Statement of the U.S. Chamber of Commerce

ON: **H.R. 5777, THE "BEST PRACTICES ACT" AND H.R. ___, A DISCUSSION DRAFT TO REQUIRE NOTICE TO AND CONSENT OF AN INDIVIDUAL PRIOR TO THE COLLECTION AND DISCLOSURE OF CERTAIN PERSONAL INFORMATION RELATING TO THAT INDIVIDUAL**

TO: **UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON ENERGY AND COMMERCE, SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION**

BY: **JASON D. GOLDMAN**
COUNSEL, TELECOMMUNICATIONS & E-COMMERCE
U.S. CHAMBER OF COMMERCE

DATE: **JULY 22, 2010**

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96 percent of the Chamber's members are small businesses with 100 or fewer employees, 70 percent of which have 10 or fewer employees. Yet, virtually all of the nation's largest companies are also active members. We are particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large.

Besides representing a cross-section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business – manufacturing, retailing, services, construction, wholesaling, and finance – is represented. Also, the Chamber has substantial membership in all 50 states.

The Chamber's international reach is substantial as well. It believes that global interdependence provides an opportunity, not a threat. In addition to the U.S. Chamber of Commerce's 113 American Chambers of Commerce abroad, an increasing number of members are engaged in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on national issues are developed by a cross-section of Chamber members serving on committees, subcommittees, and task forces. More than 1,000 business people participate in this process.

Hearing on H.R. 5777, the "BEST PRACTICES Act" and H.R. ___, A Discussion Draft to Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to that Individual

Testimony of Jason D. Goldman
Counsel, Telecommunications & E-Commerce
U.S. Chamber of Commerce

July 22, 2010

Good afternoon, Chairman Rush, Ranking Member Whitfield, and other Members of the Subcommittee on Commerce, Trade, and Consumer Protection. I am Jason D. Goldman, Telecommunications & E-Commerce Counsel at the U.S. Chamber of Commerce, the world's largest business federation, representing the interests of more than three million businesses and organizations of every size, sector, and region. On behalf of the Chamber and its members, I thank you for the opportunity to testify here today on the "BEST PRACTICES Act" and on a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

Chamber's Position on Privacy

The Chamber supports policies that foster business opportunities while respecting consumers' privacy. The collection of personal information is necessary to provide consumer, social, and business benefits. Given the diversity of the private sector, business decision makers should have latitude, within acceptable guidelines, in defining their needs for personal information. Cost control and competitive pressure in the private sector provide a strong natural deterrent to the collection of unnecessary, erroneous, or irrelevant information.

Public policymakers and business leaders should weigh protection of privacy rights against a variety of factors, such as consumer convenience, the needs of management and the ultimate cost to the individual and public at large as well as to business and governmental entities. Before proposing governmental actions, policymakers should have a thorough understanding of the possible tradeoffs of these factors.

The Importance of the Internet to the U.S. Economy

The Internet has revolutionized the way business is conducted in all sectors of the global economy—including financial services, retail, wholesale-distribution, manufacturing, and many more. Today, the vast majority of companies of all shapes and sizes are online in some capacity and use the Internet to communicate with consumers, employees, existing customers, potential customers, and business partners around the world.

In particular, ad-supported content has been key to the success of broadband. With broadband accessible to the vast majority of Americans, the amazing array of content (including applications and services) available on the Internet has convinced more and more Americans to

go online using a broadband connection every year. Frequently, online content is provided free of charge to consumers, and revenues are instead generated through advertising. U.S. Internet advertising revenues totaled $5.9 billion for the first quarter of 2010, representing a 7.5 percent increase over the same period in 2009, according to the Interactive Advertising Bureau and PricewaterhouseCoopers. Some of the products that consumers receive for free are: Web mail, maps, news sites, blogs, social networks, video, job boards, and product rating and pricing services. Consumers recognize and appear willing, in many situations but not all, to permit information to be collected about them in exchange for goods and services that are of value to them. This ad-supported business model has been a key to the success of many Internet ventures and has helped to make the Internet an engine of growth in the U.S. economy.

Analysis

The Chamber received the text of the BEST PRACTICES Act earlier this week, so the comments below are based on our initial read of the bill and may change as we further analyze the language and vet the bill through our membership. The Chamber's analysis of the Boucher/Stearns discussion draft was submitted on June 2, 2010, to the House Subcommittee on Communications, Technology and the Internet, and is attached to this testimony (Appendix A).

BEST PRACTICES Act

The Chamber appreciates the work that went into drafting the BEST PRACTICES Act. Despite the inclusion of some provisions that we support, we have strong concerns with H.R. 5777 as currently written.

I. Definition of Covered Information

The definition of "covered information" in H.R. 5777 should be narrowed. Only data elements that could be used to commit identity theft or other direct consumer harm should be included in the definition. If the "unique identifier" is publicly available and does not contain any personal information then it should be excluded from the definition. For example, as drafted, the bill would impose the same protections on user IDs as it would for name and email addresses.

Therefore, "unique identifier," "persistent identifier," "Internet Protocol address," "telephone number," "fax number," and other such data elements should be removed from the definition except where such data has already been merged with other personal information elements.

The Chamber supports standardized definitions. Therefore, rather than creating a new category of "covered information," it would be better to model this definition after the "personal information" definitions found in many recent state data security and breach notification bills. Instead of including general categories of data elements which cannot identify a person, these definitions tend to tie a person's first and last name or first initial and last name with an address to a data element such as a social security number, drivers' license number, or financial account number.

The Chamber supports the exemption from the "covered information" definition for information collected about an employee, by an employer, prospective employer, or former employer that directly relates to that relationship.

II. Definition of Operational Purpose

Generally, the "operational purpose" exemption is too limited because it does not apply if the data is also used for marketing, advertising, or sales; dual-use of such data is a common industry practice. Under the bill, if a user chooses to opt-out, then the collection of non-identifying information (e.g., cookies or the user's IP address) is prohibited.

III. Definition of Sensitive Information

Instead of codifying precise geographical information as sensitive personal information, the Chamber recommends that the collection and use of this data be governed by self-regulatory regimes.

IV. First-Party Opt-Out Requirement

Consumer privacy expectations are different when dealing directly with a first-party then when there is a third-party relationship between the consumer and the business. For this reason, the U.S. regulatory framework has long recognized a broad first-party exemption to consumer consent requirements which has been supported by the Federal Trade Commission (FTC) as recently as in its staff report on online behavioral (OBA) advertising principles. The Chamber believes this legislation should maintain this first-party exemption.

U.S. businesses would be adversely impacted by a first-party opt-out mandate. It would require all media, retailers, service-oriented businesses, marketing companies, advertisers and others—in both online and offline environments—to offer an opt-out option to all consumers for any data that may be collected or used under any circumstances. Furthermore, the H.R. 5777 should allow for flexibility to account for the inherent differences between operating in the offline and online worlds.

Also, opting out of the collection of certain information could impact Web site operation and optimization. For example, when a consumer voluntarily visits a Web site, certain information must be collected by that company, including their IP address or referrer URL, in order to deliver the content on the site.

An opt-out consent standard would create a perverse incentive of requiring all media, retailers, service-oriented businesses, advertisers and others—in both online and offline environments—that do not already collect detailed consumer information to begin doing so in order to allow them to exercise opt-out choices over time. Such a requirement, for instance, could require retailers to offer all credit-card-using consumers opt-outs for the use of bar code scanners at checkout counters. In turn, these businesses would begin to develop and maintain detailed dossiers of personal transactions, in order to render all data from past transactions

unusable if at any point in the future the consumer wishes to exercise an opt-out with respect to the prior collection of data.

The Chamber does not believe that such a statute would further consumer trust; rather it may create greater privacy concerns while costing businesses millions of dollars to implement.

V. Express Affirmative Consent

Requiring opt-in "express affirmative consent" for the disclosure of "covered information" to unaffiliated third parties profoundly alters commonly accepted business practices. The definition of covered information is extremely broad as stated previously and includes several largely anonymous types of data, including cookies, IP addresses, and unique identifiers for computers or devices. These types of data points are inherently neither personal nor sensitive in nature and, thus, should not be subject to the strictest consumer consent requirements. Current regulatory requirements subject only the most sensitive data categories to an opt-in requirement, and many of those provisions recognize a lower standard when that data is used for marketing or advertising purposes.

VI. Access and Dispute Resolution

To avoid redundancy and confusion, there should be an exemption from the access and dispute resolution requirements when an entity or information (e.g., databases containing public record data) is already regulated by other laws (mainly consumer reporting agencies under Fair Credit Reporting Act and financial institutions under Gramm-Leach-Bliley). Additionally, databases that are used for fraud, authentication, and contract enforcement should be exempted, to the extent necessary, to prevent fraudsters from accessing and/or modifying these databases. Once all of these exemptions are included, however, mainly just advertising databases would be subject to this new access and correction regime. Therefore, we would encourage policymakers to carefully study this issue before proceeding because the cost of providing access and correction for those databases is very steep, while the benefit for consumers is minimal.

VII. Safe Harbor

The Chamber believes that the safe harbor provision, as drafted, is a good start but improvements could be made. We are gratified by the recognition that industry self regulation in this area has and can continue to protect consumers. However, the safe harbor is too narrow and should follow FTC and industry principles, including the exemption of first party data practices, greater flexibility in how consumer notice is delivered, and exemption from data accuracy and correction provisions (it appears to only exempt companies from the data access requirements). Moreover, the recognition that an opt-out standard for third-party data usage sufficiently protects consumers' privacy calls into question whether the opt-in standard for third-parties in Section 104 is proper. The FTC and industry agree that opt-out is the appropriate standard, so we would urge the Chairman to seek to codify that standard as the baseline in H.R. 5777.

VIII. Activities Covered by Other Federal Privacy Laws

The Chamber agrees with the intent of Section 502, which states that H.R. 5777 should have no effect on activities covered by other enumerated federal privacy laws, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and HIPAA. However, the opening clause of this section, which states "except as provided expressly in this Act," could be interpreted by the FTC or by courts to permit the creation of another layer of regulation in addition to provisions in each of the enumerated acts. Given the potential conflicts with having the same type of data collection and use covered by more than one federal privacy regime, a covered entity could very well find itself unable to comply with two separate federal privacy laws for the same covered information, thereby involuntarily subjecting itself to fines and other enforcement actions for non-compliance with one or both of the acts. To avoid this potential conflict with existing federal privacy regimes, the Chamber strongly recommends that this section be clarified to provide an explicit carve-out from the definition of covered entity for entities already covered by the enumerated acts.

IX. Private Right of Action

The Chamber also has serious concerns about the various liability-related provisions in H.R. 5777. For example, in addition to the robust enforcement mechanisms provided to the FTC, the legislation also contains a private right of action as well as an explicit grant of authority to state attorneys general to enforce the legislation. We are concerned that all of these mechanisms will serve to impose duplicative and potentially inconsistent findings of liability as well as excessive damage awards. In addition, the explicit grant of authority for the award of punitive damages and attorney's fees will serve to increase the likelihood that elements of the plaintiffs' class action trial bar will use this legislation as a way to increase class action litigation with little benefit being given to the general public.

X. FTC Rulemaking Authority

The Chamber is pleased that the H.R. 5777 directs the FTC to promulgate rules under this Act in a technology-neutral manner. Specifically, the bill prohibits the FTC from requiring the deployment or use of any specific products or technologies, including any specific computer software or hardware.

The Chamber appreciates that the bill attempts to maximize regulatory flexibility by granting the FTC authority to engage in rulemakings on a variety of matters. Given that business must respond rapidly to market developments and technological advancements, innovation should be encouraged, not hindered. However, at the same time, the Chamber is concerned that the sheer number of rulemakings will create needless regulatory uncertainty. In addition to rulemakings to create exemptions and exceptions, there are rulemaking requirements in many other areas of the bill including definitions (e.g., sensitive information and third parties), on notice, on accuracy, and on the process for granting safe harbor for self-self-regulatory initiatives.

XI. Effect on Other Laws

The Chamber applauds the inclusion of language that would preempt state laws governing the collection and use of data. However, the Chamber believes this language could be even stronger to help businesses avoid the complexity of having to comply with 50 different laws.

Conclusion

Once again, the Chamber greatly appreciates the opportunity to testify today. The Chamber stands ready to work with you on these and other issues. Thank you very much.

Appendix A

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

R. BRUCE JOSTEN
EXECUTIVE VICE PRESIDENT
GOVERNMENT AFFAIRS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5310

June 2, 2010

The Honorable Rick Boucher
Chairman
Subcommittee on Communications,
Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Cliff Stearns
Ranking Member
Subcommittee on Communications,
Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Boucher and Ranking Member Stearns:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, thanks you for the opportunity to offer thoughts and recommendations on your draft privacy legislation.[1] The draft legislation would fundamentally change how online and offline information collection and sharing is conducted, and has the potential to harm a vibrant and legitimate part of the U.S. economy. In addition, close scrutiny is needed to determine the bill's impact on existing laws. While the Chamber is pleased that the draft bill contains appropriate provisions to ensure predictable and consistent enforcement, the Chamber has some strong concerns with the draft bill that are highlighted below.

Definition of Covered Information

The Chamber believes that, as currently drafted, the definition of "covered information" is far too broad. It is important that such a definition encompass only data elements that could be used to commit identity theft or other direct consumer harm. Furthermore, the draft bill includes the term "unique identifier" within the definition of covered information. Such a term is overly broad as many social media websites assign each user a unique identifier that is publicly available and absent of any personal information. The bill would impose the same protections on user IDs as it would for name and email addresses.

Therefore, the Chamber strongly urges that data elements such as "unique identifier," "persistent identifier," "Internet Protocol address," "telephone number," and "fax number" be

[1] The Chamber represents many different types of companies and economic sectors with different concerns in the telecommunications and Internet areas and while the position stated in these comments is the official position for the U.S. Chamber of Commerce, our comments do not reflect the views of all company members.

removed from the definition except where such data has already been merged with other personal information elements. As an example, a persistent identifier on a device owned by an individual could literally cover a product code. Additionally, "covered information" appears to be a new definition that is not used by any other relevant privacy law. The Chamber is concerned about the conflicts and confusion that could arise from the use of this broad, new definition covering nearly all data.

A more appropriate way to approach the scope of covered information would be to craft a definition similar to "personal information" definitions found in many recent state data security and breach notification bills. These definitions tend to tie a person's first and last name or initial and last name with an address to a data element such as a social security number, drivers' license number, or financial account number. Within this type of definition there are data elements that can actually identify a specific person, as opposed to general categories of data elements which cannot identify a person.

Additionally, the definition of "personally identifiable information" should specifically exclude any personal information that has been rendered anonymous or "de-identified" prior to its use. This type of information is excluded from other federal privacy laws, such as the Health Information Portability and Accountability Act (HIPAA). Under HIPAA's de-identification standard, personal health information that has been de-identified in compliance with the law's prescribed standards is not subject to the HIPAA privacy rules. The Chamber recommends a similar de-identification standard be used in this legislation and believes this is the correct standard for public policy reasons, as well as to avoid direct conflicts on this issue in federal law, as discussed further below.

First Party Opt-Out Requirement

The Chamber is concerned that the proposal requires a "covered entity"—defined to include nearly every commercial business of even moderate size (i.e., those with more than 5,000 customers annually)—to obtain consumer consent prior to the collection and use of any customer information. The federal government has long recognized that consumers have a direct relationship with first parties that they chose to do business with and that their privacy expectations are different than when third parties are involved. For example, when a consumer voluntarily visits a Web site, certain information must be collected by that company, including their IP address or referrer URL, in order to deliver the content on the site. This information will be used by the first party Web site for non-transactional purposes, including Web site optimization and internal marketing practices. For this reason, the U.S. regulatory framework has long recognized a broad first-party exemption to consumer consent requirements which has been supported by the Federal Trade Commission (FTC) as recently as in its staff report on online behavioral (OBA) advertising principles. The Chamber believes this first-party exemption should be maintained in the current legislative proposal.

The impact to U.S. businesses from a new, statutorily-mandated consent standard for first parties would be vast. It would require all media, retailers, service-oriented businesses, marketing companies, advertisers and others—in both online and offline environments—to offer a detailed menu of opt-out options to all consumers for any data that may be collected or used

under any circumstances. Opting out of these uses of covered information would have several unintended consequences, including hindering fraud prevention, disabling basic Web site monitoring and advertising metrics, and hampering content customization and retail product recommendations online.

For example, such a requirement could require retailers to offer all credit-card-using consumers opt-outs for the use of bar code scanners at checkout counters. A bottom-line concern is that it is unclear which activities trigger a choice requirement. Many direct marketing activities already require choice under various federal laws or industry practices. In the draft bill, choice is required for marketing, advertising, and sales purposes. However, choice is not required for data analytics for product improvement—which is typically performed to improve sales.

Lastly, an opt-out consent standard would create a perverse incentive of requiring all media, retailers, service-oriented businesses, advertisers and others—in both online and offline environments—that do not already collect detailed consumer information to begin doing so in order to allow them to exercise opt-out choices over time. This, in turn, would require these businesses to develop and maintain detailed dossiers of personal transactions, in order to render all data from past transactions unusable if at any point in the future the consumer wishes to exercise an opt-out with respect to the prior collection of data. The Chamber does not believe that such a statute would further consumer trust; rather it may create greater privacy concerns while costing businesses millions of dollars to implement.

Notice and Consent for Offline Information

The Chamber strongly agrees that privacy principles should be applied to the collection and use of information in both the online and offline environments. However, any such legislative or self-regulatory regimes must be flexible enough to recognize the inherent differences that technology plays in each environment. Whereas the online environment is interactive and allows a link to a Web page that can deliver a privacy policy and offer choices for information use, the offline environment is much different, particularly when businesses employ manual or small-scale data collection devices, such as "3x5" survey or warranty cards inserted into magazines and publications. A privacy policy or notice in the form proposed by the legislation cannot reasonably be delivered on such collection devices, and choice cannot be obtained unless the consumer has access to the terms and conditions of the privacy notice. Another example involves the use of security cameras in stores that also monitor wait-time-in line at checkout to speed sales transactions for customers. It would not be feasible to provide a lengthy notice of privacy practices or choice prior to data collection. Simply put, in the offline arena, covered information may be collected in different formats and technologies, so more flexibility is needed for the timing and content of notice and how and where to offer choice.

In addition to the type of notice and consent to be provided in the online and offline settings, the proposed legislation must also consider the ability for businesses to comply with a notice prior to collection of covered data. For example, in both the online and offline environments, it is often impossible to deliver a notice before information collection begins. The above examples demonstrate this impracticality for the offline world but, importantly, this

impracticability is true in the online environment, too. Data collection begins immediately when a consumer enters a Web site address in a browser and clicks the go or return function, as an IP address must be collected before a Web site can be delivered to the browser for display. Also, each third party conducting business on the Web site, whether for marketing, fraud detection, or setting a time and data stamp, begins collecting information before the Web site actually loads. Therefore, significant amounts of covered information, as defined in the proposed bill, could be collected before a consumer would actually read a privacy policy and be able to make a choice. In many cases, consumers rarely if ever choose to read a privacy policy, so presumably all data collected to display the Web site would be in violation of the proposed law.

These practical problems need to be addressed before legislation is introduced, and the Chamber recommends eliminating any requirement that notice be provided prior to the "collection" of data. Many federal privacy laws, for example, set forth notice requirements in connection with businesses' uses of information for particular purposes in order to avoid such impracticalities of placing notice and consent regimes on the broad collection of data prior to its use. The Chamber recommends a similar focus on the use of data as further discussed below.

Concerns with Collection Restrictions

The language in Section 3 is focused on both the collection and use of covered information. There are major technological hurdles that companies in the online space would face to comply with the limitations on collection of covered information.

When a user decides to go to a Web page from a Web site, routine information is usually collected to help deliver and display that Web page. The collection of this data is integral to the proper and efficient delivery of Web pages; therefore, there could be tremendous technical ramifications if a consumer blocks the transmission of this data when selecting an opt-out option.

Advertising revenue frequently allows Web sites to offer consumers content for free. This ad-supported business model has been a key to the success of many Internet ventures and has helped to make the Internet an engine of growth in the U.S. economy. Unfortunately, the draft bill would disrupt this pro-consumer business.

Generally, the "operational purpose" exemption in the draft is too limited because it does not apply if the data is also used for marketing, advertising, or sales; dual-use of such data is a common industry practice. Under the draft, if a user chooses to opt-out, then the collection of non-identifying information (e.g., cookies or the user's IP address) is prohibited. However, in the offline world, non-identifiable user information is not subject to notice and choice used to target advertising displayed in magazines, newspapers, and billboards. The draft bill should be technology-neutral and should not favor one type of advertising over another.

Express Affirmative Consent for Disclosure of Covered Information

Numerous laws, including the Cable Communications Policy Act, Telecommunications Act, Gramm-Leach-Bliley Act, and Fair Credit Reporting Act allow business to share customer or other information with unaffiliated businesses whether for a "permissible purpose" or

otherwise. This draft would cover broadly all disclosures of customer or other covered information without regard for any intended purpose or to protect any perceived harm. It is unclear how the preemption language in this law could be followed with respect to these other legal information sharing allowances. By restricting this existing information flow, numerous businesses would be affected, especially small and local businesses that regularly use marketing lists for market research or direct mail prospecting.

No Opt-In for Sharing with Unaffiliated Third Parties

As currently drafted, the proposal requires opt-in "express affirmative consent" for the disclosure of "covered information" to unaffiliated third parties. The Chamber believes that this approach is wrong, as it profoundly alters commonly accepted business practices. The definition of covered information is extremely broad as stated previously and includes several largely anonymous types of data, including cookies, IP addresses, and unique identifiers for computers or devices. These types of data points are inherently neither personal nor sensitive in nature and, thus, should not be subject to the strictest consumer consent requirements. Current regulatory requirements subject only the most sensitive data categories to an opt-in requirement, and many of those provisions recognize a lower standard when that data is used for marketing or advertising purposes. Furthermore, the exceptions for disclosure seem too narrow. It appears that the only allowed disclosures of non-employee information are those that are legally required. However, many companies with strong disclosure protections also allow limited disclosures for safety or health reasons, like product recalls, or when the company is a victim of a crime.

It should also be noted that the definition of sensitive information is overly broad and could, for example, be interpreted to expand the definition to include self-reported financial and health information in survey data. Additionally, as noted below, if this draft legislation would create a second layer of data regulation, then there could be significant conflicts in statutory regimes between this bill's provisions and those of existing federal laws such as HIPAA or Gramm-Leach-Bliley. Such a result may leave many businesses in the untenable situation of being unable to comply with two separate federal data privacy laws for the same covered information.

Greater Latitude Should Be Granted for Self-Regulation

Numerous industry self-regulatory programs exist today requiring that information used for marketing or advertising purposes be subjected to robust consumer notice and choice requirements. The following have provided such guidance: 1) the Direct Marketing Association; 2) the Network Advertising Initiative; 3) the FTC, which published self-regulatory principles; and 4) a joint effort led by five marketing industry associations—the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association, the Interactive Advertising Bureau, and the Better Business Bureau—that published "Self-Regulatory Principles for Online Behavioral Advertising." These industry groups condition membership on compliance with their self-regulatory practices and sanction members who fail to comply. Self-regulatory practices promulgated by these industry groups or the FTC should be granted "safe harbor" status along with the concepts outlined in the law specifically for "network advertisers."

In addition, the draft does not address Web site browser controls, which are the paramount forms of online activity self-regulation today. Browser companies have increasingly developed their privacy-protecting user toolsets, and in recent years have begun to market these privacy differentiations to increase consumer use of their software. There is also a burgeoning privacy-by-design business model being developed using "plug-ins" and other tools to give browsers more privacy features and user controls. Increasing emphasis should be given to this self-regulatory vehicle. However, this draft would curtail the incentive for innovation regarding these browser controls.

Definitional Inconsistencies and Suggested Clarifications

Several definitions as currently drafted are either too narrow or too broad, and as constructed might unintentionally include many legitimate business practices that should not be covered by this draft legislation. The Chamber recommends revising the definitions of the following terms to ensure that the legislation sufficiently covers present day business practices:

- The definition of "render anonymous" exceeds practical use since it would apply to any "computer or device," which would restrict all forms of Web site analytics, market research, or other commonly anonymous uses of information. In addition, it would exceed the anonymization efforts governing "protected health information" under HIPAA which seems to be a contradiction in scope when comparing website use of personalized and protected health information. The Chamber recommends harmonizing the "render anonymous" definition with HIPAA's existing de-identification standard such that compliance with a similar de-identification process would provide a similar exclusion from this legislation.

- "Covered entity," "service provider," and "unaffiliated party": As drafted, it is possible for one entity to meet the requirements of all three definitions, thereby subjecting it to a number of different compliance obligations. The Chamber recommends carefully re-working these definitions such that there is no overlap or conflicting requirements for the same collection and use of covered information.

- The "advertising network" definition refers to "individuals," yet there is no definition of "individual" that would include a "unique identifier." As a result, few if any ad networks actually have "individual" information but rather cookies that are associated with a browser, which could be shared with a household or public network like a library or cybercafé.

- The definition of "operational purpose" should be expanded to include "detecting, preventing, or acting against actual or suspected fraud targeting the individual." Fraud detection products and services should not be restricted in this bill. This definition should also include market research.

- The definition of "transactional purpose," by specifically excluding marketing, advertising, and sales, prevents practices such as a customer being recommended

a certain book or album based on previous purchases, without a notice and opt-out. Marketing efforts designed to encourage transactions or sales should be considered as part of a transactional purpose and the definition should be expanded to include such purposes.

- The definition of "unaffiliated party" allows for sharing of information without opt-in consent as long as there is corporate ownership or control. The definition should also include entities that operate websites as joint ventures.

- The definition of Sensitive Information should be changed:

  - "Race or ethnicity" could cover ads delivered in different languages
  - "Mental or physical condition" is overly broad and could encompass common ailments, such as a stomach ache. The definition should relate a specific diagnosis.

Undefined Terms

The Chamber suggests that additional terms be defined to provide greater clarity and to ensure against inconsistent interpretations of their meanings, as follows:

- "Affiliates," "first party," and "third party": Further clarification on what is meant by first- and third-party entities will help industry better comprehend who is meant to have the various notice and choice obligations found in the bill.

- The terms for "consent," "opt-out consent," "express consent," "affirmative consent," and "express affirmative consent" are not defined. It is unclear how a compliant business would be able to understand and differentiate these terms when applied to data collection and use.

- The term "individual" should be defined to cover natural persons in the United States who are customers or visitors to online or offline channels where covered information is collected, and exclude employees, companies, and other persons or entities not intended to be covered.

- "Material change" in privacy practices is not defined, and it is unclear how it could be applied in cases where traditionally non-personal information uses as defined under "covered information" could be applied, such as with IP addresses or cookies where notice to these users is typically unavailable. It is unclear when or how an opt-in would be required and delivered, particularly for aspects of a policy where choice is not offered to begin with.

- There is no definition of "all or substantially all of an individuals' online activity." It is unclear whether this section is directed to Internet service providers, advertising networks, Web analytics providers or other entities. The legislation should clarify what is the perceived threshold for "substantially all."

The Chamber also recommends such a definition exclude fraud prevention and market research services.

Data Retention Language

The Chamber has concerns with the data retention provisions in Section 3(e)(2). If covered information is collected and/or used for multiple purposes, including transactional or operational purposes, it is important to know whether this section applies. Also, there seems to be a conflict between the deletion/anonymization requirement of this section and Section 4(b)(C), which protects against the alteration or destruction of covered information. In addition, where the user is in control over his or her own information (such as account data or transaction history) through a direct relationship with a provider, retention limits appear unnecessary and counterproductive.

Location Information

Precise geographical information should not be codified into law at this time as sensitive personal information. Instead, the Chamber recommends that the collection and use of this data be governed by self-regulatory models at this time. This is a rapidly evolving technological field, which could ultimately be helpful in such areas as fraud detection. Therefore, the Chamber believes that this type of information would best be left to a more flexible framework with guidance from the FTC.

Aggregate or Anonymous Information

The Chamber agrees with what appears to be the general intent of Section 5 of the proposed draft to exclude from the draft bill's notice and choice provisions the collection, use and disclosure of aggregate information or information that has been rendered anonymous. However, it is unclear how Section 5, as currently drafted, would function, and therefore requires further clarification. Additionally, it appears that the definition of "render anonymous" may be constructed too narrowly to cover the various methods by which personal information may be de-identified prior to use so that it is subject to this exclusion. As noted above, the Chamber believes it would be important to harmonize this provision and applicable definitions with similar safe harbors in other federal privacy laws, such as HIPAA's de-identification standard.

Modification to Section 7 Report

The Chamber recommends that the report in Section 7 not be limited to the Federal Communications Commission (FCC) alone, but instead should include the FTC as well. There are myriad privacy-related laws that exist today that should be more closely studied to better assess the impact that this legislation would ultimately have. It would be prudent for the implementation of the proposed regulations in this draft to only take place after these reports are received and reviewed effectively.

Competitive Neutrality

The draft potentially subjects different entities involved in online behavioral advertising to different types of notice and consent obligations, depending upon the type of business model they employ. For example, if a covered entity collecting information via the Internet posts its privacy notice "on the website" through which it collects information, it can avail itself of opt-out notice for the collection and use of covered information. While this approach may be workable for companies engaged in the "cookie-based" online behavioral advertising business models, it is unclear how it would apply to entities that may not (presently or in the future) rely upon visits to websites to collect data. Likewise, the draft allows entities that construct and maintain user preference profiles to utilize opt-out consent for the collection and use of covered information, but appears to preclude any new or different business models from doing so.

The draft should provide all entities involved in OBA with equal opportunities to utilize opt-out consent for the collection and use of covered information. It should not disfavor particular business models with more burdensome regulatory obligations, since doing so would deter entry, harm innovation, and undermine competition and choice in the OBA marketplace.

Conflicts with Other Federal Privacy Laws

The Chamber agrees with what appears to be the intent of the provision in Section 11 stating that this bill should have no effect on activities covered by other enumerated federal privacy laws, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and HIPAA. As currently drafted, however, the opening clause of the proposed legislation would create a significant exception to this general rule (i.e., by stating "except as provided in this Act"), which could be interpreted by the FTC or by courts to imply that this legislation would create another layer of regulation in addition to provisions in each of the enumerated acts. Given the potential conflicts with having the same type of data collection and use covered by more than one federal privacy regime, a covered entity could very well find itself unable to comply with two separate federal privacy laws for the same covered information, thereby involuntarily subjecting itself to fines and other enforcement actions for non-compliance with one or both of the acts. To avoid this potential conflict with existing federal privacy regimes, the Chamber strongly recommends that this section of the proposed bill be clarified to provide an explicit carve-out from the definition of covered entity for entities already covered by the enumerated acts.

Exemption for Publicly Available Information

The Chamber strongly believes that this bill should explicitly exempt publicly available information from the definition of "covered information." By definition, publically available information is not private. Information that is already in the public domain should not be covered by the bill. Moreover, this type of information cannot be used for identity theft purposes or any other nefarious activity, so its inclusion in this bill is unnecessary and should be explicitly left out.

Exemption for Employee Information

Similar to the previous comment, the Chamber strongly believes that employee information should be excluded from coverage by the proposed legislation as this information, while confidential to the employer and employee, must not be subject to an employee's choice to prevent its collection by the employer. Not only are employers required under federal tax and other laws to collect much of the data that would meet the definition of "covered information" in this draft bill, there are numerous existing federal and state laws that already protect the privacy and security of such employee information, not to mention court decisions that have sought to strike the proper balance between employer and employee rights to the information. It would be well beyond the stated purpose of this bill to re-write the laws on employer/employee data collection and use. Moreover, if employee information were to be covered, the proposed legislation would arguably affect nearly every employer in the nation, including the smallest of commercial entities, forcing them to modify employee data management practices. Therefore, the Chamber strongly recommends that the definition of "covered information" include an exclusion for information collected from or about a former, existing or prospective employee by an employer.

The Chamber thanks you for the opportunity to weigh on this draft bill and looks forward to working with you and your staff on this very important issue.

Sincerely,

R. Bruce Josten

Cc: The Members of the Subcommittee on Communications, Technology and the Internet