January 28, 2011

Online Publishers Association
249 West 17th Street
New York, NY 10011

The Honorable Gary Locke
Secretary
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: Information Privacy and Innovation in the Internet Economy
Docket No. 101214614-0614-01

Dear Mr. Secretary:

The Online Publishers Association ("OPA") thanks you for the opportunity to provide comments on the Commerce Department's Green Paper, *Information Privacy and Innovation in the Internet Economy* (the "Green Paper"), released December 16, 2010.

OPA applauds the thoughtfulness and effort that the Department's Internet Policy Task Force devoted to the preparation of the Green Paper, and appreciates the Task Force's emphasis on formulating policies that will advance consumer privacy interests while preserving opportunities for online innovation and economic development. OPA agrees that voluntary codes of conduct are the most scalable, transparent, and flexible means of furthering these important goals. OPA also endorses the Green Paper's recommendation to create a Privacy Policy Office within the Commerce Department to coordinate multi-stakeholder discussions on privacy policy and spur the development of voluntary codes.

As the Task Force finalizes its analysis and recommendations, OPA hopes that it will consider the following observations from the unique perspective of the online publishing industry:

- The government does not need to codify Fair Information Practice Principles (FIPPs) at this time to produce meaningful and positive changes in data privacy practices;
- If FIPPs are adopted, however, the enacting law should preempt state laws, limit

enforcement jurisdiction to the Federal Trade Commission ("FTC"), and provide safe harbor protection for companies that comply with approved voluntary codes of conduct;

- Any FIPPs should exclude from consumer choice requirements the collection and use of data for certain commonly accepted practices, many of which were expressly excluded from the privacy framework recently endorsed by the FTC Staff. These practices include the collection and use of consumer information for first-party marketing, contextual advertising, internal operations, and newsgathering and editorial purposes.
- Responsibility for compliance with FIPPs in the online ecosystem should fall on the entities that collect information directly from consumers, regardless of whether those entities operate the websites visited by consumers at the moment of collection.

OPA and the Importance of Online Publishers to Consumers

OPA is a trade association dedicated to representing trusted online content providers before the advertising community, the press, the government and the public. It is the only trade association focused exclusively on the digital content business and its unique role in the future of media. OPA members include many of the Internet's most respected brands and they collectively reach an unduplicated audience of 172.5 million unique visitors, or 83% of the U.S. online population.[1]

OPA members provide an invaluable service to the public at a time when consumers increasingly look to the Internet as their primary source of news and information. Two years ago, the Internet surpassed print newspapers as consumers' primary source of both national and international news.[2] In 2010, OPA members invested more than half a billion dollars in the creation of high quality digital content, most of which they distributed free of charge.

Demand for quality digital content is increasing and content sites are fueling the growth of the Internet. A study conducted by OPA in conjunction with Nielsen Online concluded that content sites accounted for 42% of all time spent online by Web users in 2009, compared to 34% in 2003.[3] The average time that Web users spent on content sites on a monthly basis almost doubled during this period – increasing to nearly 7 hours per month from 3 hours and 42 minutes per month.[4] Web users spend more time interacting with content sites than they do with sites or applications in any other major online category, including Communications (e.g.., email services and instant messaging), Commerce (online shopping), Community (e.g., Facebook, MySpace and other social networking sites) and Search (e.g., Google search, Yahoo! search, Bing).[5]

---

[1] comScore Media Metrix, January 2010. Although the majority of OPA members operate consumer-oriented websites, they also reach millions of business users.
[2] *Post-Broadcast Democracy*, February 2009.
[3] Online Publishers Association, *Internet Activity Index* (IAI), September 17, 2009, *available at* http://www.online-publishers.org/newsletter.php?newsId=556&newsType=pr.
[4] *Id.*
[5] *Id.*

Although advertising is the lifeblood of the digital news, information, and entertainment provided by OPA members, the growth of online display advertising revenue has lagged far behind consumer demand for quality online content. Further, the value of online display ad inventory, measured on the industry-standard cost per thousand impressions ("CPM") basis, is far lower than the CPMs commanded by advertising in traditional media such as television and radio.[6] As a result, online publishers face enormous economic challenges.

To continue to provide quality journalism and other valuable content to consumers, OPA members must continue to offer innovative, effective and cost-efficient advertising services to marketers. These services require publishers to collect, use and disclose certain information about website visitors to their advertisers and service providers. Importantly, however, publishers know that their future ability to attract large audiences to their digital properties will depend on consumers' trust. As a result, OPA members are acutely aware of the need to respect consumers' privacy interests while pursuing their business objectives.

Mindful of the need to balance innovation and privacy interests, and based on the extensive experience of our well-respected members, OPA offers the following five observations for the Department to consider as it finalizes its policy proposals.

OPA Recommendations

1. OPA supports the creation of the Privacy Policy Office within the Department, as well as the Task Force's endorsement of voluntary codes of conduct as the best means of protecting consumer privacy while encouraging innovative business models.

OPA appreciates the Task Force's recognition of the online advertising industry's efforts to develop strong self-regulatory principles. As noted in the Green Paper, a coalition of key stakeholder organizations in the online advertising industry (including OPA) has spent the last two years developing a rigorous self-regulatory program to protect consumer privacy. This initiative already has produced a comprehensive set of privacy principles, a consumer education campaign, and a new standard icon designed to enable consumers to recognize targeted ads and exercise choice over the collection and use of information for behavioral advertising purposes.

While this effort continues to unfold, it represents a vigorous response to government appeals for self-regulatory action, and it deserves to be fully implemented and evaluated before policymakers consider new legislation. OPA applauds the Task Force for recognizing that the best way to promote meaningful privacy protections in a timely manner is to encourage

[6] Across media, advertising is commonly priced on the basis of CPM rates. Advertising in traditional media has been estimated to produce average CPMs of $4.54 (radio) to $10.25 (broadcast television), while non-premium Internet display advertising produces average CPMs of $0.60 to $1.10. Howard Beales, *Public Goods, Private Information, and Anonymous Transactions: Providing a Safe and Interesting Internet*, PowerPoint presentation given at the Law & Economics of Innovation Symposium at George Mason University School of Law, May 7, 2009 at 17 (citing Media Dynamics data from 2008).

continued self-regulatory efforts by private industry. To that end, OPA supports the Department's proposed creation of a Privacy Policy Office (PPO) to engage thought leaders from industry and other stakeholders and create a forum for the further development of recommended voluntary codes of conduct.

2. It is unnecessary to codify FIPPs at this time to foster meaningful protections for consumer privacy interests.

As noted above, industry already has made significant progress in the development of best practices and codes of conduct that will enhance consumer protections in the online advertising ecosystem. OPA believes that the multi-stakeholder discussion process envisioned by the Task Force will be sufficient to spur the development and adoption of voluntary codes of conduct that will enhance the public confidence necessary for full citizen participation in the Internet. Accordingly, OPA believes that formal enactment of such principles is unnecessary at this time. Premature legislative action would cement in place principles designed for practices and technologies that may become rapidly outmoded and threaten the ability of privacy frameworks to adapt to future changes and innovations.

3. If FIPPs are adopted, however, such principles should broadly preempt state law, limit enforcement jurisdiction to the FTC and provide safe harbor protection for companies that comply with approved codes of conduct.

As stated above, it is unnecessary to legislate FIPPs at this time and OPA strongly believes that self-regulation is a superior approach to addressing the privacy implications of data collection given the need to preserve opportunities for innovation and the enormous difficulty of attempting to shoehorn an infinite spectrum of data collection practices into a single rigid framework.

Nonetheless, should the Department call for the formal adoption of baseline FIPPs, however, OPA believes that any resulting legislation should include three features. First, the statute should broadly preempt state laws. The borderless nature of the Internet calls for a single set of rules rather than a patchwork of disparate state requirements.

Second, the statute should limit enforcement jurisdiction to the FTC, preclude private lawsuits, and rely on the FTC's current authority to proscribe deceptive practices under Section 5 of the Federal Trade Commission Act. Companies that subscribe to but violate a baseline set of FIPPs would be subject to enforcement actions by the FTC under the deception prong of its existing Section 5 authority. The FTC has been successful in influencing commercial data privacy and security practices by bringing such cases[7] and the related legal framework is well

[7] *See In re Sears Holding Mgmt. Corp.*, F.T.C. No. C-4264 (Aug. 31, 2009) (requiring Sears to cease data collection practices that FTC alleged were misrepresented or inadequately described in privacy notice); *In re Twitter, Inc.* F.T.C. No. 092-3093 (June 24, 2010) (requiring Twitter to adopt comprehensive privacy policy and audit program to settle allegations that Twitter misrepresented its security practices), *and*; *F.T.C. v. ControlScan, Inc.*, No. 10-CV-0532 (N.D. Ga. Feb. 25, 2010) (requiring ControlScan, a third-party validator of website privacy and security

understood by industry. Vesting enforcement jurisdiction in a single expert agency would promote predictability and ensure that decisions to prosecute cases that could significantly impact the development of the Internet economy are guided by the public interest.

Third, as proposed in the Green Paper, any legislation should create a safe harbor for companies that comply with approved voluntary codes of conduct. Novel issues of first impression should first be debated in self-regulatory organizations, not courtrooms, and self-regulatory tribunals should be the initial avenue for the enforcement of any FIPPs. As a general rule, public enforcement actions seeking monetary penalties should be permitted only after a company has violated a clearly-articulated requirement established through an approved and transparent self-regulatory process. Although these three features do not overcome OPA's strong preference for voluntary solutions in this area, they would mitigate (at least to some extent) the burdens of a prescriptive data privacy regime.

4. Any FIPPs should exclude from consumer choice requirements the collection and use of data for certain commonly accepted practices.

The Green Paper cites several examples of FIPPs that policymakers might consider adopting, and particularly focuses on the FIPPs currently employed by the Department of Homeland Security. These FIPPs call for entities to "seek individual consent for the collection, use, dissemination, and maintenance" of consumer data "to the extent practicable."[8] Such language fails to recognize several specific, commonly accepted practices that the FTC Staff recently concluded should be exempt from consumer choice requirements, either because consumer consent can be inferred from the context in which the information is collected or because it is not required to advance a substantial consumer privacy interest. Specifically, OPA recommends that any FIPPs adopted or endorsed by the Department should expressly exempt from consumer choice requirements each of the commonly accepted practices[9] recognized in the FTC Staff's Privacy Report,[10] as well as certain other practices as discussed below.

---

protections, to pay equitable relief of $750,000, notify sites to remove security "seals" awarded by ControlScan, and comply with additional regulatory oversight after alleging that ControlScan misrepresented its verification efforts to consumers and awarded security "seals" to sites without sufficient review.)

[8] Green Paper at 25-26.

[9] OPA agrees in principle that "commonly accepted practices" should generally be exempt from consumer choice requirements. OPA believes, however, that common acceptance by consumers should not be a prerequisite for the exemption of a particular data practice. A test that focused on "common acceptance" alone could not keep pace with the marketplace without stifling innovation. Developments in technology and business models may give rise to many innocuous data collection practices that do not materially affect consumer privacy interests. Such practices should qualify for exemptions from choice requirements whether or not consumers lacking a technical background commonly understand them.

[10] FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, (the "FTC Privacy Report") released on December 1, 2010.

A. First-Party Marketing.

OPA shares the FTC Staff's belief that collection and use of information for marketing purposes by companies that stand in a direct, first-party relationship with consumers have very different privacy implications than similar data collection and use by third parties. OPA thus endorses the FTC Privacy Report's conclusion that such first-party collection and use cases should be exempt from consumer choice requirements as "commonly accepted practices."[11] In a direct first-party relationship, consumers are more likely to understand why they received tailored recommendations and are in a better position to raise concerns about the use of information about them, or to exercise choice by taking their business elsewhere.

Online publishers share a direct and trusted relationship with visitors to their websites. In the context of this relationship, OPA members sometimes collect and use information to target and deliver the online advertising that subsidizes production of quality digital content. While most advertising on OPA members' sites is contextual, some of this advertising is first-party behavioral or "semantic" advertising. Such advertising uses information collected from visitors' past interactions with a member's website – typically collected anonymously – to deliver ads tailored to the inferred preferences and interests of visitors. For example, if a website visitor views articles about NFL football games or searches the site for football coverage, he or she is unlikely to be surprised to receive, while on the same site, marketing for a commemorative Super Bowl coffee table book. This is true even if the ad for the coffee table book were targeted based on the visitor's activity within the site during a prior browsing session.

The targeting of a behavioral advertisement by a first-party site is analogous to a sales clerk at a men's clothing store who recognizes a repeat customer and makes wardrobe suggestions based on the customer's past preferences for size, color, and designers. The same dynamic is involved when Amazon.com suggests books that a consumer might be interested in reading based on titles that the consumer previously purchased. Given the direct relationship between the consumer and the merchant, the consumer naturally understands that the merchant is in a position to recognize and remember its customers' preferences and is not surprised when the merchant uses that information to suggest future purchases. Accordingly, OPA urges the Department to exempt from any choice principle it may adopt the collection of data from a consumer with whom the company interacts directly for the purposes of marketing to that consumer.

B. Operational Purposes and Service Providers.

A broad and flexible "operational purposes" exemption to the proposed consumer choice requirements is also critical to the online publishing model. Such an exemption is necessary for publishers to continue to operate and improve their websites, provide customized content to consumers, and perform core functions necessary for the sale and delivery of advertising that does not involve third-party behavioral targeting. For example, publishers need to collect and

[11] FTC Privacy Report at 54-55, *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

use visitor information to create and personalize content over multiple browsing sessions, to store user preferences and login IDs, to report industry-standard metrics, and to identify needs for improvement in website design and user experience. Cookies, IP addresses, and device IDs also are used to count the number of individuals who use particular browser software, operating systems, screen resolution, and other system settings. This information is used in turn to optimize both editorial and advertising content.

Online publishers frequently also rely on third-party service providers to process, store and analyze user information on their behalf. OPA accordingly requests that the Department create an internal operational purposes exemption from any choice principle it may adopt, as well as an exemption permitting companies to share information with service providers for purposes of carrying out operational, first-party marketing or other exempt functions on their behalf. Both exemptions are critical to the ability of publishers to monetize their investment in digital content and provide a high-quality experience to consumers; both exemptions were expressly recommended in the recent FTC Privacy Report.[12]

C. Contextual Advertising.

OPA also strongly agrees with the FTC Staff's decision that the collection and use of information for "online contextual advertising should fall within the 'commonly accepted practices category'" that is exempt from consumer choice requirements.[13] Contextual advertisements are targeted based on the content of the webpage on which they are displayed or the content of a single search query, rather than on the interests of consumers inferred from their browsing history over time.[14] The information necessary to target contextual advertising is very limited and the use of that information is ephemeral.

Moreover, as the FTC Staff noted, contextual advertising "provides greater transparency than other forms of behavioral advertising, is more likely to be consistent with consumer expectations, and presents minimal privacy intrusion when weighed against the potential benefits to consumers. . . ."[15] Such benefits including "free content – made possible by the revenue from the sale of the advertisements – and receipt of contextually relevant ads that consumers may value."[16] OPA members rely heavily on revenue from the sale of contextual advertising to support their operations and we urge the Department to exempt the collection and use of consumer data for contextual advertising purposes from any choice principle it may endorse.

---

[12] *Id.*
[13] FTC Privacy Report at 55, n.134.
[14] For example, a website might serve an advertisement for a discounted vacation cruise package to visitors of a webpage devoted to budget travel in the Caribbean as the advertiser assumes that consumers who are interested in articles about budget travel are more likely than the average consumer to be interested in a discounted cruise offer.
[15] FTC Staff, *Self-Regulatory Principles for Online Behavioral Advertising* (February, 2009), at 11, *available at* http://www2.ftc.gov/opa/2009/02/behavad.shtm.
[16] *Id*

D. Business-to-Business Marketing.

Choice requirements in any consumer privacy protection scheme should also exclude the collection and use of contact information for business-to-business ("B-to-B") marketing and communications purposes. Business contact information is analogous to information printed on a business card or professional directory listing. Such information identifies or relates to an individual in his or her capacity as an employee or representative of a commercial enterprise, rather than as a consumer. The collection and use of information for B-to-B marketing purposes are commonly accepted practices in both the online and offline spheres. These practices do not implicate consumer privacy interests and accordingly should be excluded from the FIPPs contemplated by the Department, consistent with parallel B-to-B exceptions in other federal marketing privacy schemes such as the FTC's Telemarketing Sales Rule.[17]

E. Newsgathering and Editorial Expression.

To avoid treading on First Amendment rights, any choice or consent requirement included in any FIPPs endorsed by the Department should clearly exclude the collection of information about consumers for newsgathering, political commentary and other forms of editorial expression that are protected as core speech. Without such appropriate limitations, a privacy regime applicable to the collection of data about individuals could be construed to require an online news service or other commercial media organization to obtain the prior consent of a political candidate before collecting and reporting facts relating to his or her health, religious views, or financial history. Such requirements obviously would be unconstitutional. Accordingly, to prevent the subjects of news stories from attempting to use the Department's analysis to threaten news organizations and thereby chill speech, OPA requests that the Department clarify that choice requirements should not apply to information collected or used for purposes of newsgathering, editorial comment, or the dissemination of information or opinion about matters of public concern.

5. Any online privacy protection framework should limit compliance responsibilities to the entities that actually collect information, regardless of whether those entities operate the websites visited at the moment of collection.

A common misunderstanding is that website publishers control and are privy to all of the information collection that occurs through their sites. This is not the case. Much of the information collected from website users for third-party marketing purposes is collected by third parties themselves through processes that publishers do not control and for purposes that they do not condone. Advertisements that appear on websites frequently are delivered to visitors' browsers by servers controlled by advertisers or their agencies, as opposed to the website publisher. The advertiser or agency can use these communications without the publisher's involvement to deploy cookies or other tracking technologies and to collect information directly

[17] 16 CFR § 310.6(b)(7) (exempting all "calls between a telemarketer and any business, except calls to induce the retail sale of nondurable office or cleaning supplies.")

from visitors.[18] We also note that advertisers and their agencies often have superior bargaining power over even the largest publishers and frequently refuse to negotiate limitations on their use of data collected through ad spaces.

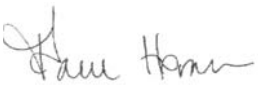
A recent study conducted by Krux Digital found that these tracking technologies have fueled a substantial and growing "gray market" for the harvesting and reuse of consumer data. Activity in this market shifts ad spending away from premium publishers towards audience-based buying via secondary channels and parties unknown to the consumer. For example, looking at the top fifty websites nationwide, the Krux Digital analysts and a team of Stanford economists found that data skimming and data theft via third-party data collectors result in at least $850 million in lost revenue annually for premium publishers.[19]

For all of these reasons, a privacy policy framework that treats website publishers as the "guarantors" of their advertisers' compliance with consumer choice requirements would create untenable burdens for the online publishing industry and would not effectively advance the Department's goals. Accordingly, OPA urges the Department to acknowledge that responsibility for compliance with consumer choice requirements should be assigned solely to the entity that directly collects the relevant information, regardless of whether that entity operates the website that a user is visiting at the time of collection.

* * *

OPA again applauds the work of the Task Force in studying the issues surrounding the collection of consumer information – both from the perspective of protecting consumer privacy and encouraging online innovation – and looks forward to working with the Department to answer any questions regarding the online publishing industry.

Sincerely,



Pam Horan
President
Online Publishers Association
212.204.1487

[18] Even in circumstances where an ad resides on a publisher's ad server, the advertiser can embed in the ad a pixel tag that allows the advertiser to collect information directly from a user's computer using remote servers that the website publisher does not control. In many cases advertisers use beacons transmitted in response to ads to redirect consumer browsers to "fourth-party" servers operated by data companies, optimizers or other demand-side service providers that in turn can insert and read their own tracking cookies on the consumer's browser.

[19] Summary and detail findings from the Krux Cross-Industry Study, as well as the companion revenue exposure report, can be found at www.cis.kruxdigital.com.