

January 28, 2011

Via electronic filing: privacynoi2010@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW. Room 4725
Washington, DC 20230

Re: Comments on the Department of Commerce Internet Policy Task Force
“Report on Commercial Data Privacy and Innovation in the Internet
Economy: A Dynamic Policy Framework”

Dear Internet Policy Task Force:

The undersigned represent a wide array of industries and companies that have come together to respond to the Department of Commerce’s Internet Policy Task Force’s (“Department”) green paper entitled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (the “Report”).¹ Included are leading trade associations and organizations from the advertising, marketing, media, financial services, retail, and Internet industries. The undersigned appreciate this opportunity to provide these comments.

We welcome the Department’s support for voluntary codes of conduct.² Voluntary codes of conduct developed through self-regulatory mechanisms constitute the most effective framework for protecting consumer privacy while ensuring the Internet remains a platform for innovation. Through self-regulatory efforts, industry will continue to quickly respond and address the evolving preferences and concerns of consumers.³ We believe that such voluntary codes should be developed by the businesses to which the standards would apply, rather than imposed by the government. This notion comports with the Department’s recognition that the government can provide incentives for industry to engage in effective private sector problem-solving.⁴

¹ Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (December 2010) (*hereinafter* “Report”).

² Report at 29.

³ As the Department has noted, the dynamic process of voluntary code development has provided protections to consumers while retaining flexibility to keep pace with commercial innovations. *See* Report at 6.

⁴ Report at 6 n.7 (“This idea draws on the more general observation that in some cases government agencies can ‘create structures or incentives for private sector problem-solving’ without acting as a full-fledged regulator.”).

Online Advertising and Marketing Provide Significant Benefits to Consumers and Businesses

The Report highlights in its opening pages that “personalized advertising” is essential to the digital economy.⁵ Indeed, online advertising and marketing provides significant benefits to the economy, consumers, and businesses. It supports valuable Internet content, services, and products that shape today’s popular Internet experience. It also provides consumers with information regarding products and services most likely to be of interest to them, including news, weather, sports, and other commercial content. Moreover, online advertising creates cost efficiencies that directly result in new entrants to the marketplace that otherwise would not be economically viable.

As recognized by the Department in the Report, a significant amount of global commerce takes place on the Internet. According to the Report, online retail sales in 2009 accounted for over \$140 billion in retail sales for U.S. companies, and three million Americans were employed directly or indirectly by advertising-supported Internet services, 1.2 million of whom hold jobs that did not exist two years ago.⁶ The Report also states that between 1998 and 2008, the number of domestic information technology (“IT”) jobs grew by 26 percent – four times faster than U.S. employment as a whole – and by 2018, IT employment is expected to grow by another 22 percent.⁷ These are extraordinary results given the current economic woes, underscoring the fact that the Internet is only increasing in its importance as a vital sector of the United States’ economy.

Online advertising and marketing significantly subsidize the cost of providing products to consumers online, allowing companies to fund the content and services that consumers have come to expect and enjoy. For example, Internet advertising supports online versions of newspapers and magazines, blog platforms, and online forums, such as resume services, job banks, and social and professional network communities, which are available to consumers at little or no costs. It also subsidizes online offerings such as e-mail, chat, video conferencing, telephone service, and online safety tools. Further, with an average return of 457 percent, behavioral advertising is 50 percent more effective in generating incremental revenue than other types of online advertising,⁸ providing much greater revenue to support free contents and services on the Internet.

In addition, online advertising and marketing has enhanced consumers’ online experience by improving the relevance of particular advertisements. Through behavioral and contextual advertising, consumers receive advertisements for products and services likely to be of interest to them, enabling them to make more informed buying decisions.

⁵ Report at vi.

⁶ Report at 13-14.

⁷ *Id.*

⁸ According to study performed by the Ponemon Institute on behalf of Evidon, available at http://www.evidon.com/documents/OBA_paper.pdf.

Online advertising and marketing also improve a company's ability to communicate with consumers. When a business can efficiently market its goods to consumers through targeted interactive advertising – connecting with audiences more likely to be interested in its particular products or services – its marketing and advertising costs are dramatically reduced, thereby lowering prices for consumers. In addition, online advertising and marketing has increased competition in the marketplace and has opened markets to new entrants that offer a diverse variety of new products and services. The Internet and online advertising have opened larger markets to small business by lowering the barriers to entry, and created national markets for previously local, regional, or niche business models.⁹ This increased competition encourages innovation and leads to lower prices, all to the direct benefit of consumers.

There is already strong evidence that privacy regulations in the European Union have resulted in an average 65 percent reduction in the effectiveness of online ads.¹⁰ Regulatory intervention in the U.S. could similarly hinder innovation in the advertising and marketing industry, undermining economic support for valuable content and services and possibly encouraging higher fees to consumers. A general contraction in the e-commerce market could result, stifling a powerful engine of the American economy.

Voluntary Codes of Conduct Developed Through Self-Regulatory Mechanisms Are the Most Effective Ways to Balance Consumer Privacy and Commercial Innovation

We agree with the Department's determination that voluntary codes of conduct are the appropriate approach for addressing consumer privacy while ensuring that commercial innovation through the Internet continues to flourish.¹¹ We believe that these voluntary codes should be developed through self-regulatory mechanisms. As the Report recognizes, self-regulation provides a framework by which new challenges that emerge in the evolving Internet ecosystem can quickly be addressed while ensuring flexibility for development of new channels, services, and products. In contrast, rigid regulations could stifle innovation as rules are out paced by evolving technologies and consumer preferences.¹² In addition, no law should establish an operational framework or impose any requirements for self-regulatory mechanisms because such action would restrain industry's ability to quickly and effectively develop self-regulatory programs that best meet changing consume preferences.

The current regulatory environment composed of sectoral laws, Federal Trade Commission ("FTC") enforcement, and self-regulation, coupled with competition in the

⁹ The Report recognizes that the Internet is global and has reduced barriers to entry. Report at 19 ("Unlike the traditional mass media, the Internet is global. Additionally, in contrast to the relatively high barriers to entry in traditional media marketplaces, the Internet offers commercial opportunities to an unusually large number of innovators, and the rate of new service offerings and novel business models is quite high.").

¹⁰ According to a study conducted by Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.

¹¹ Report at 29.

¹² See Report at 22 ("[T]o maintain the flexibility of the current U.S. commercial data privacy policy framework, an integral part of our Framework is to allow adherence to voluntary industry codes of conduct.").

marketplace, provides sufficient incentive for industry to provide strong commercial data privacy protections. As the Report notes, this framework “has facilitated innovation and spurred some of the world’s most technologically advanced services, while also providing meaningful privacy protections.”¹³ Increasingly, privacy features are a point of competition in the marketplace, providing consumers with more information about online data practices and the availability of choice and tools to control their online experience. We, like the Department, view this as a positive trend that should be encouraged by public policy and not restrained by rigid regulation.¹⁴ A self-regulatory approach will help ensure that these developments continue to flourish, providing new privacy features and protections.

There have been significant developments in self-regulation in the online privacy arena in the last two years. A very strong foundation of industry self-regulation has been in place since the beginning of the commercial Internet, including the guidelines and standards of the Direct Marketing Association (“DMA”), the Interactive Advertising Bureau (“IAB”), the Network Advertising Initiative (“NAI”), TRUSTe, the AICPA’s WebTrust, and BBBOnLine. The industry has recently built on this tradition with the development and implementation of a robust self-regulatory program to provide greater transparency and control over online behavioral advertising.¹⁵

In July 2009, a coalition of industry organizations released the *Self-Regulatory Principles for Online Behavioral Advertising* (“Principles”) and subsequently launched a related self-regulatory program (“Program”) to operationalize the Principles early in the fall of 2010.¹⁶ The Principles – developed through what the Report highlights as a “prime example” of the multi-stakeholder approach – were designed to apply broadly to the diverse set of actors that work interdependently to deliver relevant advertising intended to enrich the consumer online experience. In all, the Principles foster consumer friendly standards that are to be applied throughout the ecosystem. The Principles call for: (1) consumer education, (2) enhanced notice outside of the privacy policy, (3) the provision of new choice mechanisms, (4) data security, (5) heightened protection for certain sensitive data, (6) consent for certain material changes to online behavioral advertising data collection and use policies, and (7) strong enforcement mechanisms.

The Program, which puts the Principles into action, is now well underway (*see* www.aboutads.info). A key component of the Program is its promotion of the “Advertising Option Icon” for use within or near online ads or web pages where data is collected for online behavioral advertising purposes. When consumers click on the Advertising Option Icon, they learn about the collection and use of data by entities

¹³ Report at 11.

¹⁴ Report at 15 (“The Department of Commerce shares the belief that maintaining consumer trust is vital to the success of the digital economy.”).

¹⁵ The Report recounts this initial progress toward establishing voluntary codes of conduct to govern commercial privacy at Report 19-20.

¹⁶ 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.iab.net/media/file/ven-principles-07-01-09.pdf>. See Report at 27-28.

engaged in online behavioral advertising and can also easily opt out of such practices. The Advertising Option Icon is already being served on the Internet in ads, but in the coming weeks, billions of ad impressions will include the icon, making its use and adoption readily available and noticeable to consumers. Additionally, the Program Website includes an AboutAds Consumer Opt-Out Page linked to from the Advertising Option Icon that now allows consumers to easily choose to opt out of receiving some or all interest-based ads (*see* www.aboutads.info/choices). Approximately 60 companies are already providing choice through the Consumer Opt-Out Page with dozens more preparing to join. The Program website is now providing an enormous resource for consumer education about the operation, purposes, and real-time functioning of online behavioral advertising. Both the DMA and the Council of Better Business Bureaus (“CBBB”) ensure accountability for the program, with the former scheduled to begin monitoring compliance by the end of January 2011 and the latter scheduled to begin enforcement by March 31, 2011.

In response to the Department’s inquiry into the best way of promoting transparency to promote informed choices, in addition to the above programs, companies are rapidly advancing technologies that provide more choices to consumers.¹⁷ For example, companies are developing preference management tools to allow customers to express their preferences with respect to types of advertising they receive.¹⁸ These advancements show the value of industry self-regulation, which has provided flexibility to companies to develop transparency mechanisms that fit their business models.

A FIPPs-Based Framework Is Useful for Companies to Use to Analyze Their Practices, But Not as a Mandated Legislative or Regulatory Framework

We support the use of Fair Information Practice Principles (“FIPPs”) as a useful tool for companies to employ in analyzing their practices. As the Department considers how a FIPPs-based framework for commercial privacy would be implemented, we maintain that the implementation of FIPPs through legislation or regulation simply would not work.¹⁹ Formal codification of baseline FIPPs would not maintain the flexibility and nimbleness needed for continued online innovation. The establishment of a FIPPs-based framework through legislation or regulation would reduce industry’s ability to respond to changes in consumer preferences and would hinder advancements in technology.

The mandatory application of a comprehensive set of FIPPs to all data practices is unworkable in practice. As the Department notes in the Report, “FIPPs are designed to be comprehensive and general; thus, there may be contexts in which certain principles do not apply leading to a waste of resources when businesses must demonstrate compliance

¹⁷ Report at 37.

¹⁸ See, e.g., BlueKai’s Registry (<http://tags.bluekai.com/registry>) (providing transparency to consumers by allowing them to see and change what preferences are being logged via cookies on their computer or to opt-out); Google’s Ads Preference Manager (www.google.com/adspreferences) (enabling users to see and control interests associated with their browser or to opt-out of interest-based advertising).

¹⁹ Report at 23-24.

with each principle.”²⁰ FIPPs are high-level principles whose application varies significantly based on the type of data in question and the context in which it is used.

For example, mandatory data access and correction standards are unnecessary for data collected and maintained for marketing purposes.²¹ Although marketing databases maintain information about individuals, marketers do not need precise information on individual consumers, but only seek to understand the general characteristics of the individuals to which they are marketing. In many cases, marketing databases are compiled at the geographic or household level, rather than at the personal level, and marketing data are estimated or presented in ranges. Moreover, marketing information is not used to assess eligibility for credit, insurance, or employment, and the use of third-party information in such cases is already governed by fair information practices in statutes including the Fair Credit Reporting Act, the Fair Billing Act, the Fair Debt Collection Practices Act, and the Health Information Privacy and Accountability Act. If a consumer’s information is inaccurate in a marketing database, there is no harm to the consumer aside from the possible annoyance on receiving an irrelevant offer. More importantly, expanding access to such data would raise significant privacy, data security, and cost considerations because identifying information would need to be *added* to marketing databases in order to authenticate a consumer’s access. For these reasons, it does not make sense to apply access and correction requirements for marketing data in the same ways that FIPPs have been applied under particular statutory regimes.

First-party marketing provides another example in which a mandatory “one size fits all” application of FIPPs is neither necessary nor appropriate.²² Consumers already enjoy choice in first-party marketing – affected through industry or company opt-out mechanisms – in numerous situations deemed necessary under existing regulation or industry practice. These tailored choice mechanisms, which exist in every direct marketing channel, reflect the studied review of policy-makers and industry regarding consumer preferences and expectations for first-party marketing. Mandatory collection of additional consent in areas where consumers are aware of, and significantly benefit from, the use of such information by first parties is not necessary.

For the same reasons, mandatory application of the principles of purpose specification and use limitation should not apply to the collection or use of marketing data. The appropriate way to align consumer expectations with commercial information practices is by providing meaningful notice to consumers about a company’s data collection and use practices, and, where appropriate, providing choice. Meaningful notice does not require companies to specifically enumerate every possible use of collected data. This not only adds to the length and complexity of such notices, but it could have the effect of stifling valuable and consumer friendly innovations.

While FIPPs serve as the foundation for many self-regulatory programs and best practices, they are applied through self-regulation in a manner tailored to meet the

²⁰ Report at 41.

²¹ Report at 26 (discussing individual participation).

²² See Report at 34 n.102-103.

particular context. Industry has demonstrated that, applying the FIPPs framework as a guiding tool, it can appropriately and effectively provide consumer safeguards without a federal mandate that dictates or directs the application of principles.

Lastly, we have concerns with the prospect of enforceable mandates that would require companies to submit to costly privacy impact assessments (“PIA”) and/or audits as the Department has proposed.²³ The Department has not sufficiently demonstrated that the benefits of requiring companies to undergo regular PIAs or audits outweigh the costs. For example, the Department recommends the use of PIAs as a means to enhance transparency. However, it is unlikely that PIAs would be simpler or easier to understand by everyday users than privacy notices. Although we agree that companies should be encouraged to think through how their information systems or practices comport with privacy standards, the use of formal PIAs and audits are not appropriate in all contexts. It also should be noted that companies already conduct such assessments where appropriate.

Industry Self-Regulation Provides the Type of Choice that has been Called for through Do-Not-Track Proposals.

Industry supports the provision of uniform consumer choice mechanisms, which is the policy goal underlying “Do Not Track” proposals. Significant self-regulatory efforts are underway that provide the uniform consumer choice for online behavioral advertising contemplated by these proposals. As described in a prior section, the AboutAds Consumer Opt-Out Page is currently operational, giving consumers dynamic information about the companies that have enabled customized ads on their browsers and allowing them to opt-out of some or all of the companies participating, if they choose.

Efforts by the federal Government—through legislation or regulation—to create or mandate a Do Not Track mechanism risk threatening the Internet as it exists today. Therefore, we caution going down a path that could significantly harm this important area of American innovation and dominance, and a primary area of job growth and investment.

If Legislative or Regulatory Proposals for Online Privacy are Enacted, They Should Create a Safe Harbor for Companies that Adhere to Appropriate Voluntary, Enforceable Codes of Conduct

We have concerns with implementing privacy principles through legislation or rulemaking because in an extremely rapidly developing and transformative environment, laws or regulations are likely to lock in requirements that will stifle innovation and fail to respond appropriately to changes in the marketplace. However, should such legislation or rulemaking be considered, companies that adhere to robust, voluntary and enforceable codes of conduct, such as the Self-Regulatory Program for Online Behavioral Advertising, should qualify for a safe harbor. We agree with the Department that such a

²³ Report at 34 (recommending the use of privacy impact assessments (PIAs)).

safe harbor could provide strong incentives to companies to develop and comply with voluntary codes of conduct.²⁴

Any proposed legislation should not expand the FTC's enforcement power beyond its current authority or provide a private right of action to consumers. The FTC already has wide enforcement power to regulate consumer privacy protection under numerous sector-specific statutes and Section 5 of the FTC Act. As discussed in the FTC's *Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, the FTC has capably used its authority under these statutes to bring cases against businesses that allegedly failed to protect consumers' personal information. In the last ten years alone, the FTC has brought 29 such cases. The FTC has also brought over one hundred cases involving unwanted spam, spyware, and violations of the Children's Online Privacy Protection Act ("COPPA").

To police those entities that commit to follow voluntary codes of conduct, we recommend the use of industry accountability programs, similar to those developed by the DMA, the National Advertising Review Council and its administrator, the CBBB. These programs have a long history of successfully ensuring compliance and accountability as well as cooperation with the FTC.

The Department Should Continue Its Efforts to Encourage Global Interoperability and Harmony of Laws Across Countries

We support the Department's recommendation that the U.S. government continue to develop a framework for mutual recognition of an international data privacy framework.²⁵ The Department has an important role in representing and advocating for the interests of American businesses. We believe that the Department has the experience and expertise needed not only to represent the interests of U.S. industry, but to lead the global privacy policy debate. We recommend that the Department advocate for a global framework consistent with U.S. privacy standards, including the Self-Regulatory Principles for Online Behavioral Advertising, which have allowed U.S. companies to lead the world in innovation and to remain economically competitive. In addition to decreasing regulatory barriers to trade and commerce, global interoperability should promote—or at a minimum not impede—economic competition and innovation. We believe the U.S. approach to privacy policy meets these goals.

Industry Supports a National Standard for Notifications Following Security Breaches Involving Personal Information in the Commercial Context

As the Department has recommended, we support a national standard for security breach notification that would reconcile inconsistent state laws.²⁶ In recent years, nearly every state (and three other jurisdictions, including the District of Columbia) has enacted

²⁴ Report at 43.

²⁵ Report at 53.

²⁶ Report at 57.

a data security breach notification law. These laws have been effective in improving data security standards and ensuring robust consumer notification when there is a significant risk of harm to affected individuals following a breach of security involving sensitive personal information about them. We believe that a national standard should be based on the prevailing model developed through the states.²⁷

Consistent with our prior statements, however, we believe data that is not personally identifiable or sensitive, such as marketing and advertising data, should not be subject to an unduly burdensome breach notification regime. A national standard for commercial data breaches that broadly sweeps in all types of data would be costly to implement and bothersome for consumers. Instead, we recommend the creation of a national standard that is narrowly tailored to address and prevent actual consumer harm. We stand willing and ready to work with Congress and the Department to that end.

* * *

We thank you for the opportunity to submit these comments, and look forward to working closely with the Department on these important issues. Please do not hesitate to contact me with questions at Stu Ingis at 202-344-4613.

American Advertising Federation
American Association of Advertising Agencies
ASAE
Association of National Advertisers
Coalition for Healthcare Communications
Direct Marketing Association
Electronic Retailing Association
Interactive Advertising Bureau
MPA -- The Association of Magazine Media
National Business Coalition on E-Commerce and Privacy
Newspaper Association of America
Performance Marketing Association
TechAmerica

²⁷ For example, the majority of states that enacted breach notification standards have appropriately defined the scope of data subject to breach notification to include an individual's first name or first initial with last name, in combination with certain enumerated sets of financial data. This definition should not be broadened to include other PII or non-PII, the breach of which could not lead to identity theft. In addition the "trigger" for notification should be limited to those breaches where the information breached presents a significant risk of identity theft to one or more individuals, subject to safe harbors present in the state laws for data that is publicly available or has been rendered unreadable or unusable by encryption or other methods (as such data would, by definition, not present a significant risk of identity theft).