



February 17, 2011
Online Publishers Association
249 West 17th Street
New York, NY 10011

Donald S. Clark
Secretary
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: FTC Staff Preliminary Report on “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers” – File No. P095416

Dear Mr. Secretary:

The Online Publishers Association (“OPA”) appreciates the opportunity to comment on the preliminary FTC Staff Report on “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers” (the “Preliminary Report”) released on December 1, 2010.

OPA applauds the Staff’s thoughtful approach to the issues discussed in the Preliminary Report, and especially appreciates the Staff’s recognition that many uses of audience data are essential to delivering a quality web experience to consumers and should be excluded from the choice requirements of the proposed privacy framework. OPA also appreciates the Staff’s recognition that consumers hold different expectations of privacy with respect to information collection in the context of a direct first-party relationship with a website publisher than they do with respect to information collection by third parties in the online ecosystem.

OPA hopes that the framework proposed by the Staff will be used to inform further efforts to develop and strengthen self-regulatory principles and will not be perceived as an implicit call for prescriptive legislation. OPA strongly believes that self-regulatory principles and voluntary codes of conduct are the most scalable, flexible, and effective means of advancing consumer privacy interests while preserving opportunities for online innovation and economic development in an industry that is vital to the public interest.

As the Commission Staff works to finalize its report, we hope that it will give careful consideration to five observations offered from the perspective of the online publishing industry:

249 West 17th St
New York, NY 10011
online-publishers.org

- The proposed exemptions for first-party marketing, contextual advertising, and internal operational purposes are vital to online publishers and should be preserved in the final report;
- Any self-regulatory framework should place responsibility for compliance with choice requirements on the entity that actually collects consumer data, not the website being visited at the moment of collection;
- Any framework should permit an online publisher to condition access to its site on visitors' acceptance of the publisher's information practices;
- Any framework should harmonize any choice rights granted to individual consumers with the browser-based nature of the Internet; and
- Any framework should expressly exempt the collection, use, and disclosure of information for newsgathering and editorial purposes.

I. 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. We are the only trade association focused exclusively on the digital content business and its unique role in the future of media. Our 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. In 2008, the Internet surpassed newspapers as consumers' primary source of both national and international news.² Last year, OPA members invested more than half a billion dollars in the creation of high quality digital content, most of which they distribute 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 ranked as the #1 source of time spent online in 2010, accounting for 37%, compared to 34% in 2003.³ The average time that Web users spend on content sites on a monthly basis almost doubled during this period – increasing to 6 hours and 28 minutes per month in 2010 from 3 hours and 42 minutes per month in 2003.⁴ Web users spend more time interacting with content sites than they do with sites or applications in any other major online category, including Communications (i.e., 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.

² *Post-Broadcast Democracy*, February 2009.

³ Online Publishers Association, *Internet Activity Index (IAI)*, 2010, available at <http://www.online-publishers.org/internet-activity-index?dt=sharetime#end>.

⁴ *Id.*

⁵ *Id.*

Although advertising is the economic engine that supports 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 electronic 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 consumer 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 observations in response to the Preliminary Report.

II. OPA Recommendations

1. The Proposed Exemptions for First-Party Marketing, Contextual Advertising and Internal Operational Purposes Are Vital to Online Publishers and Should Be Preserved in the Final Report.

A. First-party Marketing.

OPA shares the Staff’s belief that collection and use of audience 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 Staff’s conclusion that such first-party collection and use cases should be exempt from consumer choice requirements as “commonly accepted practices.”⁷ 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 use of information about them, or to exercise choice by taking their business elsewhere.

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).

⁷ Although OPA agrees in principle that “commonly accepted practices” should generally be exempt from consumer choice requirements, widespread consumer awareness of a particular data practice should not be treated as a prerequisite for such an exemption. Developments in technology and business models may give rise to various innocuous data collection practices that do not materially affect consumer privacy interests and therefore should not be subject to consumer choice requirements regardless of whether they are matters of common knowledge among consumers.

These considerations sharply distinguish publishers' first-party data collection practices from the third-party behavioral advertising practices that have been the focus of much of the policy debate surrounding online privacy. As the FTC Staff has previously noted, when behavioral advertising involves sharing data with ad networks or other third parties, the user "may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites.⁸ Moreover, he may not know whom to contact to register his concerns or how to avoid the practice."⁹

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 was 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 strongly supports the Staff's proposed exemption for the collection of data from a consumer with whom the company interacts directly for the purposes of marketing to that consumer.

Such an exemption is essential to protect the ability of online publishers to continue to monetize their investments in content through the delivery of standard display advertising. Although the cost of producing quality content for online distribution is equivalent to the cost of producing quality content for distribution in print or through the broadcast media, as noted above, the CPMs paid for online advertising have been far lower than the CPMs paid for broadcast and print advertising.¹⁰ Regulators should take pains to avoid inadvertently injecting additional uncertainty into the business models that support creation of quality content. Accordingly, to guide and educate policymakers, OPA urges the Staff to expressly acknowledge in the final report that the delivery of *all* online advertising – not just behaviorally-targeted

⁸ FTC Staff, *Self-Regulatory Principles for Online Behavioral Advertising* (February, 2009) "2009 OBA Principles"), at 11, available at <http://www2.ftc.gov/opa/2009/02/behavad.shtml>

⁹ *Id.* at 27.

¹⁰ See note 6 above.

advertising – relies to some extent on the collection and use of IP addresses, cookie information and other information about users, and that such collection and use is covered by the first-party marketing exemption.

As a result of these economic realities, providing a blanket choice to block collection of all such information for advertising purposes, as proposed in the Preliminary Report, would be devastating to the basic business model that delivers quality content to consumers. For example, online publishers rely on IP address and cookie information to perform many advertising functions such as:

- executing online campaigns in accordance with contractual requirements (such as geographical requirements and category or brand exclusivity commitments);
- capping the frequency with which an individual ad is displayed – a feature that benefits both advertisers and website users;
- complying with legal requirements (for example, it may not be lawful to advertise a pharmaceutical product approved in the U.S. to audience members in the U.K. or vice versa – IP addresses are used to limit campaigns to particular countries or regions);
- preventing click fraud; and
- synchronizing and sequencing creative content, thereby enabling advertisers to “tell a story” through campaign elements that must unfold in a logical order.

Without a robust first-party marketing exemption (and related exemptions for operational purposes and sharing with service providers), the choice features of the proposed privacy framework could operate as a “kill switch” for online advertising. Given the pervasive and inextricable connections between user information and online advertising, the establishment of a choice mechanism to block collection and use of data for any advertising purpose would be tantamount to creating a right to receive news and information content without advertising. Such a provision would be like requiring television stations to offer programming uninterrupted by commercials to any viewers who found commercials annoying.

On page 56 of the Preliminary Report, the Staff asks whether a first-party marketing exemption should be limited to the context in which particular data is collected. For example, the Staff asks whether a website operator should be able to rely on the first-party marketing exemption to use information that it collects directly from a consumer online to send communications to the consumer through offline marketing channels, such as postal mail, email or text messages. OPA sees no reason to limit the first-party marketing exemption to the use of data to communicate with consumers in the same channel in which the data was collected. Across all contexts and media, the key consideration is whether the consumers knows which marketer is collecting the data. As long as the consumer understands which marketer is collecting information about his or her preferences, it should not matter, from a privacy perspective, whether the marketer uses online or offline media to deliver a follow-up offer to the consumer.

Contextual limitations on first party marketing could unduly restrict first-party marketing offers that consumers may value and, in any case, can reasonably expect. Moreover, such

limitations are unnecessary in light of existing laws and self-regulatory standards that already require first-party marketers to obtain consent or provide choice when communicating with consumers using channels such as telemarketing, faxing, direct mail, email marketing or text messaging. For example, the Direct Marketing Association's Mail Preference Service is used by millions of consumers to limit the delivery of promotional mail to their homes¹¹ and consumers also have rights under U.S. Postal Service programs to block unwanted commercial mailings from a particular sender.¹² The CAN-SPAM Act enables consumers to remove their email addresses from the marketing list of any sender with the click of a mouse.¹³ The FTC's Telemarketing Sales Rule¹⁴ and parallel state laws similarly empower consumers to prevent telephone solicitations, even from companies with which they previously formed an established business relationship. The Telephone Consumer Protection Act generally prohibits automated delivery of any text message to a consumer without the recipient's prior express permission¹⁵ and the Mobile Marketing Association's widely-followed guidelines for mobile message campaigns require every commercial SMS message to include an unsubscribe mechanism.¹⁶

Staff also requests comment on whether "marketing to consumers by commonly-branded" affiliates should be considered first-party marketing.¹⁷ OPA believes that the first-party marketing exemption should permit the exchange and use of data among corporate affiliates that share a common brand or otherwise effectively disclose their affiliation relationships and follow substantially similar privacy policies. Affiliated websites share many resources – including audience data – to improve the efficiency of their operations. Moreover, it is not uncommon for features of a single website to be provided by separate but affiliated companies. The framework accordingly should include affiliate-sharing within the scope of the first-party exemption to avoid disrupting the important operating efficiencies that exist in families of affiliated websites.

The standard for affiliate sharing should not, however, focus exclusively on whether affiliated sites have the same brand identity because sites may effectively communicate their affiliation relationships to consumers through direct disclosures or in other ways. OPA accordingly suggests the Staff adopt a standard for affiliate sharing that permits the exchange of consumer data for marketing purposes between entities that (1) are affiliated by common majority ownership or management control, (2) adhere to substantially similar policies with respect to use and disclosure of consumer information and (3) disclose their affiliation through common branding or other clear and conspicuous means.

¹¹ See https://www.dmachoice.org/dma/static/learn_more.jspDMAchoice.org.

¹² See 39 U.S.C. § 3008 and Postal Service Form 1500 available at <http://www.usps.com/cpim/ftp/bulletin/1998/pb21977.pdf>.

¹³ 15 U.S.C. § 7704(a)(4).

¹⁴ 16 CFR § 310.4.

¹⁵ 47 U.S.C. § 227(b)(1)(A)(iii).

¹⁶ Mobile Marketing Association Global Code of Conduct available at <http://mmaglobal.com/policies> ("Mobile Marketers must implement a simple termination (opt-out) process so that users can stop receiving messages, and users must be able to exercise their opt-out choice from any message.").

¹⁷ Preliminary Report at 57.

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. The 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 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 resolutions, and other system settings. This information is used in turn to optimize both editorial and advertising content.

Online publishers frequently rely on third-party service providers to process, store, and analyze user information on their behalf. OPA accordingly commends the Staff for recognizing the need for an operational purposes exemption, 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 and they should be retained in the final privacy report.

C. Contextual Advertising.

OPA also strongly agrees with the Staff’s decision to include contextual advertising in the “commonly accepted practices” category. 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.¹⁸ The information necessary to target contextual advertising is very limited and the use of that information is ephemeral. Moreover, as the Staff noted in its 2009 OBA Principles, 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” including “free content – made possible by the revenue from the sale of the advertisements – and receipt of contextually relevant ads that consumers may value.”¹⁹ OPA members rely heavily on revenue from the sale of contextual advertising to support their operations and we urge the Staff to retain this exemption in the final report.

¹⁸ For example, an advertisement for a discounted vacation cruise package may be served to visitors to a webpage devoted to budget travel in the Caribbean because 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.

¹⁹ *Id.*

D. Other Commonly Accepted Practices: B-to-B Information Collection.

The Staff also requests comment on whether the list of proposed “commonly accepted practices” set forth in Section V(C)(1) of the Draft Report is too narrow. One practice that the Staff should consider adding to the list of exemptions from the framework’s choice requirements is the collection and use of contact information for business-to-business marketing and communications purposes.²⁰ 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 is a commonly accepted practice in both the online and offline spheres. Such B-to-B information practices do not implicate consumer privacy interests and should be excluded from the framework, consistent with parallel B-to-B exceptions in other federal marketing privacy schemes such as the FTC’s Telemarketing Sales Rule.²¹

2. Any Self-Regulatory Framework Should Place Responsibility for Compliance With Choice Requirements on the Entity That Collects Information from Web Users, Whether or Not the Collector Operates the Website Visited at the Moment of Collection.

In the Preliminary Report, the Staff requests comment on its appeal for creation of a standardized consumer choice mechanism for online behavioral advertising (sometimes known as a “Do Not Track” system). The Staff recommends a browser-based setting, similar to a persistent cookie, that would alert sites of a consumer’s preferences relating to tracking of data, backed by an enforceable requirement for sites to honor such consumer choices. It is difficult for OPA members to evaluate the feasibility of the Staff’s Do Not Track proposal without knowing more about specific technology that the Staff envisions for its implementation. Regardless of its technological underpinnings, however, any self-regulatory framework for online privacy should assign compliance responsibilities to each party in the ecosystem that collects information from consumers’ browsers and should not treat publishers as the “guarantors” of data collection events and practices that they do not control.

A common misunderstanding is that website publishers control and are privy to all of the information collection that occurs through their sites. In reality, much of the information collected from website users for third-party marketing purposes is collected by third parties through processes that publishers do not control. 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 to deploy cookies or other tracking technologies without the publisher’s involvement and to collect information directly from visitors that the publisher never sees.

²⁰ Although the majority of OPA members operate consumer-oriented websites, they also reach millions of business users.

²¹ 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.”)

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.

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. Even if they do agree to limitations on the use of visitor data, it is difficult for publishers to detect breaches of these commitments or to distinguish benign and legitimate purposes for third-party data collection from purposes that may involve behavioral profiling and raise privacy concerns.

With considerable effort, publishers can use test browsers to detect the trail of cookies that are left when users navigate through their sites but they can glean little information from the values contained in these files and they cannot discern what data is actually being harvested, how it is being used by the collector, or whether it is being disclosed to other entities downstream.²²

Given these realities, a policy framework that treats website publishers as the "guarantors" of their advertisers' compliance with consumer choice requirements would create untenable burdens and would not effectively advance the Staff's goals.

Such an approach also would be inconsistent with the allocation of duties and liabilities in analogous consumer protection law contexts, such as product liability and false advertising. For example, numerous courts have held that newspapers and other media publishers have no duty to investigate the advertisements they print.²³ These holdings are based on recognition that

²² A recent study conducted by Krux Digital found that there is a substantial and growing "gray market" for the harvesting and reuse of consumer data from publisher websites. Activity in this market shifts ad spending away from online publishers towards audience-based buying via secondary channels and parties unknown to the consumer. The study analyzed the categories of companies that actively collect data from 50 top publisher websites and examined how those companies collect such data. Krux observed 167 different companies collecting data across the 50 publisher sites, with an average of about 10 and as many as 40 data collection events (defined as the setting, reference, or modification of a cookie) occurring in just one page view. Thirty-one percent of all data collection observed during the study was enabled by parties other than the publishers, few of which appeared to be collecting data in the publishers' interests. A summary and detailed findings from the Krux Cross-Industry Study can be found on the company's website at www.cis.kruxdigital.com.

²³ *Pittman v. Dow Jones & Co.*, 662 F. Supp. 921, 922 (E.D. La. 1987) ("[A] newspaper has no duty, whether by way of tort or contract, to investigate the accuracy of advertisements placed with it which are directed to the general public, unless the newspaper undertakes to guarantee the soundness of the products advertised."), *aff'd*, 834 F.2d 1171 (5th Cir. 1987) (per curiam); *Walters v. Seventeen Magazine*, 241 Cal. Rptr. 101, 103 (Cal. Ct. App. 1987) ("[W]e are loathe to create a new tort of negligently failing to investigate the safety of an advertised product. Such a tort would require publications to maintain huge staffs scrutinizing and testing each product offered. The enormous cost of such groups, along with skyrocketing insurance rates, would deter many magazines from accepting advertising, hastening their demise from lack of revenue."); *Yugas v. Mudge*, 322 A.2d 824, 825 (N.J. Super. Ct. App. Div. 1974) ("[N]o such legal duty to investigate [advertisements] rests upon respondent [,the publisher of *Popular Mechanics Magazine*,] unless it undertakes to guarantee, warrant or endorse the product. To impose the suggested broad legal duty upon publishers of nationally circulated magazines, newspapers and other publications,

imposing obligations on publishers to police their advertisers would both unduly restrict the flow of commercial speech and indirectly threaten the core, noncommercial speech that is supported by the sale of advertising.²⁴

These considerations do not suggest that online publishers should avoid responsibility for their own information practices. However, they do suggest that the final Staff report should squarely assign responsibility for compliance with consumer choice requirements to the entity that actually collects the relevant information, regardless of whether that entity operates the website that a user is visiting at the time of collection.

3. Any Framework Should Permit Online Publishers to Condition Access to Their Sites On Visitors' Acceptance of Their Information Practices.

Staff requests comment on whether and in what circumstances it is appropriate to offer a choice to prevent the collection or use of visitor data as a “take it or leave it” proposition, whereby a consumer’s use of a website, product or service constitutes consent to the company’s information practices. Online publishers should have the right to offer their content and services on any lawful terms that are explicitly communicated to consumers and withhold access from those who do not agree to such terms. To require otherwise would burden publishers’ First Amendment speech with free riders who enjoy the benefits of access to valuable content without providing fair value in exchange.

Moreover, with appropriate transparency, such “take it or leave it” propositions should not, as a general rule, raise significant policy concerns. The most powerful choice a consumer can exercise with respect to online privacy is the choice to stop patronizing a company whose data collection practices the consumer finds objectionable. Accordingly, with appropriate levels of disclosure, privacy practices in highly-competitive industries such as online publishing should be largely self-correcting. Trusted brands will be rewarded in an environment where well-informed consumers can “vote with their feet.”

At the same time, publishers should be allowed to compete on the basis of privacy and experiment with different business models within an open media marketplace where consumers have countless online content choices. By contrast, default rules that prevent fair value exchanges of digital content for user data could harm consumer welfare by reducing incentives for some publishers to invest in the production of content and/or creating incentives for publishers to charge or charge more for content that they would otherwise make available for free or at a lower cost.

would not only be impractical and unrealistic, but would have a staggering adverse effect on the commercial world and our economic system.”); *Goldstein v. Garlick*, 318 N.Y.S.2d 370, 374 (N.Y. Sup. Ct. 1971) (“Nor should the onerous burden be placed upon newspapers under ordinary circumstances to conduct investigations in order to determine the effect of a questioned advertisement.”).

²⁴ See, e.g., *Eimann v. Soldier of Fortune Magazine, Inc.*, 880 F. 2d 830, 837 (5th Cir. 1989) (“[T]he publication’s editorial content would surely feel the economic crunch from the loss of revenue that would result if publishers were required to reject all ambiguous advertisements.”).

4. Any Framework Should Harmonize Any Choice Rights Granted to Individual Consumers with the Browser-based Nature of the Internet.

Although the proposed framework would create choice rights for individual consumers, publishers usually associate information with a particular browser or device ID, as opposed to a particular individual. Individual consumers may use many different browsers and devices and any device or browser may be used by multiple individuals. For example, if an individual uses more than one computer, or purchases a new computer, or installs a new browser, or clears all of the cookies from his or her browser after exercising an opt-out choice, a publisher ordinarily could not recognize and honor that individual's previously expressed privacy preference.

OPA accordingly requests that the final report expressly recognize that an entity subject to the proposed framework will not be liable for failing to honor a choice made by an individual if such failure is attributable to the covered entity's inability, through reasonable technical means, to recognize a particular web browser or device that is used by the individual who exercised the choice. Similarly, the final report should clarify that when an individual consumer consents to the collection, use or disclosure of information covered by the framework, that consent will be effective as to all other individuals who use the same browser or device. Such an approach is consistent with other federal privacy protection schemes such as the national do-not-call rules, which frame the obligations of telemarketers in terms of their ability to contact a particular residential telephone number, rather than their rights to contact a particular individual who uses the number.

5. Any Framework Should Expressly Exempt the Collection, Use and Disclosure of Information for Newsgathering and Editorial Purposes.

Although presumably not intended to apply in these circumstances, the proposed framework does not clearly exclude the collection of information about consumers for newsgathering, political commentary and other forms of editorial expression that are protected as core speech under the First Amendment. Instead, the Preliminary Report emphasizes that the framework envisioned by the Staff generally applies to all "commercial data collection and use . . .".²⁵ Accordingly, under a broad reading, the proposed framework applicable to the collection of consumer data could be construed to prohibit an online news service or other commercial media organization²⁶ from gathering and reporting facts about the gowns worn by celebrities at the annual Oscars ceremony without providing notice and choice to the actresses featured in this coverage.²⁷

²⁵ Preliminary Report at 57.

²⁶ It is plain that speech in a form that is sold for profit is entitled to full First Amendment protection. *See Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 482, 109 S.Ct. 3028, 106 L.Ed.2d 388 (1989) ("Some of our most valued forms of fully protected speech are uttered for a profit.")

²⁷ It is well established that news and feature coverage of the fashion choices and purchasing behavior of celebrities constitutes projected expression regarding matters of public interest as we "copy their mannerisms, their styles, their modes of conversation and of consumption." *Comedy III Prods. v. Gary Saderup, Inc.*, 21 P.3d 797, 803 (Cal. 2001).

More troublingly, the framework might be construed to require a news organization to obtain the “enhanced consent” of a political candidate before collecting and reporting facts relating to that candidate’s medical or financial history. Such requirements obviously would be unconstitutional and could not have been intended by the Staff. Accordingly, to prevent the subjects of news stories from attempting to use any ambiguity in the final report to threaten news organizations and thereby chill speech, OPA requests that the Staff clarify in the final report that the framework does 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.

* * *

OPA commends the FTC Staff for taking the time to study the privacy issues surrounding the collection of information from consumers and looks forward to working collaboratively with the Staff to answer any questions it may have regarding the online publishing industry.

Sincerely,

Pam Horan
President
Online Publishers Association
212.204.1487