ICSC

Internet Content Syndication Council

A White Paper, July 2011

A 'NO TRACKING' MODEL OF ONLINE ADVERTISING: CONTENT SYNDICATION

Acknowledgements:

The Internet Content Syndication Council would like to thank the following companies for contributing their valuable insights. We invite reader comment on this white paper and future participation in the council. Thank you in advance.

For the Council,

Andrew Susman
Chairman, ICSC
President, Studio One Networks

Abbey Content Enterprises, Inc.
Air2web
Ancestry.com
Answers Media, Inc.
Anystream Solution
The Associated Press
AT&T
Atomcom LLC
Automattic
Boston Media Consultants
Brightcove
Canoe.ca
Carat
Cars.com
CBS Television Stations
Cliffhouse Media
Comcast/ iVillage Properties
COS Productions
Flixya
Grab Networks
HealthDay News
Hitwise
Howdini
iCrossing
Idea Integration Corp.
IDG
India Today
Mochila
National Association of Television Program Executives
New York Times/ About.com
Nielsen
Pheedo
The Platform
Prisma Press
SI Video Sales Group
Sony BMG
SportzVentures
Spraci
Studio One Networks
Tie Kinetix
Thomson Reuters
Travelscream Technologies
The Tribune Company

EXECUTIVE SUMMARY:

Internet Content Syndication offers online advertisers a highly effective means of reaching target audiences on a large scale without relying on behavioral targeting. As consumers' concern about the privacy of their online activities is now widespread, the savvy advertiser may well want to consider employing "non-tracking" models of online marketing to supplement or replace behavioral targeting.

This is especially so in light of the intense scrutiny behavioral targeting is facing on multiple fronts in Washington, D.C. In the past six months, there has been a flurry of privacy proposals: several in both houses of Congress; a Department of Commerce Green Paper on data privacy; and, most prominently, a Federal Trade Commission (FTC) Staff Report that recommends the creation of a "Do Not Track" system aimed specifically at behavioral targeting of consumers. It seems likely that some form of privacy legislation and increased regulation will be enacted this year or next.

As a result, advertisers who have been relying on behavioral targeting may wish to adjust their advertising strategies. When they look for alternatives, they will find that Internet Content Syndication offers a highly effective way of targeting audiences — while avoiding consumer privacy concerns.

Content Syndication: A "Do Not Track" Marketing Solution

Internet Content Syndication is defined as "the controlled placement of the same content on multiple partnering Internet destinations." That is, the content itself is placed by a syndicator on a network of pre-screened affinity destinations, rather than being linked back to a single site. The distribution of the content across multiple sites enables a cost-effective aggregation of larger audiences than would be possible with just a single site. It is a viable way of countering the fragmentation of audiences caused by the continued growth of Internet destinations, which can now be counted in hundreds of millions.

There are a variety of distribution and revenue-generating strategies used by content syndicators. The most typical arrangement is for the syndicator to negotiate agreements with their destination partners to carry a sponsor's advertisement or video embedded within the syndicated content. This means that the advertiser is assured that its ad always appears within an appropriate environment because the content is the same on all the websites in which it appears. It can be thought of as the ultimate in safe contextual advertising.

Online Privacy: An Issue Whose Time Has Come?

Online privacy issues have certainly gotten the attention of Congress. Several bills dealing with various aspects of privacy have already been introduced this session, including:

Sen. Patrick Leahy (Chair of the Judiciary Committee) announced in February the creation of a Privacy and Technology Subcommittee to be chaired by Sen. Al Franken.

In April, Sens. John Kerry and John McCain introduced the Commercial Privacy Bill of Rights, to "allow people to have a say in whether they want their information to be used."

Reps. Cliff Stearns, Jim Matheson, Brian Bilbray and Don Manzullo introduced a bill in the House, also in April, giving Web users information and control over what data Internet companies collect about them and how they are tracked and calls for the FTC to approve a policing mechanism to ensure compliance.

Sen. Jay Rockefeller (Chair of the Commerce Committee) introduced the Do Not Track Act of 2011 in May, tasking the FTC with "creating and implementing a 'Do Not Track' mechanism for users."

Reps. Edward Markey and Joe Barton introduced a "Do Not Track Kids Act of 2011" in May which would expand and modernize the Children's Online Privacy Protection Act (COPPA) and create new privacy protections for all minors.

An analysis of these bills can be found in Appendix I.

Another sign that Congress is serious about addressing online privacy is that Committees in both Houses have already held hearings: the Senate Committee on Commerce, Science and Transportation on June 29 and the Telecom Subcommittee of the House Energy and Commerce Committee on July 14. (See Appendix II.)

In December 2010, the Department of Commerce released a Green Paper, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," which recommended the creation of a "Center for Privacy Policy" and called for increased FTC enforcement of current regulations, as well as introducing possible new ones.

In nearly every privacy bill, including the Department of Commerce paper, the FTC is called upon to take the lead on online privacy. In December 2010, the FTC released a Staff Report on protecting consumer online privacy, which focused in some detail on the creation of a "Do Not Track" system. Because the FTC is likely to be the lead agency in implementing Congressional privacy regulations, this paper looks at the implications of this report for marketers.

The FTC Staff Report on Privacy

FTC issued its preliminary staff report, "**Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,**" in December 2010. The report noted that the FTC has long concerned itself with consumers' privacy rights, dating back to the 1970s with the Fair Credit Reporting Act. It expressed concern that technological advances in data collection and analysis techniques may be putting consumer privacy at risk, even as it confers significant benefits in the form of new products and services.

The Commission is particularly concerned that consumers are often unaware of the fact that an "unprecedented" amount of data is collected about them and the degree to which their online behavior is tracked. It concludes that they have a general "lack of understanding and ability to make informed choices about the collection and use of their data."1
To rectify this situation, the Report makes a number of recommendations that will "improve transparency, simplify the ability of consumers to exercise choices about how their information is collected and used, and ensure that businesses take privacy-protective measures as they develop and implement systems." 2
Specifically, it recommends implementation of the following:

"Privacy By Design": Companies should build privacy protections into their everyday business practices.

Simplified Choice: Companies should "provide choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past"
Specifically, the Report singles out online advertising that relies on behavioral targeting as a system that needs to provide consumers with choice in the use of their personal data; it recommends the creation of a "Do Not Track" system (see below)

Greater Transparency: several measures that companies should take to make their data practices more transparent to consumers include: clearer privacy notices; providing consumers with "reasonable access to the data they maintain" [on them]; providing disclosure and obtaining express consent before using the data "in a materially different manner" than originally claimed

Behavioral Targeting

What is behavioral targeting and why did the Commission single it out?

Behavioral targeting [BT] has been defined as the use of "…information collected on an individual's web-browsing behavior, such as the pages they have visited or the searches they have made, to select which advertisements to display to that individual."3 Its use is becoming increasingly popular by marketers.

According to Brandweek, Forrester Research reported that 24 percent of advertisers used BT in 2008, an increase of 50 percent over the previous year. A researcher said "…almost half of advertisers say, 'Even if I didn't use behavioral last year, I definitely want to this coming year'." 4 In early 2010, Adweek cited emarketer.com data which said that "14.2 percent of all display ad spending in 2010 will use some form of consumer behavior data indicating interest or intention to target ads."

Despite this popularity among marketers, BT has long been controversial because of privacy concerns. For example, another eMarketer report stated that "[p]ublic opinion remains heavily against tailored ads":

US Internet Users' Attitudes Toward Online Tracking for Ads

Advertisers should be allowed to match ads to interests based on websites visited

"A whopping two-thirds of internet users don't believe advertisers should be allowed to target online ads to their interests based on the sites they have visited, according to a survey by USA Today and Gallup." 5

Many Web articles talk about "the creepiness factor" — attesting to consumers' increasing discomfort with ads that appear to be based on knowledge about them and their browsing habits — for instance, a persistent ad for a dating service presented after a search for dating advice.

The marketing community has recognized the risks of turning consumers off with BT, as well as the possibility of government regulation of it. To address this, marketers have undertaken a number of self-regulatory initiatives.

For example, in early 2010, a group of marketers created an advocacy group, the Future of Privacy Forum, which introduced an "i" (for information) icon to be included on online ads that use behavioral targeting.

According to a January 2010 article in The New York Times:

> "Most major companies running online ads are expected to begin adding the icon to their ads by midsummer, along with phrases like "Why did I get this ad?
>
> "When consumers click on [the icon] they will be taken to a page explaining how the advertiser uses their Web surfing history and demographic profile to send them certain ads."6
>
> Industry groups have acknowledged that the driving force behind the initiative, as well as other self-regulatory steps, was to forestall FTC intervention.

FTC: Self-Regulation Has Been Insufficient

However, it apparently hasn't worked. The FTC Report specifically acknowledges the coalition's efforts to provide consumers with more information, in addition to stating the major browser vendors also offer mechanisms to allow consumers to limit online tracking. But the Report states that:

> "First, industry efforts to implement choice on a widespread basis have fallen short. …Although there have been developments in this area… an effective mechanism has yet to be implemented on an industry-wide basis.
>
> "Second, to the extent that choice mechanisms exist, consumers often are unaware of them, and click-through rates remain low.
>
> "Third, existing mechanisms may not make clear the scope of the choices being offered."7

Recommended: A "Do Not Track" Option

The Report asserts that the best way to address the concerns with "behavioral advertising" [sic] is to provide consumers with the ability to choose whether to allow their behavior to be tracked:

> "The most practical method of providing such universal choice would likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signaling the consumer's choices about being tracked and receiving targeted ads. Commission staff supports this approach, sometimes referred to as 'Do Not Track'."8

The Report says that this approach is similar to the Commission's "Do Not Call" system, which was effective in reducing unwanted telemarketing phone calls — with the advantage that such a system would not require setting up a Do Not Track Registry.

Therefore, the Staff report strongly recommends implementing steps that would reduce the perceived effectiveness of behaviorally-targeted advertising. Is such regulation likely to to pass?

It's not clear that the full Commission will accept all the recommendations of the Report; at least one Commissioner thinks the "Do Not Track" option may be "premature;"9 another offers qualified support for it "if technically feasible"10 and only if it is an "op-in" mechanism like "Do Not Call".

However, as the current focus on privacy legislation attests, Congress is well aware that consumers have a strongly negative opinion about overly personalized ads. Pressure is building for legislative or regulatory action and "Do Not Track" appears to be in the forefront. In this atmosphere, marketers would be well advised to consider reducing their reliance on behavioral targeting.

FTC-Approved: Contextual Advertising

However, marketers do have other targeting tools at their disposal. One of these is contextual targeting. The FTC report specifically excludes online contextual advertising from the need for oversight, saying that it falls within the category of "commonly accepted practices" and is not likely to be considered an unwarranted intrusion into consumers' privacy.

The usual online definition of contextual advertising is "advertisements… selected and served by automated systems based on the content displayed to the user" (Wikipedia definition). The FTC uses a broader description:

> "Contextual advertising involves the delivery of advertisements based upon a consumer's current visit to a web page or a single search query, without the collection and retention of data about the consumer's online activities over time. … contextual advertising is more transparent to consumers and presents minimal privacy intrusion as compared to other forms of online advertising."12

In other words, consumers are used to seeing ads that are placed on websites where the content of the ads is consistent with the environment, like in magazine ads. The targeting is done based on interest in the website's content, not on the tracked surfing behavior of the consumer.

Of course, the use of automated systems that scan websites for keywords and deliver ads accordingly have their own well-documented problems. Entire websites are devoted to contextual advertising blunders in which there is a serious mismatch between the website content and the ads delivered (i.e. a travel ad promoting a country placed in a news item about riots in the country's capital).13

To avoid these problems, ads could be placed the old-fashioned way: by the labor-intensive vetting of every website to ensure a match between the advertising and the editorial content. However, it is difficult to target an audience on a large scale this way.

Content Syndication: Safe and Scaled Contextual Advertising

Fortunately, there is a cost-effective way to ensure the placement of ads within appropriate content on a wide scale: content syndication.

When using the syndicated content model of online marketing, an advertiser doesn't need to track a consumer, trying to figure out where he or she is likely to go next. Content syndicators will have already identified — and contracted with — multiple websites that a targeted audience will likely visit, so the advertiser's message, which is embedded in appropriate content of interest to that audience, is already there when the consumer arrives.

CONCLUSION

While marketers' use of behavioral targeting for advertising has been increasing, there are warning signs that it may encounter resistance that will render it less effective, if not from threatened government regulation, then from consumers' objections. Content syndication provides advertisers with a safe, effective — and government-sanctioned — approach to large-scale audience targeting.

SOURCES

1 FTC Report, Executive Summary, page iv.
http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

2 Ibid.

3 Wikipedia entry, "Behavioral Targeting"

4 "Behavioral Targeting: A Tricky Issue for Marketers" Brandweek, 10/21/08
http://www.brandweek.com/bw/content_display/news-and-features/digital/e3i9e2284979c0b8c78ba188179079a495b?pn=1

5 "Can Consumers Learn to Love Behavioral Targeting?", Emarketer, 12/28/10
http://www.emarketer.com/Article.aspx?R=1008137

6 Stephanie Clifford, "A Little 'i' to Teach About Online Privacy', The New York Times, 1/26/2010
http://www.nytimes.com/2010/01/27/business/media/27adco.html?_r=1

7 FTC Report, pages 63-65.

8 FTC Report, Executive Summary p vi; also Page 66.

9 Concurring statement of Commissioner Kovacic, page D-1

10 Concurring statement of Commissioner Rosch, Page E-6.

11 Adweek, 6/13/2011 :
http://www.adweek.com/news/advertising-branding/nielsen-announces-new-approach-online-ad-measurement-132490

12 FTC Report, Page 55, Footnote 134.

13 See, for example,
http://njuice.com/Ten-horrifying-display-ad-placements
http://njuice.com/404/Ten-horrifying-display-ad-placements

APPENDIX I: SUMMARY OF PENDING PRIVACY LEGISLATION RELATING TO "DO NOT TRACK"

At present (July 2011), there is considerable Congressional activity on the issue of online privacy, including hearings and several bills introduced into both the Senate and the House.

It is important to note that "online privacy" encompasses both **data security** — an ongoing concern most recently evinced by the recent data breaches at companies including Sony and Citigroup, with the concomitant threat of identity theft and financial fraud — as well as the more specific one of behavioral tracking for marketing purposes (**"Do Not Track"**). Indeed, the revelations of phone hacking in the current News Corp. scandal suggest that the issue of privacy may extend beyond the Internet. This paper, however, addresses only the specific issue of "Do Not Track."

In this regard, there are four bills which have been introduced — two in the Senate and two in the House — which include some form of "Do Not Track."

S.913 – "Do Not Track" Online Act of 2011

This bill, introduced in May by Sen. Jay Rockefeller (D-WV), is the simplest and most straightforward. It calls for the Federal Trade Commission (FTC) to promulgate:

> "(1) regulations that establish standards for the implementation of a mechanism by which an individual can simply and easily indicate whether the individual prefers to have personal information collected by providers of online services, including by providers of mobile applications and services; and
>
> "(2) rules that prohibit… such providers from collecting personal information on individuals who have expressed, via a mechanism that meets the standards promulgated under paragraph (1), a preference not to have such information collected."

Important features of this bill include:

Substantial enforcement penalties: Fines of $16,000 per day for noncompliance, up to a maximum of $15 million.

State Action: States may bring civil actions for violations or the threat of violations; an FTC action against the violator would delay, but not preempt, the states' suits.

Safe Harbor/Self-regulation: There is no provision for self-regulation.

Summary: This bill requires the FTC to set a standard, so Internet users can easily participate in a "Do Not Track" system, as the FTC did for the very successful "Do Not Call" system. It also requires the FTC to be quite severe in pursuing marketers who track Internet users after they have opted out. There are not many loopholes; it lets both states and the FTC bring suits and it does not permit self-regulatory initiatives to preclude FTC scrutiny. From a marketer's perspective, this is the toughest of the bills currently pending (it has been read twice and referred to the Commerce Committee). Since the bill's sponsor, Sen. Rockefeller, is the Chair of the Commerce Committee, this bill will be in play if and when the Senate takes up the issue of online privacy.

S799 – Commercial Privacy Bill of Rights Act of 2011

Introduced in April by Senators Kerry (D- MA) and McCain (R- AZ), S799 addresses the broader issue of data privacy, but includes a specific section on "Do Not Track."

The first section ("Title I – Right to Security and Accountability") requires the FTC to promulgate rules requiring companies to take steps to ensure that the personal data it gathers is securely protected and calls for companies to adopt a "Privacy by Design" approach, as recommended in the original FTC Staff Report. Overall, this bill is quite broad in scope, but lacking in specifics.

The second section ("Title II – Right to Notice and Individual Participation") specifically deals with behavioral marketing. It requires the FTC to direct companies to make a clear statement of their practices regarding data collection, use and transfer. It then requires companies:

> to offer individuals a clear and conspicuous mechanism for opt-out consent for any use of their covered information that would otherwise be unauthorized use, except with respect to any use requiring opt-in consent…
>
> to offer individuals a robust, clear, and conspicuous mechanism for opt-out consent for the use by third parties of the individuals' covered information for behavioral advertising or marketing...

Note that this suggests that the entities themselves could use the data — just not transfer it to third parties.

There are several more sections which, among other things, require the offering of opt-in consent for the use of information for certain purposes, including, confusingly:

> "the use of previously collected covered information or transfer to a third party for an unauthorized use of previously collected covered information... if such use or transfer creates a risk of economic or physical harm..."

This is worded in such a way as to suggest that companies could use such information without consent in certain circumstances. It also allows companies to collect personal data that allows them to process transactions, prevent fraud or to "provide a secure environment." Therefore, there seem to be a number of loopholes that still allow companies to collect personal data and use it without consent.

The third section ("Title III – Rights relating to Data Minimization, Constraints on Distribution and Data Integrity") would require companies to collect only the data they need, distribute only as necessary and ensure that it is accurate. As with Section I, it is so broad and uses so many generalizations as to be virtually meaningless and unenforceable. In fact, there are no penalties associated with violations of this section.

Other features of this bill include:

Enforcement penalties: Fines of $16,500 per day or per individual for noncompliance of Title I and Title II, up to a maximum of $3 million — substantially lower than the Rockefeller bill.

State Action: States may bring civil actions for actual violations (not, as in S913, for the threat of violations). However, an FTC action against the violator would preempt the states' suits. This substantially reduces the exposure of a would-be violator.

Safe Harbor/Self-regulation: Requires the FTC to set rules and requirements for "safe harbor" (self-regulatory) programs. Companies that declare they abide by the requirements of approved programs would be safe from FTC action.

Summary: Along with several other general items, this bill directs the FTC to set standards for a "Do Not track" mechanism. In fact, it specifically mentions behavioral tracking. However, it is much more industry-friendly than S913, as the penalties are much lower, and there appear to be significant loopholes and ways to avoid FTC scrutiny.

H.R. 1895 – Do Not Track Kids Act of 2011

This bill was introduced by Reps. Edward Markey (D-MA) and Joe Barton (R-TX) in May 2011 as an amendment to the Children's Online Privacy Protection Act (COPPA) of 1998.

H.R. 1895 makes it "unlawful for an operator of a website, online service, online application, or mobile application directed to children… to collect personal information from a child in a manner that violates the regulations prescribed."

More specifically, it requires the FTC to promulgate regulations that require each such operator to:

> Provide clear notice of the type of information it collects, how it uses it and the procedures it uses to ensure it is collected lawfully.
>
> Obtain parental consent for the collection and use a of child's personal information.
>
> Provide the parent with the opportunity to refuse to permit further collection (opt-out).
>
> Not condition participation in a game or other service on the provision of a child's information.

SEC. 4. TARGETED MARKETING TO CHILDREN OR MINORS.

> (a) ACTS PROHIBITED — It is unlawful for an operator of a website, online service, online application, or mobile application directed to children or minors… to use, disclose to third parties, or compile personal information collected from children or minors, if the use, disclosure, or compilation is for targeted marketing purposes.

Other sections require operators to enact a "Digital Marketing Bill of Rights for Teens," which is not overly rigorous and forbids the collection of geo-location information for children and teens.

Another novel facet of this bill is the requirement that the FTC demands that operators provide an "**Erasure Button**" to delete previously collected information:

> SEC. 7. ERASER BUTTONS.
> "…to the extent technologically feasible, to implement mechanisms that permit users of the website, service, or application of the operator to erase or otherwise eliminate content that is publicly available through the website, service, or application and contains or displays personal information of children or minors; and to take appropriate steps to make users aware of such mechanisms.

Other features:

Enforcement penalties: None are specified; the bill simply says violators will be "subject to the penalties... provided in the Federal Trade Commission Act"

State Action: States may bring civil actions for violations or the threat of violations; the Commission may intervene and ask to be heard and to "file a petition for appeal." An FTC action against the violator would delay, but not preempt, the states' suits.

Safe Harbor/Self-regulation: There is no provision for self-regulation.

Summary: The language of this bill is relatively straightforward and seems fairly stringent with regard to tracking for marketing purposes. As such, it is similar to the Rockefeller Bill, though in this case specifically directed only to children and teens.

H.R. 1528 – CONSUMER PRIVACY PROTECTION ACT OF 2011

This Bill was introduced in April by Reps. Cliff Stearns (R -FL) Jim Matheson (D-UT), Brian P. Bilbray (R-CA) and Donald A. Manzullo (R-IL). It is lengthy and complicated and in the end relatively toothless on the issue of privacy. It neither mentions tracking, nor directs the FTC or any other entity to make rules. Instead, it issues some general guidelines, including:

directing online operators to have a privacy policy in place and to give appropriate notice to consumers. The first time personal data is collected from a user, the operator is required to state:

> what information is being collected and how it will be used
> whether the consumer is required to provide the information in order to do business with [the operator]
> whether the information may be sold or disclosed to a third party not affiliated with the operator

requiring operators to give users "the opportunity to preclude any sale or disclosure for consideration of the consumer's personally identifiable information to any covered entity that is not an information-sharing affiliate." [SEC. 6. CONSUMER OPPORTUNITY TO LIMIT SALE OR DISCLOSURE OF INFORMATION] However, it does not appear to deny the operator itself from using the information. Furthermore, the exclusion of the data is not permanent; rather, the exclusion remains in effect for five years.

Operators are required to have security policies in place to prevent the unauthorized disclosure of information.

Other features:

Enforcement penalties: A cap of $500,000 is placed on all violations — much lower than even the Kerry-McCain Senate bill.

State Action: Does not allow for either state or private action: "No private civil action relating to any act or practice governed under this Act may be commenced or maintained in any State court or under State law (including a pendent State claim to an action under Federal law)."

This clause effectively preempts state laws such as that adopted by the California Legislature.

Safe Harbor/Self-regulation: Allows for self-regulation; the FTC must approve an operator's self-regulatory policy within 90 days. If the FTC denies it, the order is subject to judicial review. An aggrieved consumer must first seek redress through the entity's dispute resolution policy before taking it to the FTC.

Summary: This bill does seem to require operators to disclose that they are gathering personal information and gives consumers a limited right to prevent the disclosure of their information. However, the language appears to put the onus on the consumer to figure out how to do so — and even then, the opt-out appears to apply to disclosures to third parties, not to the collection of the initial information. With its vague language, no mention of behavioral targeting, low penalties, emphasis on self-regulation and prevention of state or private action, this bill, if passed, would probably do little to affect present behavioral targeting practices.

APPENDIX II: ISSUES RELATING TO PRIVACY

The Senate Commerce, Science and Transportation Committee held a hearing on June 29, 2011, on three of the bills, two of which address tracking: the Commercial Privacy Bill of Rights of 2011 and the Do-Not-Track Online Act. The third bill, the Data Security and Breach Notification Act of 2011, does not address tracking.

While much of the hearing was spent addressing data security (especially the recent Citigroup and Sony breaches), "Do Not Track" was also discussed — and endorsed — by both Austin Schlick, general counsel of the FTC, and Julie Brill, an FTC commissioner. In her testimony, Brill said consumers should have more choices about their privacy and that entities should be more transparent about the data they collect.

"Most consumers are completely unaware about the data deluge being collected and sold about them both online and offline," Brill said.

On July 14, 2011, a joint House Energy and Commerce Subcommittee hearing focused on online privacy policy and perspectives of the "big three" federal agencies with potential jurisdiction over online privacy: the FTC, the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA).

The discussions provided some insight into the concerns of various members of Congress. In particular, the following issues were highlighted:

Economic Impact of Regulation: Are Congress and the regulatory bodies looking at the economic impact online privacy regulation will have on the Internet marketplace and businesses? Some committee members voiced concerns about "regulatory overreach." In response, the FTC said it was reviewing responses to the December 2011 FTC Staff Report in order to address these concerns. The FCC Commissioner emphasized the contribution privacy has to the online economy by stimulating consumer trust.

Defining the Harm: Concern was raised as to whether actual types of harm caused by consumer online behavioral tracking had been identified and whether Congress was trying to legislate in search of a problem. The FTC commissioner was pressed on this issue and responded by citing public reports that, for example, insurance companies use data aggregation to substitute for underwriting analysis. On the other hand, a member noted that self-regulation is not working and pointed to studies that have found "many participants in the Network Advertising Initiative — a self-regulatory voluntary code of conduct — violated their own privacy policies by leaving tracking cookies in place despite consumer opt-out."

Agency Jurisdiction and Authority: Defining the jurisdictional roles of the FCC, FTC and NTIA will be a point of debate in potential online privacy policy. The discussion highlighted a potential jurisdictional "turf war" between the FCC and FTC. The Commissioners disagreed over whether the FCC or FTC should have jurisdiction over telecommunications common carriers — an area traditionally under FCC jurisdiction — in protecting consumer privacy. On the other hand, the FTC Staff Report took note of the FTC's long history in dealing with privacy issues, including the creation of the very popular "Do Not Call" system, to which "Do Not Track" bears considerable resemblance.

Protecting Children: Strong support was voiced for the need to amend COPPA, as called for in the Do Not Track Kids Act. Given the explosion of the online ecosystem, obtaining parental consent and providing consumers with an "eraser button" to delete embarrassing data seemed to be an uncontroversial approach. Thus far, neither commission has a position on the Act, but the FTC is reviewing it.

Data Security: While not relating directly to behavioral targeting and "Do Not Track," recent public outcry over the revelation that News Corp. reporters hacked into cell phones served as a backdrop for the hearing and underscored the importance of data security in the debate. This would seem to make the chances for passage of some form of privacy legislation likely in the near future

Conclusion: There will be considerable debate on these issues in the months ahead, including the economic impact of regulation, agency jurisdictional authority and whether legislation or self-regulation is the appropriate response. But it is clear that privacy and data security will continue to be an important topic this year.

1 Much of this material is excerpted or summarized from the website of Kelley Drye and Warren, LLP:
"**Big Three' Weigh in on Online Privacy Hearing: FTC, FCC and NTIA Testify at Privacy Hearing**"
http://www.kelleydrye.com/publications/client_advisories/0686