



**Before the
DEPARTMENT OF COMMERCE
Washington, DC 20230**

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

**Responding to the Notice of Inquiry
on “Information Privacy and Innovation in the Internet Economy”**

Docket No. 100402174-0175-01

June 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
575 Seventh Street, NW
Washington, DC 20004
(202) 344-4613



Direct Marketing Association, Inc.

Comments on “Information Privacy and Innovation in the Internet Economy”

Docket No. 100402174-0175-01

The Direct Marketing Association (“DMA”) commends the Department of Commerce for launching its Privacy and Innovation Initiative and applauds the Department’s commitment to ensuring that the Internet remains “open for innovation.”¹ The DMA appreciates the opportunity to submit these Comments in response to the Department of Commerce’s Notice of Inquiry on “Information Privacy and Innovation in the Internet Economy” (the “NOI”).²

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 United States 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 two sections of these Comments, the DMA presents its general view that the current U.S. approach to privacy regulation has effectively fostered innovation and preserved consumer choice and explains why the DMA believes that industry self-regulation is the best approach to refining and enforcing privacy protections, especially in the marketing arena. The third and final section of the Comments responds to selected questions posed in the NOI.

I. The U.S. Approach to Privacy Regulation Has Effectively Fostered Innovation and Preserved Consumer Choice

As the NOI recognizes, the Internet is no longer a distinct industry, but penetrates every area of Americans’ business and private lives. The DMA’s member companies grapple each day with the business and ethical consequences of this expansion and the attendant technological innovation. 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 existing U.S. approach to

¹ 75 Fed. Reg. 21226 (April 23, 2010).

² *Id.*

privacy regulation, which has allowed innovation to flourish while preserving consumer choice.

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 Department of Commerce, Federal Trade 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.

With this balance in mind, U.S. privacy regulation is founded on several core principles known as “fair information practices,” which are designed to ensure that consumers can exercise meaningful control over their private information while allowing beneficial information use to continue. As summarized by the Federal Trade Commission in a report to Congress, these 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 and allowing beneficial uses of information to continue.

In keeping with this balanced approach, Congress has largely followed a “sectoral” framework in U.S. privacy legislation. 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. The Department of Commerce notes this pattern in the NOI and requests input on how it affects businesses.⁴ The DMA believes that compelling policy reasons support 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. Data practices are complex, and the sectoral framework allows Congress to devise tailored responses to specific areas of concern. 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.shtml> (last visited March 9, 2010).

⁴ 75 Fed. Reg. at 21230.

Further, the online advertising business is a highly dynamic market characterized by rapid technological change. In this environment, regulation that is specific to a technology or business model could deter entry, thwart innovation, and limit competition in the sale of online advertising. Fewer choices for online ad sales could exacerbate the already significant financial pressure on advertiser-supported media. No company can succeed in today's highly competitive marketplace unless it wins and retains the trust of its customers. Rather than impose disparate regulation, the government should promote industry self-regulatory approaches that protect privacy while promoting competition among technologies and business models.

Against this regulatory backdrop, 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. Advertising has provided critical support for this development across business models and technologies. As noted in the NOI, online commerce is thriving and increasing, even during the current economic downturn. This e-commerce is spurred by online advertising and marketing. In addition to turning to the Internet for its e-commerce resources, consumers have come to expect rich online content and services at little or no cost to the consumer.

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.

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. The DMA believes that marketing data should only be used for marketing purposes. The DMA further believes that regulation should not be specific to a technology or business model, which would impede both competition and innovation.

While there are those who 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. American consumers are avid users of the Internet, and are quickly embracing emerging technologies like cloud computing, mobile computing, and social networking. Consumers' embrace of e-commerce shows that they widely value the convenience, customization, and features that companies can offer online. It is evident that the prevailing U.S. approach to privacy regulation strikes an appropriate balance that benefits consumers and industry alike.

The DMA cautions against new legislation, regulation, or policies that could disrupt this beneficial cycle. Unnecessary restrictions on online advertising could reduce the relevance of commercial messages to consumers. 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 e-commerce, or drive businesses to shift from offering free content and services to demanding direct payments from consumers. Similarly, any restrictions on data used to power commercial messages could cause consumer confusion and undermine the very consumer trust that has enabled Internet commerce to thrive. Given the penetration of the Internet into all areas of business, it is important to note that regulation of the online ecosystem amounts to regulation across industries. Shifts in U.S. policies toward the Internet 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 DMA also believes that the Federal Trade Commission ("FTC"), as the primary federal enforcement agency in this arena, has long made an appropriate choice to focus its enforcement resources on practices that cause demonstrable harms to consumers, such as physical harms, economic injuries, or unwarranted intrusions such as spam and spyware.⁵ This approach allows the Commission to identify and target discrete practices that warrant enhanced privacy measures, as it has done with online behavioral advertising, while generally allowing innovation to thrive. This "harm-based" focus 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.⁶ The DMA also believes that the harm-based philosophy respects the individualized nature of privacy preferences and correctly recognizes that tangible harm to consumers is the most meaningful and objective yardstick to determine whether regulation or enforcement is needed. In addition, the harm-based approach tends not to favor or disadvantage a particular business model, since it zeros in on a specific, objectionable practice, which is most appropriate.

⁵ 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).

⁶ The "Preventing Harm Principle" is the first principle of the APEC Privacy Framework. APEC Secretariat, *APEC Privacy Framework* 11 (2005).

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

A. *Benefits of Self-Regulation*

The NOI requests comments about the state of efforts to develop self-regulation in the privacy arena.⁷ 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 or stymie innovation.

Self-regulatory programs such as the DMA's 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 businesses depend 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. Compliance with the DMA's comprehensive *Guidelines for Ethical Business Practice* (the "Guidelines") is required for all DMA members.⁸ The DMA can and does take action to enforce compliance, including by referring matters to enforcement authorities. 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 under federal or state laws.

Specifically, 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 and submits that self-regulation generally remains the most appropriate method for industry to improve marketing practices with input from government authorities.

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. When warranted, such practices should be addressed on a case-by-case basis to avoid unnecessarily disrupting the entire online ecosystem.

⁷ 75 Fed. Reg. at 21229.

⁸ Direct Marketing Association Guidelines for Ethical Business Practice, *available at* <http://www.dmaresponsibility.org/Guidelines/>.

B. DMA Guidelines for Ethical Business Practice

The effectiveness of self-regulation is demonstrated by the DMA's 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 Guidelines. We have repeatedly updated our Guidelines, most recently in January 2010, to take account of new technologies and concerns. Among other requirements 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;⁹
- Not transfer personally identifiable health-related data gained in a medical treatment context for marketing purposes without the specific prior consent of the consumers;¹⁰
- 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;¹¹
- Not rent, sell, exchange, transfer, or use marketing lists in violation of the Guidelines;¹²
- 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;¹³
- Identify and provide contact information for the entity responsible for a website;¹⁴
- Comply with the new self-regulatory principles for online behavioral advertising, discussed below;¹⁵

⁹ Guidelines, Article 32.

¹⁰ Guidelines, Article 33.

¹¹ *Id.*

¹² Guidelines, Article 35.

¹³ Guidelines, Article 38.

¹⁴ *Id.*

¹⁵ *Id.*

- 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;¹⁶
- Restrict data collection and marketing for children online or via wireless devices, consistent with the Children's Online Privacy Protection Rule;¹⁷ 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.¹⁸

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.

Most recently, the DMA worked with a coalition of other leading trade associations and companies to develop Self-Regulatory Principles for Online Behavioral Advertising ("Self Regulatory Principles"), released in July 2009.¹⁹ These principles require advertisers and websites to inform consumers about data collection practices and enable them to exercise control over that information. The Self-Regulatory Principles define "online behavioral advertising" as the "collection of data from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate websites for the purpose of using such data to predict user preferences or interests to delivery of advertising to that computer or device based on the preferences or interests inferred from such web viewing behaviors."²⁰ The Principles call on companies to:

- Provide enhanced notice outside of the company's privacy policy on any web pages where data is collected or used for online behavioral advertising purpose;
- Provide choice mechanisms that will enable users of websites at which data is collected for online behavioral advertising purposes the ability to choose whether data is collected and used or transferred to a non-affiliate for such purposes;
- Provide reasonable security for, and limited retention of, data collected and used for online behavioral advertising purposes;

¹⁶ Guidelines, Article 37.

¹⁷ Guidelines, Article 16.

¹⁸ Guidelines, Article 36.

¹⁹ Self-Regulatory Principles for Online Behavioral Advertising, *available at* <http://www.iab.net/media/file/ven-principles-07-01-09.pdf> (last visited May 13, 2010).

²⁰ Self-Regulatory Principles, at 2.

- Obtain consent before applying any material change to their online behavioral advertising data collection and use prior to such material change; and
- Provide heightened protection for certain sensitive data.

The Principles have been incorporated into the DMA Guidelines and are now binding on all DMA member companies. The DMA encourages the Department of Commerce and other federal agencies to recognize and promote industry self-regulation, such as the DMA Guidelines, that benefits consumers by protecting privacy without hindering competition.

III. Responses to Selected Questions Posed in the NOI

A. *Notice and Choice Should Remain the Foundation of U.S. Privacy Regulation*

1. *The Notice and Choice Model, Including the Development of Specialized Notice Mechanisms When Appropriate, Remains the Best Way to Balance Innovation and Privacy*

The NOI states that the Department of Commerce has heard from certain stakeholders that “the customary notice and choice approach to consumer protection may be outdated[.]”²¹ The DMA disagrees with this view. Furthermore, the DMA does not believe that it would be appropriate or productive for data managers to adopt “use-based” rules across all data flows that would regulate all types of uses and purposes for which personal information may be employed. Defining appropriate uses may make sense in some instances such as health or financial data but not in others. Overly broad use restrictions could limit innovation and the development of new business models.

As discussed above, notice and choice, implemented in conjunction with the other fair information principles, have been effective for decades in allowing innovation to flourish while preserving consumer control over their information. Switching to a different regime would abandon this proven model and could constrain important business practices. The notice and choice model is already designed to provide consumers with the information and tools to enforce their individual privacy preferences. A privacy commitment in the form of a privacy notice can also be used by self-regulatory enforcement, law enforcement, consumers, and consumer advocates to ensure businesses are living up to their commitments.

While there may be certain situations where additional use restrictions are appropriate, rather than abandoning the notice and choice model in favor of an untested alternative, the DMA believes that the focus should be on improving how information is presented to consumers and developing new tools to assist consumers in making more

²¹ 75 Fed. Reg. 21226, 21229 (April 23, 2010).

informed choices. The DMA suggests that further guidance from regulators on how privacy policies can be made more friendly to consumers would be welcome. To date, federal regulators have provided little concrete guidance on how website policies could be improved. In order to encourage adoption of such guidance, it would also be helpful to provide a safe harbor mechanism so that companies that follow such guidance are shielded from liability. The recent efforts of a group of agencies in issuing a new model privacy notice for financial information, based on consumer testing, provide a useful model for such an undertaking.

However, efforts to improve notice mechanisms 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. Consumers are generally busy, have many priorities, and likely 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.

The DMA recognizes that there are certain practices for which a traditional privacy policy does not provide sufficient transparency. One example of an innovative notice and choice mechanism is the DMA’s online tool, 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.

The DMA has also found that self-regulation in dialogue with federal regulators can provide an effective forum to develop specialized policies to address practices for which a traditional privacy policy may not be sufficient. As online operations become increasingly complex, such case-by-case policy responses can ensure that consumers are receiving adequate notice to make a meaningful choice about whether to use a website or service. For example, the Federal Trade 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 can easily receive notice of the data practices of third parties. As technology evolves, regulators may identify additional situations where the unique transparency and choice

solutions are appropriate. In such situations, the DMA expects that dialogue between regulators and industry will be effective to devise an appropriate and tailored response.

2. *Opt-In Consent Is Not the Solution*

The DMA notes that consumer “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. However, there has been some recent public debate about whether opt-in consent for data collection, use, and/or disclosures should be required in various settings. 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 creates a presumption against the free flow of data and will disrupt this existing online architecture. Ultimately, such new restrictions would undermine consumer enjoyment of the Internet, which is the foundation of online commerce.

There is no indication that legitimate data flows harm consumers or should be discouraged. In particular, the DMA is not aware of any evidence of concrete harm to consumers from the legitimate data practices that support online advertising. The DMA also is not aware that a societal consensus against data transfers has been identified, or that researchers have shown that consumers would be willing to accept a changed Internet experience in exchange for reducing such transfers. In the absence of such convincing evidence, the DMA believes that it would be detrimental to innovation and consumer welfare to introduce new requirements related to opt-in consumer consent. Indeed, it is likely that constant appearances of notice boxes will annoy and frustrate consumers, and will dilute the impact of such mechanisms. To the extent that the debate regarding opt-in consent is related to concerns 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.

B. Privacy-Enhancing Technologies

The NOI seeks “input on the development, use and acceptance of privacy-related technologies and business processes and their potential to enhance consumer trust in Internet commerce.”²² DMA believes that privacy-enhancing technologies and the “privacy by design” philosophy should be core tools in the effort to promote innovation while preserving consumer control. Privacy-enhancing technologies promote consumer control by harnessing innovation and competition rather than stifling them. DMA

²² 75 Fed. Reg. at 21230-21231.

strongly encourages the Department of Commerce to explore how the government can support businesses in developing new products and technologies that can address policy challenges without the need for 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, government can spur the development or adoption of such tools through steps like establishing safe harbors, extending official recognition to effective tools, or purchasing effective technologies for use by government employees or agencies.

The DMA believes that privacy-enhancing technologies will also be effective in addressing concerns about online data collection and use. 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. Browser controls allow consumers with privacy concerns to exercise control over their information in a way that does not disrupt the underlying Internet architecture. The DMA expects that browser controls and similar market-driven tools can effectively safeguard consumers' online privacy, and recommends that these promising tools should be given more opportunity to flourish before government agencies embark on any new regulation in the area of online behavioral advertising. DMA self-regulation in this area and the "PCI" standards that govern sensitive information have proven useful towards protecting data.

The NOI specifically requests comment on the concept of developing "trusted identity providers" to assist consumers in managing their data.²³ The DMA suggests that the best way to encourage the development of such providers is through the operation of the marketplace. Any new government mandate would be likely to disrupt the natural pace and direction of technological innovation by business.

C. Consumer Expectations and Education

The NOI asks whether the focus of privacy laws and regulations should be on satisfying subjective consumer expectations or on enacting objective principles.²⁴ As a general matter, the DMA does not believe that U.S. privacy policy should be based on subjective consumer expectations. 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

²³ 75 Fed. Reg. at 21231.

²⁴ 75 Fed. Reg. at 21229.

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 the essence of many proposals put forward by advocates. 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.

However, the DMA believes that consumer education is an essential and effective means to encourage consumers to exercise their privacy choices. In particular, consumer education can be valuable in advancing 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 government bodies to engage in consumer education efforts to promote privacy awareness and the use of privacy enhancing technologies of all kinds. For example, browser controls and plug-ins are widely available through leading browsers, and consumers who are concerned about privacy should be encouraged to enable these controls.

D. Minimizing Inconsistent and Unnecessary Restrictions on Business

The NOI poses several questions regarding the potential for inconsistent regulation across countries, jurisdictions, and U.S. states.²⁵ As a general matter, the DMA believes that it is appropriate to strive for consistency in the regulations that apply to business data practices. However, consistency should not be achieved by spreading restrictive regulations from one jurisdiction to the next. The DMA encourages the Department of Commerce and the Administration to work to ensure that U.S. companies are not hindered in their growth and operation by foreign countries’ efforts to impose restrictions that harm American businesses and do not comport with the U.S. approach to privacy regulation. Likewise, the Administration should refrain from supporting state efforts to limit businesses’ data practices in ways that are stricter than or out of step with the approaches of other states.

* * *

The DMA appreciates the opportunity to provide these Comments to the Department of Commerce. Please contact Linda Woolley at 202-861-2444 or lwoolley@the-dma.org with any questions.

²⁵ *Id.* at 21229-21230.