



**Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION,
U.S. DEPARTMENT OF COMMERCE
Washington, DC 20230**

**COMMENTS
of the
DIRECT MARKETING ASSOCIATION, INC.**

on the

**“Multistakeholder Process to Develop
Consumer Data Privacy Codes of Conduct”**

Docket No. 120214135-2135-01

April 2, 2012

Linda Woolley
Executive Vice President, Government Affairs
Gerald Cerasale
Senior Vice President, Government Affairs
Rachel Thomas
Vice President, Government Affairs
Direct Marketing Association, Inc.
1615 L Street, NW Suite 1100
Washington, DC 20036
(202) 861-2444

Counsel:
Stuart Ingis
Julia Kernochan Tama
Venable LLP
575 Seventh Street, NW
Washington, DC 20004
(202) 344-4613



I. Introduction

The Direct Marketing Association, Inc. (“DMA”) appreciates the opportunity to comment on the Administration’s proposed multistakeholder process for the development of codes of conduct in the area of consumer data privacy.¹ The DMA (www.the-dma.org) is the world’s largest global trade association of businesses and nonprofit organizations that use data and analytics to serve their current – and potential – consumers, customers, and donors with the most relevant messages and offers. DMA member organizations use and promote the full spectrum of marketing channels, including the Internet, email, mobile, mail, and telephone. Founded in 1917, the DMA includes more than half of the Fortune 100 companies and represents dozens of industries, including retail, hospitality, consumer products, finance, pharmaceuticals, entertainment, and publishing. The DMA advocates standards for responsible marketing and requires all of its members to adhere to strict ethical guidelines in their marketing practices.

The DMA appreciates the Administration’s recognition of the value of industry codes of conduct. For decades, as detailed below, the DMA has been at the forefront of developing robust and enforceable self-regulatory frameworks for consumer data privacy. Based on the success of these efforts, we are committed to self-regulation as the most effective and efficient means of addressing consumer privacy concerns in today’s broader information economy.

We believe that the proposed multi-stakeholder process should take into account the lessons learned by the DMA and other business community leaders from our experience in spearheading industry self-regulatory efforts over decades. These lessons can help the Administration to avoid known pitfalls that could stymie its efforts or result in stalemate. Specifically, based on our experience, we believe that the most effective way to develop codes of conduct is through private negotiations among industry. We believe that this is the most effective and fastest way to achieve “buy-in” from those who will have to actually implement and follow the agreed-upon guideline or standard of behavior. We are concerned, therefore, that the process contemplated by the Administration will face challenges. Despite this concern, we are committed to participating fully in the government-convened multistakeholder process.

To give the multistakeholder process the best opportunity to succeed, we suggest that the following core principles should apply:

- The Administration should identify and avoid duplicating areas where self-regulatory codes already exist or are nearing completion, since it is unnecessary to “reinvent the wheel.”

¹ National Telecommunications and Information Administration, Request for Public Comments on “Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct,” 77 Fed. Reg. 13098 (March 5, 2012) (hereinafter “Request for Comments”).

- The process should seek to include all companies that are representative of those working in a particular “ecosystem.”
- The process convened by government should not impede or displace private negotiations among industry stakeholders.
- The Administration should adhere to its commitment that the government will not substitute its own judgment when codes of conduct are developed.²

II. DMA’s History of Leadership in Industry Self-Regulation

a. DMA Self-Regulatory Standards and Consumer Tools

For decades, the DMA has been a leader in the development and enforcement of industry self-regulation in privacy and other areas. The DMA and its members have developed standards for online data practices and many other business activities as part of our comprehensive and longstanding *DMA Guidelines for Ethical Business Practice* (“Guidelines”).³ The Guidelines provide DMA member companies with a comprehensive blueprint for ethical marketing practices. The Guidelines are supplemented by extensive commentary and additional compliance guidance for companies.⁴ The DMA requires all member companies to adhere to the Guidelines and actively reviews and enforces compliance. In addition, companies that represent to the public that they are DMA members but fail to comply with the Guidelines may be subject to actions for violating state and Federal consumer protection laws.

The DMA has a lengthy history of effectively enforcing the Guidelines. To date, the DMA Guidelines have been applied to hundreds of direct marketing cases to review complaints about marketing practices and other ethics issues. In order to inform the public and educate marketing professionals on acceptable marketing practices, a case report is regularly issued which summarizes questioned direct marketing promotions and explains how cases were administered.⁵ The report also is used to educate regulators and others interested in consumer protection issues about DMA Guidelines and how they are implemented.

For example, between February 2010 and November 2011, the DMA’s Corporate and Social Responsibility department processed over 15,000 consumer and company complaints

² The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 27 (February 2012) (hereinafter “White House Framework”).

³ The DMA Guidelines for Ethical Business Practice are available at <http://www.dmaresponsibility.org/Guidelines/> (hereinafter “Guidelines”).

⁴ DMA, “Do the Right Thing: A Companion to DMA’s Guidelines for Ethical Business Practice,” available at <http://www.dmaresponsibility.org/DoTheRightThing/>.

⁵ The DMA 2011 Annual Ethics Compliance Report is available online at http://www.the-dma.org/guidelines/ETHICS_COMPLIANCE_REPORT_2011.pdf.



regarding marketing practices. While only a small percentage of such complaints rise to a level requiring that a formal case be opened, the Ethics Operating Committee met 11 times and reviewed 64 cases based on marketing offers during this period. The cases examined marketing practices that raised concerns under numerous Guidelines, including those on the honesty and clarity of offers (Article #1), clarity of representations (Article #3), solicitations that appear to be from government agencies (Article #10), advance consent marketing (Article #12), and consumer efforts to be removed from mailing lists (Article #31). The DMA also investigated and referred to regulatory agencies several phishing schemes.

The DMA works with both member and non-member companies to promote voluntary cooperation in adhering to the Guidelines and good business practices for direct marketers. The DMA receives matters for review in a number of ways: from consumers, member companies, non-members, or, sometimes, consumer protection agencies. Complaints referred to the Ethics Operating Committee are reviewed against the Guidelines for Ethical Business Practice as well as applicable laws. If the Committee believes there is a potential violation, the company is contacted and advised to come into full compliance. Most companies work voluntarily with the Committee to cease or change the questioned practice.

If a member company does not cooperate and the Committee believes there are ongoing ethical violations, the Committee can recommend that action be taken by the DMA Board of Directors and can make case results public. Board action could include censure, suspension or expulsion from membership, and the Board may also make its actions public. If a non-member or a member company does not cooperate with the Committee and the Committee believes violations of law may also have occurred, the case is generally referred to federal and/or state law enforcement authorities for their review. Based on compliance cases and other developments, the DMA reviews and updates the Guidelines as needed in response to new laws, technologies, and business practices.

The DMA has continuously evaluated and updated the Guidelines over their 40-year history to take account of new technologies and issues. For example, we added a guideline to address “spyware” and “adware” after policymakers and consumer advocates raised concerns about the proliferation of unwanted software downloads. Many of the current Guidelines address privacy issues. Among other provisions, the Guidelines state that companies should:

- Not display, disclose, rent, sell or exchange data and selection criteria that may reasonably be considered sensitive or intimate, where there is a reasonable consumer expectation that the information will be kept confidential;⁶
- Use marketing data only for marketing purposes;⁷

⁶ Guidelines, Article 32.

⁷ *Id.*

- Not transfer personally identifiable health-related data gained in a medical treatment context for marketing purposes without the specific prior consent of the consumers;⁸
- Treat personally identifiable health-related information volunteered by or inferred about consumers outside a treatment context as sensitive and personal information, and provide clear notice and the opportunity to opt out and take the information's sensitivity into account in making any solicitations;⁹
- Not rent, sell, exchange, transfer, or use marketing lists in violation of the Guidelines;¹⁰
- Provide notice of online information practices, including marketing practices, in a way that is prominent and easy to find, read, and understand, and that allows visitors to comprehend the scope of the notice and how they can exercise their choices regarding use of information;¹¹
- Identify and provide contact information for the entity responsible for a website;¹²
- Comply with self-regulatory principles for online behavioral advertising, discussed below;¹³
- Assume certain responsibilities to provide secure transactions for consumers and to protect databases containing consumers' personally identifiable information against unauthorized access, alteration, or dissemination of data;¹⁴
- Restrict data collection and marketing for children online or via wireless devices, consistent with the Children's Online Privacy Protection Rule;¹⁵
- Follow detailed guidelines related to social media and online referral marketing, including providing disclosures to both the referring individual and the referred person when a marketer receives personally identifiable information from social media channels or an online referral;¹⁶ and

⁸ Guidelines, Article 33.

⁹ *Id.*

¹⁰ Guidelines, Article 35.

¹¹ Guidelines, Article 38.

¹² *Id.*

¹³ *Id.*

¹⁴ Guidelines, Article 37.

¹⁵ Guidelines, Article 16.

¹⁶ Guidelines, Article 43.

- Follow specific rules for data compilers, including suppressing a consumer’s information from their databases upon request, explaining the nature and types of their sources to consumers upon request, reviewing customer companies’ use of data and requiring customers to state the purpose of their data use, and reviewing promotional materials used in connection with sensitive marketing data.¹⁷

While the DMA Guidelines apply to all member companies, the DMA has also developed self-regulatory guidance for specific industry sectors and channels. To highlight a few examples, the DMA has issued formal Online Information Guidelines and Commercial Solicitation Online Guidelines¹⁸ and the DMA’s Internet Marketing Advisory Board has put forward “Best Practices for Online Advertising Networks and Affiliate Marketing.”¹⁹

Building on our work in developing standards for company conduct, the DMA has taken an active role in helping companies put these standards into action. For example, the DMA provides online tools to assist companies in creating privacy policies to explain their practices to consumers. In addition to a general tool, we offer specialized privacy policy generators for operators covered by the Children’s Online Privacy Protection Act and financial institutions covered by the Gramm-Leach-Bliley Act. We also provide access to data security assessment and compliance resources. These tools are available at <http://www.dmaresponsibility.org/>.

To serve consumers, the DMA has also established an online mechanism, www.dmachoice.org, for consumers to set individualized preferences about what marketing communications they wish to receive. This tool is an easy, centralized, effective way for consumers to make meaningful choices about marketing uses of their personal information. These are just a few examples of the DMA’s history of proactive engagement to improve privacy protections for consumers.

b. Self-Regulation of Online Data Practices

The DMA, along with other leading trade associations and companies, has spearheaded the development of comprehensive self-regulation for online data practices. Now administered by the Digital Advertising Alliance (“DAA”), this program was recently recognized by the Administration as an example of effective codes of conduct for consumer privacy. The rapid and widespread deployment of the DAA program illustrates the key benefits of self-regulation:

¹⁷ Guidelines, Article 36.

¹⁸ DMA’s “Online Marketing Guidelines and Do the Right Thing Commentary,” available at <http://www.the-dma.org/guidelines/onlineguidelines.shtml>.

¹⁹ DMA’s “Best Practices for Online Advertising Networks and Affiliate Marketing,” available at <http://www.dmaresponsibility.org/OnlineAdvertisingFAQ/>.



flexibility, speed, and decentralization.²⁰ The DMA believes that these qualities make industry self-regulation the ideal strategy for tackling privacy challenges in the rapidly evolving consumer data ecosystem.

The DAA's self-regulatory framework was developed, and continues to evolve, through extensive dialogue with policymakers. The *Self-Regulatory Principles for Online Behavioral Advertising* ("OBA Principles") were published in 2009,²¹ following the blueprint set forth by the Federal Trade Commission ("FTC") in its staff report calling for industry to develop self-regulation directed at online data collection for targeted advertising purposes. In November 2011, this framework was enhanced and extended with the release of the *Self-Regulatory Principles for Multi-Site Data* ("MSD Principles"), which apply to data collected from a particular computer or device regarding Web viewing over time and across non-Affiliate Web sites. Building on these Principles, the DAA is now working to extend self-regulation to the mobile ecosystem, including mobile Web, app, and location data. This effort is ongoing and has made substantial progress to date.

Implementation of the DAA's Self-Regulatory Program centers on the Advertising Option Icon, an easily recognizable symbol that provides consumers with transparency and control with respect to online data collection. The Icon is used across participating companies and is delivered in over 900 billion ad impressions each month. By clicking on the Icon, consumers can link to a clear disclosure statement regarding the company's online data collection and use practices as well as an easy-to-use opt-out mechanism. The AboutAds Consumer Opt-Out Page provides a uniform mechanism for consumers to easily opt out of having data collected and used (see www.aboutads.info/choices). Consumers can make granular choices with respect to specific companies or can select a single option to opt out with regard to all participating companies.

On average, there are over 76,000 new visitors to the AboutAds Web site each week, with 90 percent of these reaching the site by clicking on the Advertising Option Icon. In December 2011, the DAA began to offer persistency tools that enable consumers to make their choices on the AboutAds Web site durable in the Google Chrome, Microsoft Internet Explorer, and Mozilla Firefox browsers.

Adherence to the DAA Program is enforced by the DMA and by the Council of Better Business Bureaus ("CBBB"). Consumers have already utilized these programs to submit compliance concerns for evaluation. In November 2011, the CBBB announced its first

²⁰ White House Framework at 23-24.

²¹ 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/government/ven-principles%2007-01-09%20FINAL.pdf>.



enforcement actions under the Self-Regulatory Principles for Online Behavioral Advertising. While DMA has received complaints, none thus far have required escalation to case status in order to reach resolution.

With the program in wide implementation, the business community is currently funding a major consumer education campaign (www.youradchoices.com) to inform consumers about their choices and to promote awareness of the Icon. This campaign, designed by McCann Erickson Worldwide, features display advertising that links to a new informational website with short videos about how interest-based advertising works and how consumers can exercise control over online data collection. The DAA has secured hundreds of millions of dollars' worth of donated ad inventory space to present this campaign to Web users.

III. Lessons Learned from Effective Self-Regulation

The DMA offers several observations based on our decades of experience in developing and implementing successful self-regulatory programs. The DMA believes that the Administration's proposed process will have the best opportunity to be effective if it draws on lessons learned from industry's prior experience. Specifically, we submit that the Administration should adhere to several core principles, discussed in turn below.

- **The Administration should not undertake to set standards in areas where self-regulatory codes already exist.**

NTIA has asked what factors should be considered in selecting issues for the code development process.²² The DMA recommends that prior to convening a process to develop any new code of conduct, NTIA should evaluate existing industry codes of conduct that address consumer data privacy and areas where industry has made substantial progress toward self-regulation. Such codes represent areas where the business community has already developed consensus and is addressing privacy concerns. The Administration should not convene processes to discuss these areas, which would unnecessarily consume resources and could create confusion for businesses and consumers. However, the process can look to existing codes of conduct as models for what the process is striving to achieve in other areas.

The DMA's Guidelines and other self-regulatory standards discussed above and the DAA's Self-Regulatory Program (including the mobile aspects of the Program that are currently under development) are examples, among others, of areas that should not be revisited by the Administration. As we have described, these programs are robust, widely implemented, and actively enforced.

²² Request for Comments, 77 Fed. Reg. 13,098, 13,100 (Question 2).



- **The process should seek to include all companies that are representative of those working in a particular “ecosystem.”**

The DMA Guidelines reflect the participation of DMA member companies from across the marketing and advertising industries. When the DMA and its partner associations convened the group that developed and adopted the OBA Principles, we were careful to ensure that there was at least one company representing each category of “players” that functions in that marketplace. Similarly, we sought the participation of representative industry participants when developing the MSD Principles and in our current mobile initiative. We would encourage the government to do the same in convening its multistakeholder process. Broad participation by industry representatives is important to lend legitimacy to the deliberations, to provide technical expertise, and to assure that resulting codes are workable and will preserve companies’ ability to innovate.

- **The process should be advanced largely through private negotiations.**

The Administration’s framework presumes that all involved stakeholders will participate in an open, transparent process to develop codes. NTIA specifically has requested comment on possible procedures for stakeholders to explain their decisions reached in the code development process or in concert with other stakeholders.²³

As the Administration recognizes, processes to create industry codes of conduct are different from agency rulemakings.²⁴ The level of transparency need not be the same level that is required in rulemakings. Rather, the process of developing codes of conduct is more akin to legislating, which requires policymakers with diverse interests to balance concerns and reach consensus when no action is legally required. Such delicate and voluntary negotiations are often best advanced through informal private discussion.

The DMA’s experience confirms that open meetings are not the best way for companies to reach consensus on difficult issues. Businesses operate in highly competitive marketplaces, and are also closely scrutinized by the media, consumer advocates, and policymakers. In this environment, businesses are unlikely to engage in open discussion of practices that may involve proprietary information or trade secrets. Consumer groups, in particular, have a history of using information about business practices to file complaints with federal agencies and bring class action suits against companies. Even when such claims are meritless, companies are understandably wary of discussing their practices in a manner that could expose them to risk, harm their shareholders, or affect their competitive positions.

²³ *Id.* (Questions 11-12).

²⁴ White House Framework at 24.



For these reasons, we encourage the Administration to ensure that the multistakeholder process does not discourage or preclude private discussions among industry representatives. We believe that such private discussions can play a productive role in the multistakeholder process, allowing industry to efficiently explore issues and build consensus in order to expedite and streamline the broader process. The Administration should include that proven, constructive process in any multistakeholder endeavor.

- **The Administration should adhere to its commitment that the government will not substitute its own judgment when codes of conduct are developed.**²⁵

The Administration has recognized that participants, not the government, should control the progress and results of any code development process.²⁶ This is appropriate given that “codes will not bind any companies unless they choose to adopt them.”²⁷ Businesses are the primary category of stakeholders that would be subject to the codes. Moreover, the business community is uniquely capable of identifying principles that are workable and that appropriately balance consumers’ privacy interests with consumers’ ability to access exciting services and products.

The Administration has already set forth its general views on consumer data privacy in its recent report. The DMA agrees with the Administration that the government’s role should be limited to facilitating the process and believes that the government should avoid taking positions on substantive issues or disagreements that may arise in the process.

* * *

The DMA appreciates this opportunity to provide our comments on the proposed process to develop industry codes of conduct. Based on our experience in leading the development and implementation of successful self-regulatory frameworks, we believe that the principles outlined above would support the Administration’s efforts toward codes of conduct that can attract voluntary industry participation. We look forward to participating in the multistakeholder process and continuing to work with the Administration to address consumer data privacy issues while preserving the Internet as an engine of innovation and economic growth.

²⁵ *Id.* at 27.

²⁶ *Id.* at 24.

²⁷ *Id.*