THOMPSON COBURN LLP

One US Bank Plaza
St. Louis, Missouri 63101
314-552-6000
FAX 314-552-7000
www.thompsoncoburn.com

February 17, 2011

Mark Sableman
314-552-6103
FAX 314-552-7103
msableman@
thompsoncoburn.com

Via Electronic Submission

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

Dear Secretary:

American Business Media ("ABM") hereby submits its comments on the FTC's preliminary staff report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," issued December 1, 2010 (the "Report").

Summary

As more fully set forth below, ABM believes that in addressing personal privacy concerns, the FTC should remain mindful that essential business-to-business communications are not unnecessarily affected or inhibited. To that end, ABM believes that:

- Voluntary codes of conduct and industry self-regulation procedures, particularly should be preserved, including for new and emerging technologies because of the benefits they provide in flexibility, practicality and workability.

- The FTC should specifically recognize as a "commonly accepted practice," or as otherwise exempt from rules designed to protect personal privacy, the collection and use of information obtained in a person's *business capacity or business interests* (that is, information obtained about an individual in his or her capacity as an employee or representative of a business enterprise, which may include for-profit businesses, individual consultancies, associations, non-profit entities, and other organizations).

- Contextual advertising, first party marketing, data sharing among affiliates, third party marketing and legal compliance information collection should also be recognized as "commonly accepted practices" for the reasons explained below.

- The "consent by action" approach should be recognized as appropriate for business-to-business communications and activities.

- In promoting standardization and clarity of privacy policies, the commission should recognize the flexibility needed in the business-to-business marketplace, as well as the successful self-regulation that has long been a key feature in the growth and success of that marketplace.

- With respect to online behavioral advertising, the commission should permit self-regulatory programs to develop flexible and meaningful protection for users. The commission should further study "Do Not Track" proposals before recommending or implementing any such regulations.

- In addressing privacy concerns, the Commission should also consider carefully the constitutional rights of business and other publishers to gather news and information, apply editorial judgment and filtering, and prepare and disseminate both news and advertising.

Background

Business-to-Business Communications and Transactions

American Business Media is an association representing more than 200 business-to-business ("B-to-B") information providers, including print and digital publishers, websites, and organizers of trade shows and similar events. The B-to-B industry includes approximately 2,000 magazines and approximately 3,500 websites, with publications from *Oil and Gas Journal* to *Advertising Age* to *Insect & Disease Control Guide*. ABM members play an essential role in assembling and disseminating the industry-specific news and information needed by businesses and key industries in thousands of different fields worldwide, thereby fostering commerce and economic growth.

Like other information providers, ABM members have increasingly turned to digital methods of publishing and distribution. This medium enables them to communicate quickly and effectively with their subscribers and constituents, and provides other benefits as well, including the ability to tailor information and advertising to business users' particular needs, interests and even geographic location. Just as the Internet and digital technologies have spurred many advances, efficiencies and new business models, digital business models will continue to change and evolve with technological advances, creating new opportunities and new economic efficiencies.

Business-to-business information providers use various kinds of data, including, for example, technical data, industry metrics, and government reports, in order to assist their customers in their decision-making. To the extent B-to-B data collection activities, both offline and online, include data about individuals, such information relates to data about individuals acting in their business or professional capacities. For example, such B-to-B data about an individual

may consist of a name, job title, business name, business contact information, and particular business interest (articles read, webinars attended, etc.) — all quite different from the data concerning individuals acting in their private capacities for personal, household or family purposes, which is more fundamentally the subject of privacy protections under US law.

ABM believes that emerging privacy concerns raised by new technologies are best dealt with through industry self-regulation rather than statutes or regulations. More specifically, ABM believes that the FTC should refrain from taking actions that could interfere with B-to-B communications, particularly in regard to the industry's ability to meet the demands of our customers for valued content and services. One certain lesson for the B-to-B content industry from its experiences with the Internet is that we must have the ability to remain flexible in order to accommodate future innovations. ABM believes that imposing new regulations on providers of B-to-B information, particularly regulations written with a view to perceived problems in business-to-consumer transactions, could improperly inhibit or restrict valuable and unique B-to-B activity, now and in the future.

Like all business entities, ABM members are subject to laws such as section 5 of the FTC Act, and to various self-regulatory codes of conduct. Such laws and self-regulatory measures have proven to work well in B-to-B context. Our interactions with customers occur in relation to business issues of mutual interest, where only business information and credentials are likely to be exchanged, and flexible rules are needed because of technological and market-driven advances in how business communications and transactions are handled. With marketplace-driven guidelines, customers turn to competitors if one company's practices are not satisfactory, and it is precisely this aspect of competition in the B-to-B information markets that helps ensure strong self-regulatory programs.

Usefulness of Targeting in B-to-B Communications

The ability to track user interests and target them with information and advertising geared to their particular interests is particularly critical in B-to-B communications. Business users use B-to-B websites, and otherwise utilize the services of B-to-B companies (for example, at trade shows), for the purposes of obtaining and sharing industry information and making industry connections. Their personal privacy interests are not at stake, and as explained below, the sharing of their business credentials and interests does not implicate traditional privacy concerns.

Consider the Chief Information Officer who browses B-to-B websites devoted to information technology services, focusing specifically on directories of web hosting providers and articles about web hosting. That CIO may subsequently be presented with advertisements from web hosting providers on his business computer. Such business advertisements, directed to a business user on a business computer, in response to business activities on business websites, provide useful business information and connections. Such activities support the efficient and productive conduct of business. Indeed, business would be impeded if general privacy laws prevented such targeted advertising, and required, instead, our CIO to be presented with only non-targeted ads that may not be relevant to his or her interests.

Or consider the attorney who uses *American Lawyer* magazine and other law-related websites and publications serving the legal services market that are operated by ABM member ALM Media Properties LLC. A particular lawyer may, in the course of using ALM's publications, websites and services, register for an employment-law related seminar, peruse articles relating to employment law, purchase an employment-law related book, and register for an employment-law related trade show. Using tracking technologies, ALM can quite logically assume that this lawyer practices in the employment law area, and would be interested in employment law information, tools and opportunities. ALM could, using that information, tailor both its editorial or advertising offers to this user, and permit ad networks to do the same. As a result, the employment lawyer would be presented with employment-law related information and offers, on ALM's sites and on other sites—rather than, say, tax or patent law information and offers that the lawyer will find irrelevant or even bothersome. No harm arises from such tailoring. Indeed, to the busy employment lawyer, the presentation of useful information and offers in response to his business browsing on business related websites on a business computer, rather than useless or irrelevant information and offers, is a great benefit.

ABM submits that the benefits of targeting, particularly in the B-to-B area, need to be carefully considered in connection with any attempt to legislate or regulate in this area. Moreover, as part of the consideration, the FTC should note that business users and customers still retain the ability to opt out of collection and use practices as part of notice and consent regime in the self-regulatory frameworks that have brought such benefit to users since the early days of Internet commerce.

Preference for Industry Self-Regulation

ABM strongly supports actions that encourage the development of voluntary codes of conduct and industry self-regulation procedures. Broad proscriptive rules developed by government agencies often lack the flexibility, practicality and workability of voluntary industry codes and procedures, and could be harmful to the development of new technologies and business practices that could enhance users' online experiences.

ABM also supports the concept that the government should recognize a safe harbor for industry actions made in compliance with recognized and approved self-regulatory standards. For example, ABM believes that compliance with the carefully developed self-regulatory program with respect to online behavioral advertising should qualify a participant for a safe harbor.

Specific Comments on Proposed Privacy Framework

1. Scope of covered data

Are there practical considerations that support excluding certain types of companies or businesses from the framework?

As discussed more fully in section 2.a. below, ABM believes that B-to-B communications and activities are so qualitatively different from business-to-*consumer* communications and activities that they should be treated differently, through recognition of a "commonly accepted practice" for business communications. The recognition being sought here is limited to those circumstances in which a B-to-B company collects and uses business related-data for business purposes.

Is it feasible for the framework to apply to data that can be "reasonably linked to a specific, consumer, computer, or other device?

ABM believes that it is neither feasible nor necessary to apply the proposed framework to data that can be linked to a specific consumer, computer or device. In the business world, Internet Protocol (IP) addresses often do not correspond to particular computers or users, but rather to business portals or gateways. Many users operate among various computers, making the use of IP addresses as an identifier difficult to achieve. In short, individual IP addresses are of only limited use in serving as unique identifiers in a business context and should not be treated in the B-to-B context as such identifiers.

2. "Commonly accepted practices"

Is the list of proposed "commonly accepted practices" set forth in Section V.1 of the report too broad or too narrow?

Are there practices that should be considered "commonly accepted" in some business contexts but not in others?

ABM believes that the Privacy Framework should recognize that certain practices, including both offline and online B-to-B practices, do not require new regulations and should be specifically included among "commonly accepted practices" as referenced in the Report. More specifically, we view "commonly accepted practices" as including: (a) business-to-business communications and transactions, (b) contextual advertising, (c) first party marketing, (d) data sharing between affiliates, (e) third party marketing, and (f) enforcement of legal and intellectual property rights.

a. Business-to-Business Communications

Any new privacy laws or regulations should recognize collection and use of information obtained in a person's *business capacity or business interests*—that is, information obtained about an individual in his or her capacity as an employee or representative of a business enterprise (which may include for-profit businesses, individual consultancies, associations, non-profit entities, and other organizations)—as a "commonly accepted practice." Additionally, any new privacy laws or regulations should be framed to exclude business transactions from its coverage. ABM would submit that this notion is implicitly recognized in the Report, since business transactions would fit within the "product and service fulfillment" commonly accepted practice described on page 53 of the Report.

Importantly, courts have recognized this distinction between business users and individuals acting in their personal capacities with respect to privacy interests. "[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy." *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *see also* Restatement (Second) of Torts § 652I cmt. c ("A corporation, partnership or unincorporated association has no personal right of privacy."); *Browning-Ferris Indus. v. Kelco Disposal, Inc.*, 492 U.S. 257, 284 (1989) (O'Connor, J., concurring in part, dissenting in part) ("[A] corporation has no ... right to privacy."). Indeed, the Supreme Court has recognized that "a business, by its special nature and voluntary existence, may open itself to intrusions that would not be permissible in a purely private context." *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 353 (1977). Many courts have found that business employees, acting as such, have little or no privacy interests in their business conduct. *E.g., Curto v. Medical World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. 2006) ("Employees expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network.").

Subjecting communications with persons in their business capacities to the same limits and rules that apply to communications with persons in their personal capacities, especially if those rules involve what are essentially opt-in requirements for collection and sharing of information, would significantly hamper the flow of business information and subsequently the flow of commerce crucial to America's economic growth and prosperity.

The context in which information is collected or used usually clarifies B-to-B and business-to-consumer activity. For example, someone who shops at Macy's online should be presumed to be acting in a personal capacity, while someone who visits the *Engineering News-Record* website should be presumed to be acting in a business capacity. Focus should be placed on the likely *purpose* of the activity, and the nature of the transaction between provider and user, as judged by the context and information obtained through that activity.[1]

The competitive marketplace is likely to impose more appropriate and flexible restraints on collection and use of business information. For example, as virtual tradeshows have become more common and accepted, attendees in such events have come to accept practices such as distribution of attendee lists, sharing of contact details, and targeted messages—practices that are all compatible with the goal, common to exhibitors and attendees, of sharing as much exhibitor data as possible in a set period of time. In other business communities—for example, journalists or IT security specialists—industry norms and the marketplace may dictate more restrictive sharing practices. Clearly, however, these different business communities will not be well served by one-size-fits-all rules, particularly ones derived from the totally different consumer marketplace.

[1] In distinguishing between business and personal users, we submit that the distinction should *not* be based on whether a home or office address is used, since in many fields of business, including the agricultural and medical fields, home addresses are often used for business purposes.

b. Contextual Advertising

ABM agrees with FTC staff recommendations that contextual advertising should fall within the "commonly accepted practices" category. Report, p. 55 n.134. (The FTC has defined contextual advertising in the online context as advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result.) This view was first expressed in the FTC's February 2009 STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING at 29-30.

c. First Party Marketing

What types of first-party marketing should be considered "commonly accepted practices"?

ABM believes that where information is collected by a trusted first party, it should be sufficient for that party to give traditional notice and choice as to its practices in using or sharing that information. Trust in the first party's disclosures and promises is key. ABM agrees that first parties must provide clear and conspicuous privacy notices, and at the same time, users have an obligation to read and understand those notices.

As recognized in the FTC February 2009 report (pages 26-28), "first party" behavioral advertising practices "are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites" and accordingly do not need to be regulated at this time. Thus, in the context of the current Privacy Framework, first party data collection for marketing purposes should be considered a "commonly accepted practice."

Should first-party marketing be limited to the context in what data is collected from the consumer?

Regardless of the method of collection, limits should not be placed on first party marketing to a consumer who has had the opportunity of reviewing appropriate notice of collection practices and the ability to opt out of such practices, regardless of delivery methods. In our multi-faceted communications world businesses typically communicate using multiple and different means of channels, and any presumption that communications initiated by one means (e.g., email) must continue solely through that particular medium would stifle the conduct of business and the flow of commerce.

d. Data Sharing Among Affiliates

Should marketing to consumers by commonly-branded affiliates be considered first-party marketing?

ABM believes that marketing by business units under common control or close affiliation, even if under different branding, should be treated as first party marketing, at least in the B-to-B

context, because business users understand that information provided to one business unit of a corporation may be shared with another unit belonging under the same corporate umbrella.

While ABM understands that the FTC may be concerned that non-business users may not understand that differently branded consumer companies may have common ownership, such a concern does not apply in the B-to-B world. In the B-to-B information content world, providers serve particular business communities, and users of B-to-B websites understand and expect that their business credentials and interests may be used within that community, regardless of branding, for the purpose of promoting business connections and opportunities.

Moreover, B-to-B companies often expressly explain, on their websites and/or privacy policies, their subsidiary and affiliate network. In some cases they may even post a common privacy policy on the parent company's website. To ABM's knowledge, B-to-B companies disclose their data sharing practices, disclose the business units under common control and opt-out mechanisms, and disclose sharing among affiliates, and permit that sharing only to the extent that the privacy practices of the affiliates are consistent with their own practices. These practices, which are common and expected in the B-to-B marketplace, suggest that no new special rules are needed.

Therefore, at least in connection with business communications, the "commonly accepted practice" for first party marketing should not be limited on a business unit basis, or to commonly branded business units, but rather should apply to all commonly owned or controlled or affiliated companies, using the common tax and securities law definitions which include affiliates owned 20% or more by a parent within that parent's umbrella.

e. Third Party Marketing

Under current practices, B-to-B companies that collect information that may be transferred to third parties provide notice to their users of their information sharing practices, and provide either an affirmative choice or means by which users may opt out of such sharing. This well-established notice-and-choice practice works well in the B-to-B marketing context and should be allowed to evolve as expectations evolve. Indeed, such third party marketing is an essential and important part of the user experience in the B-to-B space, and B-to-B users expect it. For example, a construction contractor who subscribes to *Engineering News-Record* is more likely to welcome and appreciate third party business marketing that is narrowly focused on his region or construction specialty. The expectations of B-to-B users are fully protected by the opt-out choice mechanisms that are commonly provided.

The Report, at pages 57-63, is unclear as to what notice-and-choice mechanism, or other approach, the FTC staff views as most appropriate for third party marketing. ABM stresses that customary notice-and-choice practices satisfy the objectives set forth in the Report for B-to-B communications. For example, the Report suggests that choices should be offered "clearly and concisely," "at a time and in a context in which the consumer is making a decision about his or her data," and that "easy-to-use choice mechanisms" should be provided. Customary notice-and-choice practices meet these standards; specifically, before the user provides personal

data, he or she is informed of the first party's data practices, most often through a prominent link to or copy of the first party's privacy policy. That policy customarily contains a simple and clear statement of the first party's information sharing practices (e.g., "We may share your name and address with marketing partners," or "We will not share your name and address with any other parties"). The user upon reviewing the first party's information-sharing practices will at that point have several easy-to-follow choices, which may range from turning away from the first party's site, or, if more granular choices are offered, clicking on election boxes as to the extent of third-party sharing to be permitted.

More restrictive rules with respect to information sharing with third parties would prevent or inhibit many useful business practices, particularly in the B-to-B marketplace. The very nature of successful commerce is to establish contacts and relationships that further opportunities for business and economic growth.

For example, when a businessperson attends a trade show relating to his or her industry, the privacy policy of the trade show provider usually explains that registration information is given to all exhibitors, such as in a conference participant directory. Most trade show operators already offer their attendees options on whether to include the participant's registration information. That information sharing practice is thus fully disclosed to all attendees—and indeed it is no surprise, since business attendees go to trade shows with the specific expectation of making business connections and obtaining useful industry information—whether immediately or at some future date. Indeed, the sharing of business credentials (i.e., the information that is typically printed on a business card) at a trade show significantly facilitates commerce and new business opportunities and is a long standing precedent. Business persons do not consider their business credentials to be personally private information and in most cases, gladly share contact information for business leads. In these circumstances, the only rule that makes any sense is requiring disclosure of information sharing practices and opt-out capabilities, as is customarily done.

Any across-the-board "opt-in" requirement for third party marketing would wreak havoc on business-to-business meetings like trade shows or industry conferences. If, for example, trade show exhibitors had to get specific permission from each attendee before contacting any attendee, or if attendees could not themselves market to trade show exhibitors without express opt-in permission, the wheels of commerce would slow considerably. In fact, we believe this change in practice would hinder business information sharing that historically has been a commonly accepted practice, beginning with the exchanging of business cards and contact information.

Many other kinds of information sharing with third parties customarily occur in business-to-business communications. Business people understand and generally welcome exchanges of information that might open up business connections and opportunities. No harm occurs to the affected business users from such exchanges; at most, such exchanges simply prompt a communication from a business that may or may not interest the user, and follow-ups from that business will occur only if the user expresses interest in the connection or opportunity that is offered. B-to-B providers typically notify their users of the possibility that they will engage in

such information sharing, and the users have the opportunity, if they wish, to opt out of such sharing of their business credentials and interests.

For all of these reasons, in the context of the current Privacy Framework, ABM believes that sharing of first party collected data collection with third parties for marketing purposes should be considered a "commonly accepted practice" subject to the current "notice-and-choice" regime, and that no new laws or regulations are necessary.

f. Legal compliance.

Information content businesses often must collect data about their users in order to track compliance with legal requirements such as licensing restrictions, and in order to prevent copyright infringement or piracy. As the Report notes (pages 54-55), in any data privacy regulations, care must be taken to exempt customary data collection measures designed for such purposes and for other necessary purposes, such as product and service fulfillment.

2. Consent by Action

Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices?

ABM believes the approach sometimes characterized as "consent by action" or "conditional access," outlined on page 60 of the Report, is very appropriate for business-to-business activities. The Internet offers a plethora of choices to users, and in making choices as to what sites and applications they will access, users consider, among other things, data privacy practices. Internet users expect those who collect data to explain their practices via their privacy policies and to provide choices, and the FTC has required such disclosures. They, therefore, accept the disclosed privacy practices of a particular site by virtue of the fact they are accessing the site or using its applications.

Notably, this "consent by action" principle allows collection and use of information on an opt-out basis, which is customary, necessary, and expected in many business-to-business situations, where business people actively seek ways to connect with others and with useful information. It is therefore important that laws and regulations not inhibit such useful communications, and we believe the "consent by action"/"take it or leave it" works well in that context. It permits users to make their own choices and does not impede communications. Put another way, the presentation by business users of their business identity and credentials, and other data that they willingly disclose, to business websites or applications, and the collection and use of that information by a business entity, needs no further regulation.

3. Privacy Policies

What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?

ABM agrees with the FTC's desire for simple, standard, easy-to-understand privacy policies. In fact, ABM members post such policies to make sure their data practices are transparent. We believe, however, that any forced standardization in privacy policies is not a workable approach for many industries. While ABM supports general rules promoting clarity, simplicity, and understandability of privacy policies, any enforced standardization could interfere with the necessary flexibility in business practices in this context and cannot anticipate the wide variety of commercial transactions that occur over the Internet on an hourly basis. The business-to-business marketplace essentially self-regulates when businesses have fair and understandable privacy policies, thus enhancing customer trust. ABM and its members acknowledge that failure to accurately describe privacy practices is enforceable through Section 5 of the FTC Act or class action litigation.

ABM adopted "Customer Privacy Guidelines" for its members to follow. Among other things, these guidelines direct members to respect the privacy of their customers, prospects, and Web site visitors when conducting business, to adhere to all applicable privacy laws in the countries in which they operate, and to adopt and implement privacy guidelines for the protection of customer information. The guidelines cover 15 privacy principles related to issues such as notice, collection, choice, compliance and security. ABM believes such practices support members' efforts to develop transparent relationships with their users and clients.

4. Online Behavioral Advertising

How should a universal choice mechanism be designed for consumers to control online behavioral advertising?

What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?

If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?

ABM believes that the promising and emerging techniques of online behavioral advertising, developed by those who best understand the technology and backed by robust enforcement, should be handled through flexible and intelligent industry self-regulation. Inflexible and possibly inappropriate legal regulations could hinder future innovation, which has been the cornerstone of expanded e-commerce.

Current efforts across the content, marketing and advertising industry are developing and continue to grow and strengthen. We strongly urge that self-regulatory actions be allowed to demonstrate their effectiveness and that formalized regulations are not hastily employed. Furthermore, regulation runs the risk of stifling advances in the rapidly evolving technology

environment, for instance, additional granularity in opt-out choices, as well as changing customer demands and expectations.

ABM remains concerned about a "Do Not Track" proposal without receiving clarification on the technology and means by which such a program would be implemented. "Do Not Track" efforts may gloss over important differences in terms of costs, benefits, and operations, and thus may lead to bad policies and negative outcomes, especially for business users.

Analogies with "Do Not Call" lists are highly flawed, because the telephone and Internet situations are quite different. Among other things, "Do Not Call" procedures were implemented at a time when the telephone technology and telemarketing procedures were well understood, and various non-legislative solutions had been tested. Behavioral advertising, however, is still quite new, most Internet users are not familiar with how it works and what it does, targeted Internet ads are far less intrusive than unwanted telephone calls, and it is not yet clear how Internet users will react to behavioral advertising and industry self-regulation. Implementation of "Do Not Track" rules at such an early stage of the technology's development could effectively kill what is otherwise a promising and useful practice—for example, if a large segment of consumers, acting on unfounded theoretical concerns, cut off all tracking before even viewing the benefits of the practice.

Finally, many specific issues would need to be addressed before any "Do Not Track" rules are finalized. The Report contains few specifics on this concept, and many issues would need to be considered, including, for example, how the mechanism would distinguish between different users of the same computer, and between a single individual's personal and business activities.

ABM believes that "Do Not Track" technologies imposed by law are certainly premature and may inhibit much legitimate online behavioral advertising.

5. First Amendment Concerns

Particularly with respect to B-to-B content providers, ABM would respectfully remind the FTC that care must be taken in formulating any privacy rules that might chill or inhibit expression protected by the First Amendment. ABM members engage in publishing both traditional core speech (news and editorial content) and commercial speech (advertising). They take part in all aspects of the publishing process—gathering raw news and information, applying editorial judgment and filtering, and preparing and disseminating both news and advertising. We remain concerned that overly broad privacy rules and regulations could chill or inhibit any of these protected activities.

For example, the gathering of data is an essential element of newsgathering. In some cases, states have recently legislated, in the name of personal privacy, prohibitions on the gathering and use of certain kinds of information for marketing purposes. ABM agrees with the recent decision of the United States Court of Appeals for the Second Circuit that the First Amendment bars such efforts by government to prohibit use of truthful information by content providers. *IMS Health v. Sorrell*, 2010 WL 4723183 (2d Cir. Nov. 23, 2010), *cert. granted sub*

nom. Sorrell v. IMS Health, 131 S.Ct. 857 (2011). At the very least, while *Sorrell v. IMS Health* is pending before the United States Supreme Court, the FTC should not take any action to regulate the collection and use of information on grounds of protecting personal privacy, as was done in that case.

Additionally, commercial speech (advertising and other invitations to engage in business transactions) is an important aspect of our national commerce which receives constitutional protection because it helps citizens make intelligent and well informed decisions. *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748, 775 (1976). In *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980), the Supreme Court created a four-part test for regulation of commercial speech: (1) lawful and not misleading commercial speech is presumptively protected, and regulation is allowed only (2) where a substantial asserted governmental interest exists, (3) the regulation directly advances that governmental interest, and (4) the regulation is no more extensive than is necessary to serve that interest. Assuming *arguendo* that protection of personal privacy would qualify as a substantial governmental issue, the third and fourth *Central Hudson* factors would need to be met. These factors, however, do not permit regulations based only on speculative or unproven concerns. *Turner Broadcasting Sys., Inc. v. FCC*, 512 U.S. 622, 664 (1994); *Greater New Orleans Broadcasting Association, Inc. v. United States* 527 U.S. 173, 188 (1999). Particularly where a particular technology, like online behavioral advertising, is relatively new and untested, regulatory restrictions based on speculation about its likely effect are unlikely to meet the stringent *Central Hudson* test.

These constitutional concerns further suggest that regulation of online advertising should be approached carefully since by its very nature, such regulation would inhibit B-to-B information providers to gather the information necessary to determine when and to whom they communicate. Again, we would urge that self-regulation should be given room to develop, that full empirical evidence should be developed to test claims of privacy harms, and that if regulations are developed, they should be narrowly tailored to address proven empirical harms, so as to not unnecessarily inhibit business communications that are vital to our economy and protected under our Constitution.

Thank you for your consideration of these comments.

Sincerely,
THOMPSON COBURN LLP

By
Mark Sableman

Attorneys for American Business Media

cc: Mr. Clark Pettit
5292353