Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

COMMENTS
of the
DIRECT MARKETING ASSOCIATION, INC.

Responding to the Privacy Roundtables – Project No. P095416

April 14, 2010

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

Counsel:
Stuart Ingis
Emilio Cividanes
Julia Kernochan Tama
Venable LLP
1575 Seventh Street, NW
Washington, DC 20004
(202) 344-4613

Direct Marketing Association, Inc.

Privacy Roundtables – Comment, Project No. P095416

The Direct Marketing Association ("DMA") appreciates the opportunity to submit these Comments on the Federal Trade Commission's ("FTC" or "Commission") proceedings in its roundtable series entitled "Exploring Privacy."

The DMA (www.the-dma.org) is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. The 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, the 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 cataloguers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them.

In the first section of these Comments, the DMA presents its general observations. We review the Commission's roundtable series against the backdrop of current privacy regulation, discuss our view that the Commission's existing approach to privacy regulation has effectively fostered innovation and preserved consumer choice, identify areas for further policy development, and explain why we believe industry self-regulation is the best approach to refining and enforcing privacy protections in the marketing arena. In the second section of these Comments, the DMA responds to each of the specific questions posed by the Commission in its requests for public input.

SECTION ONE: COMMENTS

I. The Commission's "Exploring Privacy" Roundtable Series

Over the past several months, the Commission has convened a series of roundtable discussions with the goal of "determin[ing] how best to protect consumer privacy while supporting beneficial uses of [consumer] information and technological innovation."[1] The roundtables have addressed a broad range of topics related to privacy and technology. DMA understands that the Commission plans to build on these roundtable discussions to issue a report on privacy issues this summer.[2]

---

[1] Federal Trade Commission, "Exploring Privacy: A Roundtable Series," *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/.

[2] Stephanie Clifford, "F.T.C.: Has Internet Gone Beyond Privacy Policies?" *New York Times Media Decoder Blog*, http://mediadecoder.blogs.nytimes.com/2010/01/11/ftc-has-internet-gone-beyond-privacy-policies/.

A. Background

More than a century of law, as well as more than a decade of FTC workshops, enforcement actions, rulemakings, and other agency activities, preceded the roundtables. A review of the privacy statutes and regulations in the United States and abroad reveal common core principles. These are the fair information practices, designed to ensure that consumers can exercise meaningful control over their private information.

As summarized by the Commission, the five principles are:

1. Notice/awareness,
2. Choice/consent,
3. Access/participation,
4. Integrity/security, and
5. Enforcement/redress.[3]

Over the decades, the fair information practices have been proven to be a flexible and adaptable framework that preserves consumer choice while promoting innovation and economic growth.

The Commission's privacy regulation has generally advanced these core practices in a fashion that allows beneficial uses of information to continue. In enforcing these principles, the Commission has long focused on practices that pose a demonstrable harm to consumers, such as physical harms, economic injuries, or unwarranted intrusions such as spam and spyware.[4] This is consistent with the approach that the United States, often represented by the FTC, has taken in the development of the Information Privacy Principles of the Asia-Pacific Economic Cooperation ("APEC") economies. The "Preventing Harm Principle" is the first principle of the APEC Privacy Framework.[5]

Congress has likewise been cautious in regulating privacy issues. Federal privacy statutes that apply to businesses typically address particular areas of concern, such as children's online privacy, or specific sectors perceived as handling sensitive information, such as the financial industry or health care entities. There are compelling policy reasons for this reluctance to regulate business privacy practices more broadly. It would not be feasible or prudent to impose a "one size fits all" set of standards across the economy, given the wide variation in different industries' information collection and uses. In addition, sweeping legislation is not necessary given that self-regulation and other existing tools continue to be effective in preserving the fair information principles.

---

[3] Federal Trade Commission, "Fair Information Practice Principles," in *Privacy Online: A Report to Congress* (June 1998), *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited March 9, 2010).
[4] David Vladeck, Remarks on "The Role of the FTC in Consumer Privacy Protection" before the International Association of Privacy Professionals, Washington, DC (December 8, 2009).
[5] APEC Secretariat, *APEC Privacy Framework* 11 (2005).

These patterns in privacy regulation also reflect the fact that the United States has traditionally placed a high value on the free flow of information, because access to information has been viewed as a bulwark against tyranny. This value is most prominently enshrined in the First Amendment to the federal Constitution, which safeguards freedom of speech and freedom of the press.[6] The First Amendment's freedoms have been vigorously extended to commercial speech. In keeping with this societal value, privacy frameworks have recognized that consumers largely benefit from the free flow of information, and have treated privacy as one of a few exceptions to the general preference for information access.

This is the backdrop against which the roundtables were conducted.

B. The Three Roundtables

The first roundtable, held on December 7, 2009, in Washington, DC, consisted of five panels focusing on: (1) the risks and benefits of information-sharing practices, (2) consumer expectations regarding such practices, (3) behavioral advertising, (4) information brokers, and (5) the adequacy of existing legal and self-regulatory frameworks.

The second roundtable was held on January 28, 2010, in Berkeley, CA. This event featured two panels on the topic of technology and privacy, as well as panels that explored the privacy implications of three emerging technologies: mobile computing, cloud computing, and social networking.

The third and final roundtable, held on March 17, 2010, in Washington, DC, included a panel on privacy and Internet architecture and panels on health and other sensitive consumer information. The series closed with a panel discussing lessons from the roundtable series and possible paths forward.

II. The Commission's Existing Approach to Privacy Regulation Has Effectively Fostered Innovation and Preserved Consumer Choice

The DMA welcomes the Commission's effort to evaluate the current state of consumer privacy and whether there is a need for further policy development. Since the advent of the Internet, the Commission has focused its regulatory efforts on addressing identifiable consumer harms through the fair information practices, while otherwise preserving the ability of industry to grow and innovate. The DMA submits that this longstanding approach strikes the appropriate balance between protecting privacy and promoting technological innovation. Companies have been able to develop new online

[6] U.S. Const. amend. I. Similarly, the Freedom of Information Act ("FOIA"), signed into law in 1966, codifies the national preference for government openness. 5 U.S.C. § 552. Although FOIA contains a privacy exception to the release of information, it is narrow, exempting only "personnel and medical files and similar files the disclosure of which would constitute a *clearly unwarranted* invasion of personal privacy[.]" 5 U.S.C. § 552(b)(6) (emphasis added).

services, tools, and content that benefit consumers greatly. At the same time, the Commission can wield enforcement tools to restrict and punish harmful practices. The Commission should retain this general approach given its demonstrated effectiveness, as detailed in this section of our Comments.

Speakers during the roundtable series have suggested certain areas where additional policy refinements may be helpful. Several of these areas are highlighted in the next section. To the extent that such refinements are necessary, the DMA submits that any policy development can best be accomplished through industry self-regulation in dialogue with the Commission.

A. The Commission's Current Approach Benefits Consumers and Industry

Like the Commission, the DMA recognizes that technology is changing, and the world is changing with it. The Internet is no longer a distinct industry, but penetrates every area of Americans' business and private lives. Our member companies grapple each day with the business and ethical consequences of this expansion and the attendant technological innovation. However, the DMA does not believe that this rapid pace of change heralds a need for new regulation. On the contrary, today's vibrant Internet ecosystem results from, and demonstrates the need to retain, the Commission's existing approach.

The United States was the birthplace of the Internet and remains the global leader in online technological innovation. As the Internet became available to consumers in the late 1990s, the Commission, other regulatory bodies, and Congress assessed the need to regulate the new medium. This consideration weighed the harms and benefits of information use. The result was a broad consensus in favor of avoiding heavy-handed regulation in order to foster technological innovation and economic growth.

The rise of the Internet has led to an explosion of innovation that has transformed every aspect of our lives, generating advances ranging from more efficient business communications to unprecedented forms of digital entertainment. American consumers are avid users of the Internet, and are quickly embracing emerging technologies like cloud computing, mobile computing, and social networking. Throughout this development boom, the fair information practices have provided flexible safeguards for consumers, while the Commission retains strong enforcement tools that can be deployed in response to practices that harm consumers. Today, it is evident that the Commission's existing approach to privacy regulation strikes an appropriate balance that benefits consumers and industry alike.

Advertising has provided critical support for the Internet's explosive development. Consumers have come to expect rich content and free services online. The wide availability of these benefits is subsidized by online advertising revenues. Market innovators also rely on advertising revenues to create and implement new products and services. Online advertising can be targeted based on context (the content of a website or

webpage) or on the browsing history associated with a particular computer. Conducted responsibly, this type of collaboration does not jeopardize consumer privacy. It relies largely on anonymous data that is not linked back to a named individual, much of which may be discarded after a single online session. Although not all online advertising is targeted, the ability to make advertising more relevant to consumers' likely needs and interests is a benefit to consumers, and also allows advertising efficiently to subsidize other activities.

While alarmists may claim that privacy concerns affect online usage, this argument is discredited by American consumers' evident enthusiasm for Internet technologies and the resultant growth in online economic activity. Consumers' embrace of e-commerce shows that they widely value the convenience, customization, and features that companies can offer online. Indeed, e-commerce has continued to thrive despite the current economic downturn. For example, on "Black Friday" in 2009, the day after Thanksgiving and traditionally a strong day for holiday shoppers, sales in retail locations were only 0.5% higher than in 2008,[7] while online retail sales showed an 11% improvement.[8] During the 2009 holiday season, despite high joblessness and a weak economy, e-commerce sales amounted to $27 billion, a five percent increase over 2008.[9] This spending buoyed holiday sales despite analysts' initially bleak predictions.[10]

The DMA cautions the Commission to avoid significant new regulation that could disrupt this beneficial cycle. Unnecessary restrictions on online advertising could reduce the relevance of commercial messages to consumers. Moreover, if online advertising becomes less effective, it will impede companies' ability to provide ad-supported content and services to the public. This could hinder innovation or drive businesses to shift from offering free content and services to demanding direct payments from consumers. The Commission should retain its existing approach of encouraging companies to provide consumers with notice of information practices and the ability to opt out of unwanted practices.

The DMA also believes that the Commission's current approach of promoting the fair information practices through harm-based enforcement respects the individualized nature of privacy preferences. The rise of social networking, cloud computing and mobile computing, among other technologies, has illustrated the fact that consumers have very different preferences about what information is private and what constitutes a sufficient reason to share information. The Commission's harm-based approach

---

[7] Janet Morrissey, "After Black Friday, Doubts Grow About a Shopping Uptick," TIME.com (November 30, 2009).
[8] comScore Press Release, "Black Friday Boasts $595 Million in U.S. Online Holiday Spending, Up 11 Percent Versus Year Ago" (November 29, 2009).
[9] comScore Press Release, "E-Commerce Sales Rise by 5 Percent to Reach $27 Billion for the 2009 Holiday Shopping Season through Christmas Eve" (December 30, 2009).
[10] Linda Sandler, "Holiday Retail Sales Rose an Estimated 3.6%, SpendingPulse Says," Bloomberg (December 28, 2009), *available at* http://www.businessweek.com/news/2009-12-28/holiday-retail-sales-rose-an-estimated-3-6-spendingpulse-says.html?chan=innovation_branding_marketing.

recognizes that tangible harm to consumers is the most meaningful and objective yardstick to determine whether regulation or enforcement is needed. It preserves consumers' individual choice and freedom unless an identifiable harm may ensue.

Finally, the DMA cautions that, given the penetration of the Internet into all areas of business, regulation of the online ecosystem amounts to regulation across industries. Any significant new regulation would likely have economic "ripple effects" that are difficult to predict. This type of instability is to be avoided at any time, but especially when the economy is fragile. The existing approach to privacy regulation has defended the fair information practices while fostering innovation. The DMA urges the Commission to adhere to its existing approach, which has proven effective, rather than adopting today's regulatory fashions at the expense of tomorrow's technological revolutions.

B. Opt-in Consent Is Not the Solution

The DMA understands that Chairman Jon Leibowitz has expressed a "sense … that [the Commission] might head toward opt-in" consent in lieu of the prevailing method of opt-out consent. Even if applied narrowly, the DMA strongly believes that a new opt-in requirement would be both unwarranted and unwise.

Although the Commission has promoted the importance of consumer notice and choice, "choice" has been construed in most contexts to require allowing consumers an opportunity to opt out of unwanted practices. This approach allows beneficial data flows to proceed unless an individual expresses a contrary preference. The DMA is concerned that opt-in consent, even on a limited scale, would drastically alter the online experience as we know it. Given the collaborative architecture of the Internet, data-sharing interactions between website owners and other companies are commonly required for the orderly functioning of a website. These interactions are currently seamless, and facilitate website features and efficiencies that consumers value. A requirement for opt-in consent will disrupt this architecture. The constant appearances of notice boxes will annoy and frustrate consumers, and will dilute the impact of such mechanisms.

To the extent that the Commission's interest in opt-in consent is related to a concern about the sufficiency of disclosures about data practices to enable consumers to make more informed decisions, the DMA submits that such a concern would be better addressed by focusing on methods to improve the provision of notice. Opt-in consent is an inappropriate response because it creates a presumption against the free flow of data. Yet there is no indication that most data flows harm consumers or should be discouraged. In particular, the Commission has not pointed to evidence of any concrete harm to consumers from the legitimate data practices that support online advertising. The Commission also has not produced evidence of either a societal consensus against such data sharing or consumers' willingness to accept a changed Internet experience in exchange for reducing such sharing. Moreover, the Commission's extensive roundtable

series has yielded little discussion and no consensus on opt-in consent that could justify a move in this policy direction.

The DMA believes that a drastic shift in policy toward opt-in consent should be based on something more than guesswork. Opt-in consent is often promoted as a panacea for online privacy concerns, but no illness has yet been identified. Without widespread consumer support, a shift to opt-in consent would be no more than a paternalistic effort to impose on consumers the Commission's view of what is best for them.

III. Areas Proposed for Policy Development

As discussed above, the DMA believes that the Commission's existing privacy framework largely strikes an appropriate balance between consumer privacy risks, on the one hand, and the many benefits of innovation and beneficial data use, on the other. Nevertheless, the DMA recognizes that commenters at the roundtable series and elsewhere have proposed ways to refine the existing notice and choice framework on a case-by-case basis when necessary to address new practices or technologies.

Three of the areas of proposed policy development that were discussed most extensively during the roundtables were: (1) the need in some circumstances for additional means of informing consumers regarding data collection and use practices, (2) the blurring in some circumstances of the distinction between personally identifiable information ("PII") and non-PII, and (3) the promotion of "privacy by design." The DMA believes that any further policy development in these proposed areas can best be accomplished through industry self-regulation in dialogue with the Commission, for reasons discussed further in the next section.

A. Notice and Transparency

Commission officials have recently criticized website policies as tending to be overly lengthy or complex.[11] The DMA believes that the Commission's concerns about privacy policies do not justify a wholesale abandonment of the notice and choice model. The reality is that privacy policies tend to be complex because online data practices are complex. Such practices defy easy explanation, especially when most consumers lack even a basic understanding of how the Internet functions. The Commission should also recognize that company privacy policies are shaped, in part, by efforts to respond to past enforcement actions by the Commission, which has repeatedly used its Section 5 authority in past years to pursue enforcement actions based on misstatements in privacy policies.[12] It is not surprising that companies now seek to avoid such liability by relying

[11] Stephanie Clifford, "F.T.C.: Has Internet Gone Beyond Privacy Policies?" *New York Times Media Decoder Blog*, http://mediadecoder.blogs.nytimes.com/2010/01/11/ftc-has-internet-gone-beyond-privacy-policies/.

[12] *See, e.g.*, *In the Matter of Guess?, Inc.*, Docket No. C-4091 (Federal Trade Commission, July 30, 2003) (requiring that the company "shall not misrepresent in any manner, expressly or by implication, the extent to which Respondents maintain and protect the security, confidentiality, or integrity of any personal

on attorneys to write policies that are as precisely worded as possible. In the face of these risks, it is commendable that commercial websites almost universally post privacy policies that are exceptionally transparent about the company's operations.

New regulation is not warranted given that companies have already shown a widespread willingness to adopt detailed privacy policies. Nevertheless, the DMA recognizes that there is room for improvement in how information is presented to consumers and that this, in turn, assists the consumer in making a more informed choice.

To date, the Commission has issued little concrete guidance on how website policies could be improved. The DMA suggests that further Commission guidance on how privacy policies can be made more friendly to consumers would be welcome. In order to encourage adoption of such guidance, it would also be helpful to provide a safe harbor mechanism so that companies that follow the Commission's guidance are shielded from liability. For example, the Commission and other agencies recently issued a new model privacy notice for financial information, based on consumer testing. It separates out the informational aspects of a privacy notice from the role that privacy notices play in holding financial institutions accountable for their practices. The use of this model notice affords financial institutions a safe harbor from liability, which provides a strong incentive to adopt the notice. A similar effort for website privacy policies would assist companies in complying with the Commission's expectations.

In addition, the DMA recognizes that there are certain practices for which a traditional privacy policy does not provide sufficient transparency. When such practices are identified, self-regulation in dialogue with the Commission provides an effective forum to develop a specialized policy. As online operations become increasingly complex, case-by-case policy responses will help to ensure that consumers are receiving adequate notice to make a meaningful choice about whether to use a website or service. For example, the Commission recently drew industry's attention to the unique considerations raised by online behavioral advertising. When third parties contribute to advertising operations, their data practices may not be included in the website privacy policy where a consumer would most likely seek such information. Thus, the Commission recognized a need for a specialized policy response.

In response to the Commission's call for action, "enhanced notice" to consumers is a key part of the Self-Regulatory Principles for online behavioral advertising. Participating advertisers will present a consistent and recognizable logo in close proximity to every behaviorally-targeted online advertisement. Consumers may click this logo for more information about why they received the advertisement and directions on how to opt out of targeted messages. This innovative solution will ensure that consumers

---

information collected from or about consumers"). The Commission has also taken the position that material changes to a policy should not be retroactively applied without consumer consent, which creates an incentive for companies to write expansive policies to avoid annoying consumers with repeated notifications of changes. *In the Matter of Gateway Learning Center*, Docket No. C-4120 (Federal Trade Commission, Sept. 10, 2004).

can easily receive notice of the data practices of third parties. As technology evolves, the Commission may identify additional situations where the unique transparency and choice solutions are appropriate. In such situations, the DMA would welcome the opportunity to work with the Commission in devising an appropriate response.

As the Commission considers ways to improve notice to consumers, the DMA also suggests that the Commission should recognize that the percentage of consumers that read or take action on privacy policies is not a valid measure of whether policies are adequate or the notice and choice model is working. The most likely explanation is that consumers are generally busy, have other priorities, and see no need to consult a policy – no matter how accessible or readable – unless they have specific concerns. The fair information practices invite the consumer to play a role in his own protection, but the consumer is free to decline this invitation. Declining to read a privacy policy is not evidence of a policy failure, but a preference which should be respected to the same extent as a choice to be actively concerned about privacy. (For example, it may be that only a tiny percentage of visitors to the Commission's own website read the privacy policy posted there, but this would not warrant an assumption that the policy is inadequate or confusing.) By the same token, consumers who consult a privacy policy and then continue to use the associated website are likely signaling that they are comfortable with the website's practices, perhaps because they believe that they are receiving a valuable and worthwhile service in exchange for any information shared. Finally, a privacy commitment in the form of a privacy notice can be used by self-regulatory enforcement, law enforcement, consumers, and consumer advocates to ensure businesses are living up to their commitments.

B. PII and Non-PII

Traditionally, the applicability of privacy and data security rules hinges entirely on whether the data constitutes PII. The policy roundtables raised the issue that, in some cases, it is difficult to distinguish whether data constitutes PII or non-PII. Certain speakers voiced a concern that data that is not inherently personally identifiable, such as clickstream data, browsing behavior, and search queries, may nevertheless raise privacy concerns when it is sufficiently detailed or granular.

What emerged from these discussions is the notion that, in some circumstances, certain privacy protections should apply regardless of whether the data is clearly personally identifiable or not. Maybe certain privacy protection should be reserved for personally *identifying* information, and a subset of privacy protection should be extended to information that is personally *identifiable*. (*i.e.*, *potentially* identifying information) This could avoid the sometimes endless debate of whether certain types of information constitute PII and thereby qualify for *any* privacy protections.

The FTC raised similar concerns in setting out its privacy principles for online behavioral advertising. In that instance, the FTC recognized self-regulation as the

appropriate approach to addressing such concerns.[13] Shortly thereafter, DMA and other leading trade associations responded by developing and releasing robust Self-Regulatory Principles in July 2009 that apply to data collected and used for online behavioral advertising, regardless of whether or not it qualifies as PII.[14] The DMA recognizes that there may be additional instances when the collection or use of non-PII implicates additional notice and choices. Such situations, however, should not result in removing an important policy distinction that treats PII differently from non-PII. In such cases, a similar refinement through self-regulatory standards may be helpful in guiding industry.

C. Privacy by Design

Finally, the DMA believes that the recent privacy roundtables highlighted the importance of engaging in "privacy by design" to ensure that notice, choice, and other principles are built into products and services from the beginning. Fundamentally, "privacy by design" entails making consumer privacy a proactive, preventive, and default mode of operation. The DMA agrees that privacy by design can be an important way of balancing innovation and privacy, since it encourages businesses to develop new technologies in a manner that respects consumer interests. The DMA suggests that the Commission should explore additional ways that it can encourage companies to engage in privacy by design, while not limiting important data flows.

This is reflected in the privacy enhancing technologies that continue to help in addressing Internet-related privacy concerns. The DMA believes that privacy enhancing technologies can play an important role in safeguarding privacy, and encourages the Commission to explore how such technologies can resolve policy challenges without regulation.

Time and again, issues perceived as privacy threats have been successfully addressed with technological solutions. Unwanted "spam" email is an instructive example. As email became widely used, unscrupulous parties took advantage of this efficient new medium to flood consumers with unwanted or offensive messages. The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act laid an important foundation by giving legitimate marketers a way to distinguish their practices.[15] However, unscrupulous competitors continued to violate the new rules. The decisive advance in the battle against spam was the development of numerous "filtering" technologies accurate enough to block spam from reaching consumers' mailboxes. Largely as a result of these technologies, spam has become a menace of the past, while

---

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

[14] 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.

[15] Pub. L. 108-187.

legitimate companies may freely communicate the messages that consumers value and wish to receive.

The DMA believes that privacy enhancing technologies will also be effective in addressing concerns about Internet tracking. In an example of "privacy by design," leading Internet browsers have already developed and deployed privacy controls that allow consumers to make detailed choices about whether and what information is tracked or saved as those consumers navigate the Internet. It is probable that increasing numbers of consumers will use browser controls as awareness and functionality increase.

Innovative browser controls address privacy concerns raised by the Commission in a way that preserves consumer choice yet does not disrupt the underlying Internet architecture. In combination with the self-regulatory efforts discussed below, the DMA expects that browser controls and similar market-driven tools can effectively safeguard consumers' online privacy. The DMA therefore recommends that the Commission give these promising tools more opportunity to be improved and adopted before embarking on any new regulation in the area of online behavioral advertising.

The DMA also encourages the Commission to explore other areas where privacy enhancing technologies can avoid the need for new regulation. Companies have a natural incentive to develop privacy enhancing technologies that address issues that concern consumers, and consumers will provide a market for tools that are effective and meet their needs. Where these incentives are not quite strong enough, the Commission can explore ways to promote the development or adoption of technology, such as by establishing safe harbors or extending official recognition to effective tools.

IV. Self-Regulation Is the Best Approach to Refining and Enforcing Privacy Protection in the Marketing Arena

A. Benefits of Self-Regulation

The DMA strongly believes that industry self-regulation based on the fair information practices is the best approach to online privacy protection, especially in the realm of marketing and advertising. Self-regulation is flexible enough to respond quickly to changes in the market and in business operations, ensuring that rules do not become outdated. Self-regulatory programs such as the DMA's also provide meaningful controls and accountability. DMA member companies have a major stake in the success of e-commerce and Internet marketing. They understand that their success on the Internet depends on consumers' continued confidence in the online medium, and they support efforts that enrich a user's experience while fostering consumer trust in online channels.

In particular, the self-regulatory approach is the most efficient and effective way to respond to privacy issues related to marketing and advertising. Advertising provides great benefits to consumers by making them aware of products, services, and offers that may interest them. Receiving such messages does not harm consumers in any

conceivable way, because unwanted messages can easily be ignored. Data collection and uses in support of advertising have raised some privacy questions, but the DMA believes that these questions are being adequately addressed through self-regulation as detailed below. Without additional evidence of consumer harm, the DMA submits that self-regulation generally remains the most appropriate method for industry to manage marketing practices with input from the Commission. Thus, to the extent that the Commission wishes to influence business practice in the areas highlighted above or in other areas, the DMA submits that engaging in dialogue with industry toward self-regulatory improvements is the most effective and efficient way for the Commission to realize its goals.

The DMA acknowledges that steps beyond self-regulation may be appropriate where a specific practice is found to cause identifiable and concrete harm to consumers. For example, some of the issues explored in the Commission's roundtable series, such as health or other sensitive information, may prove to merit such additional steps. When warranted, such practices should be addressed on a case-by-case basis to avoid unnecessarily disrupting the entire online ecosystem. The DMA looks forward to working with the Commission to evaluate and respond to these important questions.

B. DMA Guidelines for Ethical Business Practice

The DMA has a lengthy history of leadership in establishing effective and thorough industry self-regulatory standards. The DMA and its members have developed standards for online data practices and many other business activities as part of our comprehensive *Guidelines for Ethical Business Practice* ("Guidelines").[16] We have repeatedly updated our Guidelines, most recently in January 2010, to take account of new technologies and concerns. Under the current Guidelines, 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;[17]

- Not transfer personally identifiable health-related data gained in a medical treatment context for marketing purposes without the specific prior consent of the consumers;[18]

- 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;[19]

[16] Direct Marketing Association Guidelines for Ethical Business Practice, *available at* http://www.dmaresponsibility.org/Guidelines/.
[17] Guidelines, Article 32.
[18] Guidelines, Article 33.
[19] *Id.*

- Not rent, sell, exchange, transfer, or use marketing lists in violation of the Guidelines;[20]

- 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;[21]

- Identify and provide contact information for the entity responsible for a website;[22]

- Comply with the new self-regulatory principles for online behavioral advertising, discussed above;[23]

- 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;[24]

- Restrict data collection and marketing for children online or via wireless devices, consistent with the Children's Online Privacy Protection Rule;[25] and

- 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.[26]

These examples are only a sample of the restrictions contained in the Guidelines, which provide DMA member companies with a comprehensive blueprint for ethical marketing practices. Compliance with the Guidelines is required for all DMA members and the DMA can take action to enforce compliance by its members. In addition, companies that represent to the public that they are DMA members but fail to comply with the Guidelines may be liable for deceptive advertising.

In particular, the DMA believes that the promising Self-Regulatory Principles for online behavioral advertising, which were spurred by the Commission, should be given an adequate opportunity to continue and to be effective before additional regulation is

[20] Guidelines, Article 35.
[21] Guidelines, Article 38.
[22] *Id.*
[23] *Id.*
[24] Guidelines, Article 37.
[25] Guidelines, Article 16.
[26] Guidelines, Article 36.

considered in this area. Without such an opportunity, the Commission cannot meaningfully assess the success of the self-regulatory effort or the need for further intervention.

SECTION TWO: RESPONSES TO SPECIFIC COMMISSION INQUIRIES

In conjunction with the roundtable series, the Commission has solicited public comment on specific questions. Below, the DMA offers its views on each of these questions in turn.

I. Questions for the First Roundtable

1. *What risks, concerns, and benefits arise from the collection, sharing, and use of consumer information? For example, consider the risks and/or benefits of information practices in the following contexts: retail or other commercial environments involving a direct consumer-business relationship; data broker and other business-to-business environments involving no direct consumer relationship; platform environments involving information sharing with third party application developers; the mobile environment; social networking sites; behavioral advertising; cloud computing services; services that collect sensitive data, such as information about adolescents or children, financial or health information, or location data; and any other contexts you wish to address.*

The DMA believes that the benefits of data collection, sharing and use for advertising and marketing purposes far outweigh any risks to consumers. In general, marketing causes no identifiable harm to consumers. Marketing allows consumers to receive information about commercial opportunities that they may value, and consumers are free to respond (or not) as they see fit. If a consumer does not value a particular message, the consumer will simply ignore it. Moreover, marketing carries societal benefits as a facilitator of economic growth, and is a form of constitutionally protected speech. While the DMA recognizes that certain data practices do raise specialized policy concerns, the DMA strongly believes that these concerns should be addressed on a case-by-case basis and in dialogue with industry, while allowing most advertising and marketing uses of data to continue unhindered.

2. *Are there commonly understood or recognized consumer expectations about how information concerning consumers is collected and used? Do consumers have certain general expectations about the collection and use of their information when they browse the Internet, participate in social networking services, obtain products from retailers both online and offline, or use mobile communications devices? Is there empirical data that allows us reliably to measure any such consumer expectations? How determinative should consumer expectations be in developing policies about privacy?*

Consumers' privacy expectations and preferences are nuanced, highly individualized, and constantly changing in response to new technologies. Given the intricacy of today's technology, consumers also may not be in the best position to understand or assess the benefits and risks of a particular data practice. It is therefore practically impossible to measure such expectations with any level of reliability or to translate them into useful policy judgments. Any attempt to set broad standards by identifying an "average" consumer view will likely hinder technological development that other consumers may find valuable. Further, it would cause great economic harm and thwart innovation to set standards based on the "eggshell" consumer, which is what we believe various advocates are suggesting.

This inability to measure or generalize consumer expectations supports the DMA's view that consumer notice and choice remain the most simple, elegant, and effective solution for managing privacy concerns, especially in the rapidly evolving online world.

3. *Do the existing legal requirements and self-regulatory regimes in the United States today adequately protect consumer privacy interests? If not, what are the particular privacy interests that warrant increased protection? How have changes in technology, and in the way consumer data is collected, stored, and shared, affected consumer privacy? What are the costs, benefits, and feasibility of technological innovations, such as browser-based controls, that enable consumers to exercise control over information collection? How might increased privacy protections affect technological innovation?*

As discussed above, the DMA strongly believes that the Commission's existing approach to privacy regulation, which includes support for robust self-regulatory regimes, has been effective in promoting innovation and preserving consumer transparency and choice. This approach allows the Commission to identify and target discrete practices that warrant enhanced privacy measures, such as online behavioral advertising, while generally allowing innovation to thrive. As particular privacy interests are identified that warrant specialized protections, these interests can be addressed on a case-by-case basis. In keeping with this approach, the DMA also believes that privacy enhancing technological innovations can provide more tailored forms of consumer control than the blunt instrument of regulation, and are an excellent way to provide specialized protections when warranted.

II. Questions for the Second Roundtable

1. *What role do privacy enhancing technologies play in addressing Internet-related privacy concerns? Consider the efficacy of technological innovations in areas such as identity management systems, new means of providing consumer notice and choice, and emerging methods of ensuring accountability in data usage. In framing comments, consider the costs and benefits of privacy-enhancing technologies in the following contexts: cloud computing services; social*

networking sites; online behavioral advertising; the mobile environment; services that collect sensitive data, such as location-based information; and any other contexts you wish to address. If privacy enhancing technologies do play a role in resolving privacy concerns, discuss whether and how to create incentives for the development and adoption of such technologies, and ways to ensure they are effective and useful to consumers.

As detailed above, the DMA believes that privacy enhancing technologies can and should play a large role in addressing privacy concerns. Such technologies preserve consumers' control over their information by harnessing the innovative power of technology. With continued innovation, privacy enhancing technologies can potentially provide an efficacious response to all of the areas identified by the Commission's question.

The DMA further believes that consumer education is an essential and effective means to promote both the development and the adoption of privacy enhancing technologies. As consumers learn more about existing technologies and adopt them in greater numbers, this market incentive will naturally spur additional technological development, establishing a virtuous cycle that expands the range and usefulness of consumer offerings. Consumer education is an important facet of the DMA's efforts to implement the Self-Regulatory Principles for Online Behavioral Advertising. The DMA also encourages the Commission to engage in its own consumer education efforts to promote the use of privacy enhancing technologies of all kinds. For example, browser controls and plug-ins are widely available through leading browsers, and the Commission could encourage consumers who are concerned about privacy to enable these controls.

2. *What challenges do innovations in the digital environment pose for consumer privacy, and how can those challenges be addressed without stifling innovation or otherwise undermining benefits to consumers? For example, consider the technology and business practices that enable greater collection, use, and distribution of consumer data, including evolving methods of observation and tracking; techniques for correlating data, including the re-identification of anonymized data; the merging of data between on-line and off-line environments; and the emergence of third-party application developers in online platform environments.*

Advances in data practices carry many benefits for consumers, such as greater customization, ease of use, and support for free services through relevant advertising. Consumers' embrace of new technologies demonstrates that they generally value these benefits. If such innovations raise privacy questions for some consumers, the fair information practices remain the best way to address these questions. Specifically, given varying individual preferences about personal data use, the single most effective measure is to provide consumers with notice of data practices and an opportunity to choose whether their information may be used for such practices. For this reason, the DMA established an online mechanism, www.dmachoice.org, for consumers to set

individualized preferences about what marketing communications they wish to receive. This centralized tool is an effective way for consumers to make meaningful choices about marketing uses of their personal information.

III. Questions for the Third Roundtable

1. *How can we best achieve accountability for best practices or standards for commercial handling of consumer data? Can consumer access to and correction of their data be made cost effective? Are there specific accountability or enforcement regimes that are particularly effective?*

As detailed above, the DMA believes that self-regulatory enforcement regimes have proven to be extremely effective in holding companies to a high standard of conduct, without unnecessarily limiting innovation. Legitimate and law-abiding companies have a strong incentive to promote good practices that build consumer trust, and to enforce those practices against bad actors that damage such trust. In the event that peer enforcement is inadequate, the Commission retains the authority to step in and hold recalcitrant companies accountable. Another overlooked accountability mechanism is privacy policies, because the Commission can and does require companies to abide by their promises to consumers.

The DMA finds consumer access and correction abilities to be appropriate in some settings. For example, certain companies are successfully allowing consumers to view and change the marketing preference data that is used to provide them with relevant advertising. However, not all companies may have the same technological capabilities. The DMA therefore cautions against generalized access and correction rights that may simply overwhelm consumers with too many choices. In particular, access and correction for marketing data in many instances are both impractical and unnecessary. In establishing www.dmachoice.com, the DMA learned first-hand that access and preference tools for complex marketing data are both difficult and costly to place into operation. It would not be helpful to create a consumer expectation that such tools will be universally available, when in fact many entities lack the capacity to create end-products that are usable and meaningful for consumers.

2. *What potential benefits and concerns are raised by emerging business models built around the collection and use of consumer health information? What, if any, legal protections do consumers expect apply to their personal health information when they conduct online searches, respond to surveys or quizzes, seek medical advice online, participate in chat groups or health networks, or otherwise?*

Given the traditional sensitivity of health information and the new and evolving uses of such information, the DMA believes that there is a need to evaluate carefully whether and how the fair information practices and other privacy principles should apply to such information.

3. *Should "sensitive" information be treated or handled differently than other consumer information? How do we determine what information is "sensitive"? What standards should apply to the collection and uses of such information? Should information about children and teenagers be subject to different standards and, if so, what should they be?*

The DMA believes that sensitive information should be treated and handled differently than other consumer information, and addresses this issue throughout its Guidelines. For instance, the DMA Guidelines impose specialized rules on the handling of personally identifiable financial, health, and children's data. These categories of data are also specifically addressed in the Self-Regulatory Principles for Online Behavioral Advertising, which state that information should be collected from children under 13 only in accordance with the Children's Online Privacy Protection Act ("COPPA") and that certain financial and health information should be collected for online behavioral advertising with consent. Nevertheless, it is critical to design any rules for sensitive data in a way that allows information practices that do not harm consumers to continue.

The DMA acknowledges that additional types of data may be sensitive in certain contexts, and supports the Commission's effort to continue evaluating what data is sensitive. However, with regard to standards for such data, the DMA believes that different types of standards would likely be necessary for different types of data. If a consensus is reached that additional types of data are sensitive and merit different handling, then specialized standards should be developed to respond to the particular privacy concerns connected with that data.

For example, while children's data is already subject to different standards under COPPA, the DMA does not believe that these standards or other specialized standards should be extended to teenagers. Children younger than 13 are at a very different stage of development from teenagers, who are in the process of assuming many adult responsibilities. It is not appropriate to treat a 6-year-old the same way as a 16-year-old who is legally able to drive, work, or choose to drop out of school. Congress recognized this important distinction when it decided to apply COPPA to children younger than 13, and not to teenagers.

* * *

The DMA thanks the Commission for the opportunity to submit these Comments, and we look forward to working with the Commission as it continues to evaluate the important issue of online privacy.