



## DMA COMMENTS ON STEARNS AND BOUCHER PRIVACY LEGISLATION DISCUSSION DRAFT

[Tell a friend about this page](#)

[Suggestion box](#)

**June 7, 2010** — The Direct Marketing Association (DMA) has sent comments to House Representatives Rick Boucher (D-VA) and Cliff Stearns (R-FL) regarding their privacy legislation discussion draft. DMA expressed its concerns regarding the changes the bill would cause in the collection of online and offline information.

The full text of DMA's comments follows.

\*\*\*\*\*

**COMMENTS OF THE DIRECT MARKETING ASSOCIATION  
TO CHAIRMAN BOUCHER AND RANKING MEMBER STEARNS  
ON THE STAFF DISCUSSION DRAFT OF PRIVACY LEGISLATION**

**June 4, 2010**

The Direct Marketing Association (“DMA”) appreciates the invitation to comment on your Discussion Draft of legislation on information collection, use and disclosure. The DMA ([www.the-dma.org](http://www.the-dma.org)) is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. DMA advocates industry standards for responsible marketing, promotes relevance as the key to reaching consumers with desirable offers, and provides cutting-edge research, education, and networking opportunities to improve results throughout the end-to-end direct marketing process. Founded in 1917, DMA today represents thousands of companies from dozens of vertical industries in the U.S. and 50 other nations, including a majority of the Fortune 100 companies, as well as nonprofit organizations. Included are Internet-based businesses, cataloguers, financial services, book and magazine publishers, retail stores, industrial manufacturers, and a host of other segments, as well as the service industries that support them.

The DMA has significant concerns with the manner in which the bill would change the online *and* offline collection and use of information. We strongly believe that self-regulation is the appropriate approach to address information practices. Unlike legislation, self-regulation is better suited for governing a rapidly changing environment and responding to evolving consumer expectations. We respectfully ask that any proposed legislation set forth by your Committee allow for the continuation of industry

self-regulatory efforts as a means of providing transparency and choice to consumers. We explain our concerns with the Discussion Draft below.

## **1. Self-Regulation Is the Appropriate Approach for Addressing Information Practices**

The DMA strongly supports industry self-regulation as the appropriate avenue for addressing information practices, whether they be offline or online, for advertising and marketing. The DMA, along with other organizations such as the Interactive Advertising Bureau, Network Advertising Initiative, TRUSTe, the AICPA's WebTrust, BBBOnline, the Online Privacy Alliance, and the Council of Better Business Bureaus National Advertising Review Council, have long been committed to promoting business practices among our members that provide for effective transparency and choice to consumers. Our programs protect consumer privacy offline and online, and offer the most flexible and effective means of doing so.

For instance, in the offline world, DMA requires all of our members to adhere to the *Commitment to Consumer Choice Guidelines*, which apply to our members that use mail to communicate with consumers. These guidelines reflect our belief that the direct marketing community must meet consumers' expectations of choice in today's marketplace. The guidelines require DMA members to provide existing and prospective customers and donors with notice of an opportunity to modify the receipt of future mail solicitations from their organization in every commercial solicitation.

In the online arena, in July 2009 the DMA was one of the leading associations that partnered with the American Association of Advertising Agencies, the Association of National Advertisers, and the Council of Better Business Bureaus to create the *Self-Regulatory Principles for Online Behavioral Advertising*, a comprehensive set of self-regulatory principles for online behavioral advertising.<sup>[1]</sup> We have since incorporated the principles into our *Guidelines for Ethical Practice*, to which all of our members must adhere.<sup>[2]</sup> Along with the Council of Better Business Bureaus, the DMA will enforce these principles through both new and existing robust compliance mechanisms.

The Discussion Draft seeks to regulate a variety of entities that are presently subject to industry self-regulatory programs, including those described above, and sets heightened and unworkable standards that far exceed current industry guidelines and best practices. Such entities already adhere to robust and transparent privacy principles, and the Federal Trade Commission ("FTC" or Commission) has encouraged and is very supportive of self-regulation as the right approach for marketing and advertising regulation.

The FTC has encouraged the development of such self-regulatory programs. In February 2009, the Commission staff issued a report on *Self-Regulatory Principles For Online Behavioral Advertising*, with the stated purpose of "guid[ing] industry in developing more meaningful and effective self-regulatory models."<sup>[3]</sup> The Commission's report also expressed support for self-regulation "because it provides the necessary flexibility to address evolving online business models."<sup>[4]</sup> Since the issuance of that report, we released the *Self-Regulatory Principles for Online Behavioral Advertising*, which reflects our commitment to providing robust transparency and choice to consumers. We thus firmly believe that self-regulation plays a vital role in setting forth best information

practices. To the extent that any legislation proceeds, we encourage you to preserve and allow incentives to continue to exist for this essential role for industry self-regulation.

**2. The Bill's Express Affirmative Opt-In Consent Requirement for the Transfer of Data to Third Parties Would Disrupt Marketing and Discriminates Against Offline Transfers. [PP. 14-15, Sec. 3(b); PP. 17-18, Sec. 3(e)]**

With limited exceptions, the bill would require opt-in consent for the transfer of personal data to third parties. We are concerned that this requirement would disrupt widespread and legitimate business practices, particularly in the offline arena. It is a longstanding DMA principle to provide an opt-out choice for data practices. Indeed, the draft bill seems to recognize the value of an opt-out regime for first party collection and use. Current law and industry practices also do not require first parties to obtain express affirmative consent for the transfer of data to third parties for marketing purposes. The draft bill would therefore fundamentally change the prevailing framework for the transfer of data to most third parties by requiring entities to obtain express affirmative consent.

To be clear, the bill would have a profound effect on all of the societal benefits of direct marketing. It is not an overstatement to say that the "opt-in" for transfers to third parties would significantly undercut direct marketing. We envision that the cost of products will go up for consumers, and that they will have less access to relevant information at a time when they need it.

The draft bill builds in some flexibility for online transfers by including an exception to the opt-in regime for information that is transferred online to third-party advertising networks. However, there is no comparable provision for offline data transfers. By omitting offline data transfers, the exception creates a discriminatory regime in which offline data transfers are subject to a stricter consent requirement than online data transfers. Thus, for example, bill would require opt-in consent for data collected online to be shared with offline cataloguers and publishers for marketing purposes. The DMA is concerned about the bill's effort to hold offline data transfers to such a standard, which is more restrictive than the standard for online transfers. We believe that this approach is at odds the stated goal of the bill to protect commerce, and we are not aware of any new privacy concerns regarding offline data transfers that would justify such a restrictive requirement, which is far beyond industry best practices or standards.

In general, offline marketing uses of data, such as direct mailing, constitute longstanding business practices that are already subject to adequate regulation, including industry self-regulation, and with which consumers are familiar and comfortable. Indeed, consumers value the opportunity to shop from a catalogue, and this opportunity is critical for consumers with limited mobility such as elderly or disabled consumers, and consumers who live in rural areas. The opt-in requirements set forth in the draft bill could effectively eliminate such offerings. Even those companies that do not themselves transfer data to third parties will suffer from diminished access to data under the regime that the draft bill would impose. Such data from third party providers is used by a widespread group of leading retailers and marketers. We, therefore, respectfully urge you to consider adding a comparable exception to the opt-in consent requirement for the transfer of data offline that allows for continuation of the opt-out model. DMAchoice,<sup>[5]</sup> a consumer mail preference tool created by the DMA, is an example of the type of consumer

preference tool that may obviate any opt-in consent requirement for offline data transfers.

**3. Imposing Opt-Out Consent Requirements on the Collection of Data by First Parties Is Highly Disruptive and Will Restrict Offerings to Consumers. [PP. 8-14, Sec. 3(a)]**

The bill would impose new standards for first party data collection practices by requiring first-party covered entities to provide an opt-out. This is not currently a business best practice and the DMA is concerned that such a requirement will interfere with the business-customer relationship. This proposal would mark a sea change from existing practices and law, which have long recognized that consumers expect first parties to collect at least some information from them to provide them with products and services. It will require that hundreds of millions of dollars be committed to redesign complex information systems with no comparable policy benefits. The FTC stated the issue clearly when it noted that “given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it.”<sup>[6]</sup> Thus, transparency has always been the key to first-party uses and industry remains committed to this principle as the foundation of consumer protection in this area.

If you pursue such an opt-out consent requirement, we recommend clarifying the draft bill to provide better guidance to business regarding what practices trigger a requirement to provide consumer choice. It appears that, if enacted, this draft legislation would not require consumer consent for data practices for a “transactional” or “operational” purpose, but would require businesses to obtain opt-out consent for data practices for “marketing, advertising, or sales” purposes. However, the draft bill does not provide further information on what purposes or activities would fall within this general category of “marketing, advertising, or sales”. It is important to recognize that businesses often undertake data-related activities for multiple purposes including marketing. For example, data analysis in order to optimize or improve products and services is defined in the legislation as an “operational purpose” but also serves the goal of increasing eventual sales. Moreover, applying an expansive definition of marketing, advertising, and sales purposes is likely to result in excessive consent requests that are likely to confuse or frustrate consumers. We ask that you consider providing additional explanation and guidance in order to clarify this critical term and the new obligations that you seek to impose on businesses.

We also strongly recommend that you consider an exemption for marketing, which is truly the most benign reason to collect and use consumer information, and a principal economic driver. In 2009, direct marketing accounted for 8.3% of total U.S. gross domestic product and directly employed 1.4 million Americans. The collective sales efforts of these employees supported an additional 8.4 million jobs, for a total of 9.9 American jobs. Considering past controversial uses of personal information by law enforcement and other agencies, we question whether it is appropriate to grant exemptions to the government and for other business uses while singling out marketing for more restrictive treatment. The DMA strongly believes that marketing data should only be used for marketing purposes.

Finally, we suggest that the draft bill could be clarified to better define the requirement that a covered entity may not “use” information previously collected if an

individual subsequently declines consent for use. Even if an individual wishes to opt out of some uses of collected information, other uses may be necessary to business operations, including to complete or bill for a transaction previously requested by a consumer.

**4. The Scope of “Covered Information” Is Too Broad and Includes Information That Does Not Inherently Personally Identify an Individual. [PP. 3-4, Sec. 2(5)(G)-(H)]**

“Covered information,” as defined by the draft bill, would apply to a much broader set of information than that which is typically included as personally identifiable information within the scope of U.S. privacy laws. Including information such as unique persistent identifiers and preference profiles within the definition of “covered information” goes beyond traditional privacy regimes and the DMA is concerned that this expansion would have fundamental and negative impacts on consumers and business offerings. We firmly believe that information that constitutes “covered information” should only include information that actually identifies a specific person. Information should not be considered personal simply because it may link back to a particular *computer*, which may be used by multiple individuals. Rather, we respectfully recommend that the definition of “covered information” should apply only to data when it *is* linked back to an *individual*. The fact that certain information *can* be used to identify an individual does not mean that such information in practice *is* used for such purposes. We therefore suggest revisiting the definition of “covered information” so that it only captures information that personally identifies individuals.

**5. The Bill Imposes the Unnecessary Burden of Requiring Consent When Material Changes Are Made to Policies Governing the Prospective Collection of Information When Notice Alone Is Sufficient. [P. 13, Sec. 3(a)(4)(B)]**

The draft bill’s provision on notice and consent to material changes in privacy policies extend beyond existing law, which does not require entities to obtain express affirmative consent for information collected *prospectively* so long as sufficient notice is provided. See Sec.3(a)(4)(B). We do not believe that consumers are harmed by changes to company data practices if they are sufficiently notified of upcoming changes to the treatment of data that has yet to be collected. Thus, we question why a consent requirement should be imposed on covered entities when notice alone is sufficient to inform persons how their data will be treated going forward. Moreover, imposing this requirement could have the perverse effect of either discouraging entities from updating their information practices because obtaining consent from customers can be technologically challenging, or encouraging entities to collect and retain more data from consumers to avoid needing to provide them with notice of prospective changes to privacy policies.

**6. The Term “Sensitive Information” Includes Within Its Scope Information That Is Not Sensitive and Information That Should Not Be Subject to Opt-In Consent. [P. 6, Sec. 2(10); P. 16, Sec. 3(c)]**

We respectfully recommend that the definition of “sensitive information” be narrowed to cover only information that is truly sensitive. For years, marketers have

employed market segmentation (by using information that the bill includes under the proposed definition of “sensitive information”) to provide beneficial information to individuals in a manner that has not been shown to cause harm. We are concerned that imposing an opt-in regime on the use of such information would negatively impact the ability of marketers to provide such tailored offerings, which in turn would be a disservice to consumers who find value in such marketing techniques. We agree that some aspects of the areas delineated in the proposed definition of “sensitive information” should be subject to heightened standards. However, because this is a complicated area, we suggest that further studies be conducted before requiring such a drastic change to current practices.

Further, we submit that the definition of “sensitive information” is overly vague because it reaches any information that “relates to” certain facts regarding an individual. This definition could be read to include any information that might permit inferences about these facts, even if the information is not actually sensitive. For example, a language preference could indicate that an individual is a member of a specific ethnic group, but is not unequivocal and would not generally be considered sensitive information. We ask that you consider limiting the definition of sensitive information to data gathered directly from the individual rather than any information that “relates to” the enumerated items.

Finally, the DMA has concerns with the inclusion of “precise geolocation information” in the definition of “sensitive information.” Locational technology is currently an area of rapid innovation and advancements, which are likely to have beneficial applications, and we caution against the creation of new restrictions that are likely to stifle this vibrant technological growth and evolution. We therefore believe that this area would be better left to self-regulation at this time.

**7. Requiring Privacy Notices to Include 15 Prescribed Disclosures Runs Counter to the Purpose of a Privacy Policy. [PP. 9-12, Sec. 3(a)(2)(B)]**

Privacy policies are intended to provide consumers with a window into the information collection and use practices of an entity. As the FTC has recently noted at its Privacy Roundtable Series, however, critics suggest that privacy policies may not be the most effective means of providing transparency to consumers. Commission officials have expressed the view that many persons do not read privacy policies or do not understand the provisions included in them. Requiring such privacy notices to include fifteen prescribed disclosures, as this bill contemplates, is therefore at odds with the current debate on how best to provide consumers with transparency. Moreover, we are concerned that some of the disclosures contemplated by the bill will have negative consequences or may not be helpful to consumers. For example, offering disclosures about how a covered entity stores or disposes of information could assist identity thieves or other wrongdoers in compromising the covered entity’s security. Rather than prescribing lengthy disclosures, we support providing entities with flexibility in describing their data collection and use practices.

**8. Delivering Privacy Notices Before the Commencement of Information Collection Is Impractical If Not Impossible. [PP. 8-9, Sec. 3(a)]**

The draft bill envisions requiring covered entities to provide detailed prescribed privacy notices to persons *before* any online or offline collection of information may take

place. We are concerned that such a requirement would disrupt the free flow of information and would prove, in many situations, impossible to fulfill. In the online context, data collection begins from the moment a person types in a URL address. Covered information such as an Internet Protocol address must be collected from the device to know where to deliver the requested content. Even if a privacy notice could be delivered before a person is transferred to the requested site, an entity would need some information to know where to deliver the notice. Requiring a privacy notice to be provided before any online collection of information would thus be impossible.

We further believe that requirement would also be disruptive and challenging to implement in the offline world. While the bill includes exceptions to the notice requirement (e.g., for transactional or operational purposes), the exceptions would not extend to instances such as when information is collected for marketing purposes with third parties (a practice which many entities depend on for their business models). Moreover, the operational purpose exception explicitly carves out information collected for marketing and advertising purposes and the fraud provision embedded within the operational purposes carve out only applies to fraud directed against a covered entity, not to consumers.

If enacted, this new requirement would severely impact companies' ability to gather preference information for marketing purposes. We do not believe that marketing should be singled out for such restrictive treatment. On the contrary, marketing is one of the least risky information practices, fuels commerce and economic growth, and offers consumers access to products and services that they value. Among other negative consequences for commerce, the draft bill would effectively eliminate the ability of companies to gather marketing information through call centers that consumers reach to order products seen in a catalog or on television, because it would be impracticable for operators to provide a written privacy notice. In offline environments that involve a personal interaction, such as a shopping or hotel transaction, companies would face a need to make vast investments in new materials and infrastructure in order to comply with the requirements in the draft bill.

**9. The Proposed Definition of “Render Anonymous” Is Impractical. [P. 6, Sec. 2(9); P. 20, Sec. 5]**

We appreciate the bill's attempt to include an exemption for the use of aggregate or anonymous information. However, we are concerned that the term “render anonymous,” as currently defined, is too broad to serve as a meaningful exemption. As with the definition of “covered information,” we believe that the bill should only apply to information that *is* linked back to an *individual*. The bill's definition of “render anonymous” would apply to “a computer or device,” which essentially means that the provision of many useful services that do not harm consumers, such as market research and analytics, would not be carved out.

**10. Any New Requirements Should Apply to the Entity That Collects Data from a Consumer, Not to Recipients of Data Collected by Other Entities. [P. 3, Sec. 2(4)]**

The draft bill defines a “covered entity” as a “person engaged in interstate commerce that collects data containing covered information[.]” An entity that falls under this definition would be subject to the many restrictions and requirements in the

legislation. Thus, we suggest that you consider clarifying that a covered entity is one that originally collects covered information from an individual, and that the definition does not include a “downstream” entity that receives covered information from a data collector or another entity. For example, many companies obtain data from third party aggregators in order to combine it with information collected from customers. We believe that when obtaining such data, businesses should be able to rely on the practices of the company that originally collected the information, because it would be impracticable for the receiving company to reach out again to consumers to provide any notice or choice required.

**11. The Provisions of the Draft Bill Relating to Data Retention Are Not Workable. [P. 10, Sec. 3(a)(2)(B)(vii); P. 17, Sec. 3(e)(2)]**

The draft bill includes an “individual managed preference profiles” exemption from the general requirement of obtaining opt-in consent to disclose covered information to unaffiliated parties. The exemption would apply if covered entities meet certain requirements, including deleting or rendering anonymous any covered information not later than 18 months after the information is collected. While this time limit may be feasible in some instances, the DMA does not believe that it is workable as a rule for online data. For example, a company that has an ongoing relationship with a consumer would need to retain information about that consumer in order to conduct billing, service, and transactional operations. Similarly, we also believe that it would frequently be impracticable for covered entities to disclose how long information is retained, because retention periods may differ for various data types and uses or may depend on a consumer’s interactions with the covered entity.

\* \* \*

We thank you for the opportunity to provide comments on the bill. Should you have any further questions, please do not hesitate to contact Linda Woolley, Executive Vice President of Government Affairs, at 202-861-2444 or [lwoolley@the-dma.org](mailto:lwoolley@the-dma.org).

###

---

[1] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), available at <http://www.the-dma.org/privacy/Self%20Regulatory%20Principles%20for%20Online%20Behavioral%20Advertising%2007-01-09.pdf>.

[2] Direct Marketing Association, *Guidelines for Ethical Business Practice*, available at <http://www.dmaresponsibility.org/Guidelines/>.

[3] FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising, at 11 (February 2009) (*hereinafter* Staff Report), available at <http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

[4] *Id.*

[5] See <http://www.dmachoice.org>.

[6] Staff Report at 27.

[back to top](#)

