consumers' past purchases. Before it was presented to consumers, this marketing concept was initially misunderstood and labeled by consumer advocates as "profiling". Now this use of purchase history and known product interests is universally recognized to be what it is: a valuable information service to help consumers learn about potentially desirable products and to lower their

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

search costs. Whether the service is provided by Pandora, Netflix, or Apple's iTunes, consumers are willing to share their purchasing and interest information because the beneficial result is a more valuable service. This is an instructive example of how perceptions of privacy change over time, as what was once a misunderstood marketing concept that, *in theory*, raised consumer privacy concerns is now a successful commercial service demanded by consumers.

A similar debate is again taking place in the context of new, growing, and rapidly changing practices and technology. The law of unintended consequences suggests that overbroad regulation, divorced from very specific and agreed upon findings of harm, will have detrimental effects on the economy and, thus, consumers as well. In contrast, a harms-based approach focusing on the majority view, while not outright rejecting esoteric preferences, would not allow policy decisions to impose direct and indirect costs on the vast majority of consumers without a demonstration of overwhelmingly convincing impacts.

E. The Draft Report Fails to Address Whether Broadly Regulating Simple Information Tracking Can be Justified Under a Harms-Based Approach

The Draft Report's treatment of the harms-based approach is merely descriptive of the concept, without offering any substantive analysis. In contrast, the Draft Report's concept of harm is skewed heavily towards the idea of "intrusive harm" (e.g., telemarketing). However, all advertising is by its nature "intrusive"—if noticed. But effective advertising is the type of intrusion consumers can, should, and do welcome when appropriate. Coupons, information about special deals, and information about new goods and services are all consumer benefits of advertising. Notably, when not done in a consumer-friendly manner, for example the discredited "cover-the-page pop up ad," the effect may be counterproductive for the advertiser.

Thus, targeted (and even non-targeted advertising) is a very weak form of intrusion and is counter-balanced by concrete financial benefits. Again, the debate over the appropriate privacy framework would be better served by making a direct cost-benefit analysis, albeit on a broad basis, of any suggested proposals. Otherwise, the FTC should continue to study which practices are best for consumers and follow its analysis and findings with ongoing consumer education.

III.) Definition of Sensitive Information and Sensitive Users

Rather than focusing on whether particular data meets a static definition of sensitive information, self-regulation of all data should turn on whether the information, if in the public domain, could be used to cause harm, as determined on a case–by–case basis. This premise is likewise applicable to the Draft Report's statement that the

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

distinction between personally identifiable information (PII) and non-PII is vanishing. Rather than focusing on the types of data in question and the identification of individual consumers, industry obligations should turn on whether the data could cause harm when they are associated with a particular consumer.

Websites invariably collect IP addresses for purposes of not only advertising and direct marketing but also to authenticate users, prevent fraud, identify general geographic areas of visitors, log website usage, etc.–all of which allow for the safe, accurate and seamless functioning of the Internet. It is unreasonable to mandate that consumers may opt out of the collection and use of IP addresses and still expect to continue to use Internet-based applications and enjoy free website content and services without an associated revenue stream resulting from these commercial products. Restricting collection and use of IP addresses for authentication and fraud prevention will have the perverse effect of increasing identity theft and other consumer harm rather than reducing it.

With respect to sensitive users and sensitive uses of information, again the framework should focus not on the type of information or the particular class of individuals but on harm. Information related to sensitive users is generally covered by existing statutory frameworks applicable to specific groups (e.g., information on children is covered by the Children's Online Privacy Protection Act (COPPA), financial information is covered by the Gramm-Leach Bliley Act (GLB) and Fair Credit Reporting Act (FCRA), health information is covered by the Health Insurance Portability and Accountability Act (HIPAA), and wireless location data is covered by the Communications Act).

IV.) Inconsistency with Existing Law

At the outset, the Coalition agrees that the scope of the privacy framework proposed in the Draft Report should cover information collected in all media. However, we presume that the framework is not intended to cover data lawfully collected under existing legal regimes, whether FCRA, HIPAA or GLB, among others. Our comments therefore are confined largely to information collected and used for marketing purposes. Nonetheless, we raise concerns later in these comments regarding the Draft Report's recommendations relating to access and correction of data files used for consumer authentication.

Existing law should not fall victim to conflicting principles in an informal self-regulatory framework. No new self-regulatory framework should conflict with existing statutory obligations. Many companies, including our members, already have unilaterally implemented internal practices that exceed existing statutory requirements,

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

but it is inappropriate for the FTC to attempt to achieve by indirection, via imposing expanded self-regulatory obligations, that which has not yet been enacted into law.

A self-regulatory framework should carve out both activities and entities subject to existing law or contractual terms requiring compliance. Service providers offering outsourced services such as payments processing to financial services companies, although not explicitly subject to GLB as regulated entities, are bound by the terms of their outsourcing agreements to comply with the statute. Focus should be on *activities* subject to existing law rather than simply *entities* in order to avoid imposing conflicting privacy rules upon entities that operate within an existing privacy regime due to contractual obligations. Such conflicts would have a substantial economic impact on both these entities and the regulated entities that pay them to process information.

V.) Do Not Track (DNT)

A DNT paradigm, as envisioned by the Draft Report, would have significant economic consequences on both businesses and consumers. Targeted advertising underwrites the free use of the Internet, and any unreasonable adjustments or limitations of its use will likely have a distinct and immediate adverse economic effect on not only free content, but also on innovation and employment opportunities in the online industry. Consistent with our comments above, in advance of the placement of any limitations on the use of such advertising, the Commission should prepare a detailed economic analysis of the likely after-effects of the introduction of DNT into the economic mix that currently sustains the Internet's growth.[1] No changes in current practice should be proposed in the absence of such an analysis, and such an analysis is absent from the Draft Report.

There is also little evidence that DNT would address any actual economic harm, and thus far there has been no demonstrable broad consumer rejection of online advertising, including targeted advertising and other promotions.

Moreover, DNT is not analogous to the Do Not Call (DNC) registry. The purpose of DNC was to allow consumers to avoid irrelevant and unwanted telephone advertising that interrupted their planned activities. In contrast, DNT would have just the opposite effect, as it would facilitate the receipt by consumers of irrelevant and untargeted advertising.

[1] According to "The State of Retailing Online 2010," a Shop.org survey of 109 online retailers conducted by Forrester Research, web sales increased by 29% in 2009 over 2008. In response to a question regarding the three most effective sources used to acquire customers in 2009, the survey also revealed that 90% of the respondents pointed to search engine marketing, which is inherently tied to targeted advertising.

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

Further, there are significant operational and technological differences between "do not collect" and "do not use" – current law does not significantly restrict the collection of data (except COPPA, which is limited to children), but rather only the use and further disclosure of that information. DNT would create a new barrier to the collection of information on the Internet, with corresponding down-stream economic ramifications for consumers as described above.

VI.) Choice/Consent

The timing and methods of delivering notice and obtaining consent from consumers must be flexible and appropriately tailored to the medium, type of data and intended use. Notice and choice is a system that has worked well and has encouraged market-based solutions and industry "best practices" in response to demonstrated consumer needs and expectations. The proposed FTC framework should not attempt to standardize when notice should be delivered, the content of notices, methods of obtaining consent or the terms of organizations' privacy policies. We believe that robust notice that is "clear and conspicuous" is key to the ability of consumers to exercise informed choice. There is no justification for affirmative consent or complex privacy notice requirements, which would be both costly and counterproductive.[2]

The Coalition supports clear and concise privacy policies. However, there should be flexibility regarding omissions in privacy statements. It is precisely this concern about being incomplete that fuels the long and legalistic statements in privacy policies that the Draft Report faults. Further, companies should be free to change their policies on the use of collected data so long as a company's privacy policy is updated to reflect the change in use, consumers are properly notified of the change, and the company provides the consumer with the opportunity to opt-out prior to using the data in the materially different manner. Thus if a company changes its previous policy of not sharing costumer data with third parties, to one of sharing with third parties, this would constitute a material change necessitating notice and choice.

Companies should—and our members do—provide meaningful notice and choices about their data practices and acquire consent from consumers where appropriate. Most of our members already have robust notice and choice regimes in place, and many of these regimes have been driven both by the marketplace and the current U.S. regulatory framework applicable to various types of data and data transfers

[2] As noted previously, for categories of information – such as financial information, medical information and information about children – where disclosure or third party use poses a signification risk of harm, strong sectoral laws have been enacted, such as HIPAA, COPPA and GLB, to regulate the collection, use and sharing of such categories of information.

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

(*e.g.*, the U.S.-European Union Safe Harbor framework, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and the CAN SPAM Act). We believe that requiring more detailed and elaborate privacy notices electronically or on paper – particularly by those companies that have long been subject to existing federal legal requirements – is unnecessary and would only serve to further confuse consumers.[3]

Further, as long as there is a robust, clear and conspicuous notice posted on a web site and available to a consumer, the consumer's consent to the merchant's privacy practices should be inferred from the consumer's conducting business via that website. Notice and choice is a system that has worked well and has encouraged market-based solutions and industry "best practices" in response to demonstrated consumer needs and expectations. We believe that robust notice that is "clear and conspicuous" is key to the ability of consumers to exercise informed choice. There is no justification for an affirmative consent or complex privacy notice requirement, which would be both costly and counterproductive.[4]

As with the provision of notice, choice should not interfere with the customer experience or the provision of service. As with a flexible notice paradigm able to accommodate different mediums, choice does not always need to be offered or exercised at the moment of information collection. As long as there is a robust, clear and conspicuous notice on a website – and a consumer continues to browse the website or revisits the website – then he or she is by definition acting in an informed manner.

This notice and choice framework ensures that consumers' privacy interests are protected while at the same time enabling continued investment by businesses into innovative new uses of consumer data that may ultimately benefit all consumers.

Finally, the Draft Report defines data brokers in overly broad terms. Third parties and other downstream, non-consumer facing entities are not by default, data brokers. With respect to notice and choice for downstream parties use of consumer information, the first party with the initial relationship with the consumer must provide the notice and choice. It is unnecessary and impractical for downstream parties to return to the consumer for additional notice and choice. However, the downstream

[3] It may be more productive to avoid duplicative or excessive layers of regulation on businesses that are already subject to a rigorous regulatory regime, and focus any legislative efforts on those entities that are not subject, whether directly or contractually, to such strict laws or regulatory requirements as well as on government agencies that repeatedly receive failing grades on their computer security.

[4] For categories of information – such as financial information, medical information and information about children – where disclosure or third party use poses a signification risk of harm, strong sectoral laws have been enacted, such as HIPAA, COPPA and GLBA, to regulate the collection, use and sharing of such categories of information, and those sectors have worked effectively for years using an opt out approach.

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

party must honor the consumer's choice and it is the responsibility of whichever party holds the data to preserve the consumer's decision for a subsequent holder of the data. Additionally, the first party should not be held liable for what a downstream party does with the data as it would be virtually impossible for that first party to know either the identity of successive downstream parties or the downstream parties use of the data.

VII.) Specific Business Purpose or Need and Commonly Accepted Business Practices

Business needs and practices differ widely from company to company and industry to industry, so any self-regulatory framework must not be overly prescriptive so as to limit business processes or innovation over time. Business practices generally do not lend themselves to a "one-size-fits-all" definition. So long as the "business need" can be reasonably linked to a legitimate internal business purpose, it should not be subject to choice.

Further, what may be a "commonly accepted" practice in one business context may not be in another. For example, it is commonly accepted to have strong authentication requirements for a banking website, but you would not expect the same degree of rigor for data collected when a consumer accesses a subscription news site. Likewise, it would be a common expectation that your registration data would be shared with other companies on a site where you could download free content such as ring tones, backgrounds, etc., but not on your brokerage company's website.

Instead of defining commonly accepted practices where a company does not need to provide choice, the FTC should simply identify those practices with a potential risk of consumer harm that do require notice and/or choice. Commonly accepted, as used by the FTC, implies that a particular approach to privacy has achieved a certain level of adoption. However, a self-regulatory framework should not disadvantage companies developing new approaches to protecting consumer privacy, which may not yet be commonly accepted, by requiring consent.

Websites offering free content and services invariably collect IP addresses. They also offer advertising and engage in direct marketing, which, in some cases, is the only way they can generate revenue. It is simply not feasible, however, to notify consumers before a server automatically collects an IP address when a computer visits a website. Nor is it reasonable for consumers to opt out of these uses and still expect to continue to use such free websites, free content and free services. Therefore, where appropriate, the collection of IP addresses should be treated as a legitimate business need not requiring consent.

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

VIII.) Third-Party Data/Non-Consumer Facing Service Providers

The Draft Report fails to recognize the value of third-party data. The collection and sharing of third-party consumer data provides numerous significant benefits to consumers. For instance, the use of third-party data lowers prices, enhances competition by providing small entities access to consumer data that larger companies already maintain, creates consumer convenience, facilitates access to consumer and business credit, and reduces fraud.

Third-party data also facilitate the relevancy of first-party marketing efforts, especially for small businesses and start-ups, which rely heavily on marketing to prospective customers. Even large first-party marketers with extensive customer databases rely on third-party data to provide better services and relevant marketing offers to existing customers. The practice of "data enhancement" – companies obtaining data about their customers from third-party sources to enrich their databases – should not necessitate or trigger an independent choice for the consumer.

Marketers cannot rely solely on their own transactional and experiential data to effectively make offers that are tailored to specific individual or household preferences. For example, a company's transaction information probably cannot help a company understand even the most basic segmentation factors for effective marketing, such as gender, estimated age, estimated income, type of dwelling and the like. Imagine how wasteful and ineffective to the company, and annoying to recipients, a marketing campaign would be if advertisements for lawn mowers are sent to those who live in apartments and condominiums.

Routine management of customer databases to ensure accuracy requires organizations to undertake "data hygiene" processes to ensure that addresses are up-to-date, given that some 40 million Americans move each year. Third-party data are essential to this process. In addition to increasing the relevancy of advertising, whether online or offline, third-party data helps marketers (1) identify new 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.); and (6) reduce irrelevant marketing communications.

As a national framework for privacy evolves, it is essential that it acknowledges the importance of third-party data and carefully balance restrictions on the collection and sharing of third-party information with the significant benefits it provides to consumers. The Coalition is concerned that the proposed framework does not consider this balance in its approach to third-party data.

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

Further, as the staff notes in the Draft Report, service providers should not be restricted from providing services to financial services companies as permitted under GLB and any other applicable statute. The Draft Report's attempt to make a distinction between affiliates that are linked to the first-party's brand and those that are not is an unjustified interruption in accepted and lawful business practices, and any alteration of that practice should be subject to evidentiary justifications that are presently absent from the Draft Report.

Financial services companies are permitted to share information with service providers under GLB. The FTC's proposed framework should not require a financial services company to return to a consumer for multiple rounds of notice and choice in order to disclose information to its own subcontractor. "Service providers" is a very broad category, and interrupting their activities with unnecessary obligations would likely have adverse consumer and economic impacts. Use and disclosure of information by service providers can be adequately controlled through contracts, as is done under GLB (and even under the restrictive EU rules).

IX.) Privacy by Design

The Draft Report offers few details about the concept of "Privacy by Design," but based upon what we can glean from the text, we would support continuing evolution of this concept and are prepared to be part of the ongoing dialogue. Coalition members already incorporate privacy protections into virtually every relevant stage of their product and service development, including when possible, starting during the initial stages of development. The Coalition agrees with the Draft Report's recommendations that companies that handle large amounts of data should continuously advance employees' understanding of privacy issues, conduct regular evaluations of privacy, privacy protections, and data management, and immerse personnel responsible for privacy in relevant stages of product planning and development.

Nonetheless, attempting to require a "privacy by design" regime in a legislative or even a self-regulatory context to apply across the board to companies of all sizes and all business sectors would be elusive and could result in an overly restrictive framework that limits innovation. In particular, if "privacy by design" means imposing blanket procedural requirements (such as "privacy impact assessments" and record-keeping and reporting of the same) on a broad category of activities, it would result in unintended and not insignificant economic burdens.

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

X.) Market Driven Incentives to Anonymize or De-Identify Data Should Be Encouraged and Embraced

As potential consumer concerns about online tracking have been highlighted by policy makers, consumer advocates and the media, the private sector has responded by developing new ways to use de-identified data sets for delivering targeted advertisements. The Commission should support these efforts to anonymize and de-identify data and should avoid recommending guidelines that would create disincentives to further development of these practices. As technology advances, companies increase the use of de-identified and anonymized data. Processes used under HIPAA, FCRA, and by the Census Bureau are good examples of such advancements in technology. Accordingly, expanding the scope of privacy rights to apply to non-personally identifiable data, as suggested in the Draft Report, would reduce incentives to use anonymized and de-identified data, thus reducing the demand for such technology. Correspondingly, it would also confine consumers to practices that depend on the collection and use of more identifiable information.

The Coalition agrees that companies should fully understand any data they collect, use and transfer, regardless of whether or not the data are 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. Applying choice, security, access, and other principles to non-identifiable data does not meet any established public policy purpose tied to privacy and, as discussed above, could have the perverse effect of inhibiting technological innovation. Industry self-regulation already allows consumers to opt-out of the use of anonymized data to track them for online behavioral advertising purposes. Anonymous or anonymized data are not necessarily and easily re-identifiable. Therefore, this data should not be subject to privacy considerations such as choice and access.

Finally, if such data can be easily re-personalized or re-identified, then the obligations of the data custodian should increase proportionally. Security is the key obligation with respect to such data, and self-regulatory guidelines to protect data already include the endorsement of reasonable measures and processes to prevent re-identification.

XI.) Consumer Access and Correction to Data Files

The Coalition supports the Commission's proposal to increase the transparency of corporate data policies. However, we have deep reservations regarding any new legislative, regulatory, or self-regulatory requirement that would impose any mandatory accuracy or data access and correction standards on data files. Consumers already have

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

considerable ability to access and correct personal information under existing law, including the FCRA, the Fair Debt Collection Practices Act, the Fair Billing Act, HIPAA and the Wall Street Reform and Consumer Protection Act. The Coalition agrees with the Draft Report's recommendation suggesting a sliding scale approach for providing consumer access and correction to personal data. While certain data uses command a robust access and correction regime, other data uses, such as for marketing purposes or for consumer authentication, do not.

A "one-size–fits-all" approach to data access and correction could have the effect of undermining data security and consumer protection. The Draft Report has not identified—nor is there—a need for new requirements for accuracy and data access and correction. Further, the final report should not promote recommendations that are in opposition to existing law and which could have the effect of increasing privacy risks and diminishing consumer protection.

With regard to the Draft Report's inquiry about new accuracy, access and correction rights to information tools used for consumer authentication, we believe consumers are not harmed by the use of such services, nor is there any evidence that they are. Instead, these information tools have helped reduce the incidence of financial identity theft, once the fastest growing white collar crime in America. Typically, the only result from failing an authentication test is that the consumer is asked to provide additional information or documentation. However, the ability for consumers, including fraudsters, to access and correct data files designed to prevent fraudulent behavior could significantly reduce the efficacy of these data files. Such a reduction would have a substantial negative impact on the effectiveness of the Commission's own Identity Theft Red Flag Guidelines, as well as on the Obama Administration's national cybersecurity initiative.

Finally, the nature of marketing databases renders the need for new requirements of accuracy, access and correction irrelevant and unnecessary. Providing enhanced standards for accuracy, access and correction of marketing databases would not only be expensive to implement but also would raise additional privacy and data security concerns. Marketing data are largely benign and are not used to make substantive decisions about an individual consumer. More important, however, expanded access raises significant privacy and data security considerations because sensitive identifying information would need to be added to marketing databases in order to properly authenticate a consumer's access. Providing access would also require the integration of multiple, separate consumer databases, raising 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.

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361

Continuing the practice of providing robust notice, combined with a consumer's right to opt-out, is the most practical option for addressing the privacy concerns of consumers. This provides a sensible substitute for consumer access without imposing undue costs to businesses and unnecessary new risks to consumers that would result from adopting access requirements.

XII.) Retention

Retention periods should not be prescribed by law or by a self-regulatory framework but instead should be determined by a company on a case–by–case basis as a business decision. Companies retain data at a cost to the company because the retention has a business purpose, enables them to provide a consumer benefit, or is required by law. It is not the role of the FTC to determine how long data should be retained; it is sufficient that the Commission require that all custodial entities provide sufficient security for personal information.

Rather than regulating retention or duration, a self-regulatory framework should facilitate security of the data. On a related question included in the Draft Report, maintenance schedules for "legacy data systems" are best managed by entities on a case-by-case basis to ensure appropriate safeguarding and security of data.

XIII. Conclusion

The Coalition appreciates the opportunity to submit comments on the Draft Report. While the Coalition welcomes the opportunity to work with the FTC in order to continue to meet the privacy expectations of consumers, we believe it is first necessary to establish whether existing protections are inadequate and, if so, to what degree. We urge the FTC to refrain from establishing a rigid framework, even one that is self-regulatory, that is binding on companies and industries across the board without a comprehensive evaluation of the impact on companies in both online and offline contexts and the impact on our economy and the ongoing growth of Internet commerce and innovation. Further, until the need for a new U.S. privacy framework is conclusively established, the FTC can continue to protect consumers from companies that violate consumer privacy and fail to adopt adequate data retention and protection policies under its Section 5 authority.

Respectfully submitted,

Thomas M. Boyd
Counsel

Acxiom Corporation
Affinion Group
Assurant, Inc.
Bank of America
Charles Schwab & Co.
Deere & Company
Experian
Fidelity Investments
Fiserv
General Motors Corporation
Investment Company Institute
JPMorgan Chase & Co.
Principal Financial Group
The Vanguad Group
Visa Inc.

Kim Quish
Chair

500 8th Street, N.W.
Washington, DC 20004
202.799.4361
Fax: 202.799.5361