

**“Information Privacy and Innovation in the Internet Economy”
U.S. Department of Commerce
Docket No. 101214614-0614-01**

Comments of the Center for Digital Democracy and U.S. PIRG

Protecting Consumers in the Digital Marketplace

28 January 2011

Although the title of the Department of Commerce’s recent report—“Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,”—might suggest that privacy and innovation are somehow at odds, that meaningful privacy protection can be achieved only at the expense of marketplace innovation, our experience suggests that the two are actually complementary. Indeed, in a real sense privacy and innovation are inseparable, in that technological innovation will mean nothing if consumers lack the motivation and confidence to *use* that technology. And nothing erodes that motivation and confidence more thoroughly than the perception that consumer participation in the Internet economy comes at the expense of personal privacy.

Unfortunately, much of the marketplace innovation being unleashed on the Internet today comes perilously close to exacting that toll. Too often, the drive to deeply engage a consumer using increasingly personalized, multi-platform interactive marketing runs roughshod over fair information practices, employing techniques of surveillance, tracking, and profiling that simply would not be tolerated in the bricks-and-mortar marketplace.

Imagine, for example, innumerable floorwalkers monitoring the browsing behaviors of department store shoppers, or sales agents following shopping mall visitors from one store to another, or the shelves in those stores magically rearranged in response to the demographic or behavioral profiles of individual consumers. These “Nightmare on Main Street” scenarios, however far-fetched they may appear, are played out daily in the online marketplace.

Nor has industry self-regulation come close to offering meaningful protection of consumer privacy. So-called “Notice and Choice,” which has been the foundation of the self-regulatory regime, has done nothing to stem the tide of increasing data collection and use—all without the genuinely informed understanding and consent of users. As with our financial system, privacy and consumer protection regulators have failed to keep abreast of developments in the area they are supposed to oversee. In order to ensure adequate trust in online marketing—an important and growing sector of our economy—we need sensible public policy regulatory safeguards to protect consumers.

The Department of Commerce is not positioned to play a leading role formulating and enacting meaningful public policies ensuring that consumers can have trust in the digital marketing environment. One looks in vain, for example, for any reference to consumers—or their privacy—in the department’s Mission Statement, or in its online overview (“About the Department of Commerce”). And the NTIA’s 2011 budget submission and the “Statement of Operating Objectives, as well as the description of the Assistant Secretary for Communications and Information position, are equally bereft of such references.¹ The Department’s “Privacy and Innovation” report, and the framework it proposes, must be substantially revised as it evolves into a final “white paper” blueprint for the Obama Administration. A more thorough analysis of contemporary online marketing and consumer data collection practices is required if U.S. consumers are to be ensured both their privacy and their transactions are fully respected online.² It is disconcerting, to say the least, that this “green paper” neglects to raise and meaningfully discuss the range of online consumer data collection practices that threaten privacy, including mobile and

¹ The NTIA’s “Statement of Operating Objectives” include the following provisions:

Domestic Policies—NTIA formulates and promotes national policies for consideration by the President and other executive branch agencies and by the independent Federal Communications Commission (FCC), Federal Trade Commission (FTC), and other government and non-government organizations. NTIA’s domestic policy objectives are to:

- promote the deployment of broadband services;
- open telecommunications and information markets to greater competition;
- refrain from regulating telecommunications and information markets wherever market forces are sufficient to ensure reasonable prices and terms of services and to protect consumers;
- preserve and promote an open Internet, consistent with service providers’ need to manage their networks in a transparent and nondiscriminatory manner;
- encourage the development of new telecommunications and information technologies and services for the American public;
- promote economic growth; and
- promote minority ownership in the telecommunications industry.

U.S. Department of Commerce, National Telecommunications and Information Administration, FY 2011 Budget as Presented to Congress, Feb. 2010, p. 30, http://www.ntia.doc.gov/budget/NTIA_FY2011_Congressional_Budget.pdf (viewed 23 Jan. 2011).

² The Commerce Department’s green paper falls far short in describing the privacy threats from behavioral profiling and other methods. For a more informed discussion on the issue, see the EU privacy commissioners’ recent “Opinion 2/2010 on Online Behavioural Advertising,” Article 29 Data Protection Working Party, <http://joshuabaer.blogs.com/files/wp-171-opinion-22010-on-online-behavioural-advertising.pdf> (viewed 25 Jan. 2011).

location targeting, social media marketing, “smart” behavioral targeting, and real-time ad exchanges—to name a few.³ The current data collection system that consumers confront daily—whether on their personal computers or mobile devices—is non-transparent, sophisticated, and ubiquitous. Indeed, it is astonishing that the Commerce report fails even to discuss the substantial privacy concerns documented in the *Wall Street Journal’s* “What They Know” series (and many other news reports as well). The failure of the Commerce report to address the fundamental issue raised by the *Journal*—that “One of the fastest-growing businesses on the Internet... is the business of spying on Internet users”—reflects an attempt, we fear, to whitewash the real privacy problems that confront U.S. citizens and consumers.⁴ Commerce and its Task Force should also have addressed the unique privacy concerns of children and adolescents, as well as the online data collection targeting multicultural groups (such as behavioral targeting of Spanish-speaking U.S. consumers).⁵

Recent self-regulatory regimes now provide some users access to an information “icon” that accompanies various self-regulatory codes of conduct.⁶ But while these new developments—embraced under political pressure and as a maneuver to

³ See, for example, Center for Digital Democracy and U.S. PIRG, “Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices,” 1 Nov. 2006, <http://www.democraticmedia.org/files/pdf/FTCadprivacy.pdf>; Federal Trade Commission Filing; Center for Digital Democracy and U.S. PIRG, “Supplemental Statement In Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices,” 1 Nov. 2007, http://www.democraticmedia.org/files/FTCsupplemental_statement1107.pdf; Center for Digital Democracy and U.S. PIRG, “Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices,” Federal Trade Commission Filing, 13 Jan. 2009, http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing; EPIC, Center for Digital Democracy, and U.S. PIRG, “In the matter of Google, Inc. and DoubleClick, Inc., Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission,” 20 Apr. 2007, http://www.epic.org/privacy/ftc/google/epic_complaint.pdf; and EPIC, Center for Digital Democracy, and U.S. PIRG, “In the matter of Google, Inc. and DoubleClick, Inc., Second Filing of Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief,” 17 Sept. 2007, http://epic.org/privacy/ftc/google/supp2_091707.pdf (both viewed 12 Oct. 2009).

⁴ Julia Angwin, “The Web’s New Gold Mine: Your Secrets,” *Wall Street Journal*, 30 July 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html?mod=what_they_know; “What They Know,” WSJ Blog, <http://blogs.wsj.com/wtk/> (both viewed 24 Jan. 2011).

⁵ CDD and other groups will be filing separate comments in this proceeding on the issues of adolescent online marketing and privacy.

⁶ “The Self-Regulatory Program for Online Behavioral Advertising,” 2010, <http://www.aboutads.info/> (viewed 25 Jan. 2011).

undermine the growing call for effective regulation in the U.S. and elsewhere—fail to effectively capture the realities of the current data collection and targeting system. Through techniques involving personalization, for example, along with other digital marketing applications, the online ad industry has created a highly intrusive but largely invisible system designed to encourage consumers to provide data and other information—often without understanding the implications and consequences.⁷ Just three years ago, online ad lobbyists denied there was even a privacy problem. Their attempt to dissuade growing bipartisan interest in Congress and the FTC to enact consumer protection safeguards, by adding graphic notices to ads and PR campaigns that offer assurances that behavioral profiling and tracking contribute to a positive consumer experience, illustrate a serious lack of commitment to protecting U.S. Internet users.⁸

The Commerce Department’s Internet Policy Task Force should have engaged in a proactive effort to gather information and ensure participation from consumer and privacy groups. Given the Department’s orientation—to protect the interests of U.S. business interests before the needs of consumers—it is not surprising that it did not work to ensure the creation of a record that included meaningful consumer and privacy group feedback. The Department’s efforts, in short, stand in sharp contrast to the Federal Trade Commission’s series of privacy roundtables around the country, which developed a record with much greater consumer participation.⁹

⁷ Center for Digital Democracy and U.S. PIRG. “Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices”; Center for Digital Democracy, U.S. PIRG, Consumer Watchdog, and World Privacy Forum, “In the Matter of Online Health and Pharmaceutical Marketing that Threatens Consumer Privacy and Engages in Unfair and Deceptive Practices. Complaint, Request for Investigation, Public Disclosure, Injunction, and Other Relief: Google, Microsoft, QualityHealth, WebMD, Yahoo, AOL, HealthCentral, Healthline, Everyday Health, and Others Named Below,” Federal Trade Commission Filing, 23 Nov. 2010, <http://www.democraticmedia.org/files/u1//2010-11-19-FTC-Pharma-Filing.pdf> (viewed 25 Jan. 2011). Mobile marketers, for example, have begun to incorporate a variety of techniques, including video, rich media, SMS, and the like to initiate the data collection and profiling process.

⁸ Randall Rothenberg, “War Against the Web,” *Huffington Post*, 21 Apr. 2008, http://www.huffingtonpost.com/randy-rothenberg/war-against-the-web_b_97811.html; The Self-Regulatory Program for Online Behavioral Advertising, “Welcome to the Online Home of the Self-Regulatory Program for Online Behavioral Advertising,” <http://www.aboutads.info/>; IAB, “IAB Privacy Matters: Understanding Online Advertising,” <http://www.iab.net/privacymatters/> (all viewed 27 Jan. 2011).

⁹ See, for example, Federal Trade Commission, “Exploring Privacy: A Roundtable Series,” <http://www.ftc.gov/bcp/workshops/privacyroundtables/>, and compare the diversity of comments elicited by those events (Federal Trade Commission, “# 309; FTC Project No. P095416; FTC to Host Public Roundtables to Address Evolving Consumer Privacy Issues,” <http://www.ftc.gov/os/comments/privacyroundtable/index.shtm>) with the narrower range of commentary generated by the NTIA’s task force in May-June 2010, National Telecommunications and Information Administration, “Public Comments on Docket#

The Department of Commerce report also reflects a lack of clear understanding of the history of privacy debates in the U.S., most notably the pivotal discussions in the 1990's (Or perhaps the report reflects an attempt to revise the facts in order to serve the Department's own goals to assist the U.S. online marketing industry.) Indeed, the Department of Commerce report is rife with historical inaccuracy. It fails to acknowledge the call for privacy safeguards by a wide spectrum of privacy and consumer groups throughout the 1990's, including at the FTC. For example, it was only with the advocacy of the nation's leading consumer, education, child welfare and educational and health groups that the Clinton administration finally reversed its opposition to privacy rules to protect children.¹⁰ The report is also incorrect in suggesting that what happened during the 1990's led to some kind of model in terms of Internet privacy. The problems consumers face online today from digital marketing and data collection are largely due to the failure of policymakers back in the 1990's to act decisively in support of a new law. It has been a lack of action in addressing behavioral profiling, tracking, and other intensive data-collection techniques that has led to the current crisis confronting US consumers.¹¹ Similarly, the failure of the recent Commerce report to support a "Do Not Track" system, such as that proposed by the FTC, suggests that the Department may be more concerned with boosting online data collection revenues for industry than with protecting consumers.¹² As a recent study noted, the Department of Commerce does not have a positive track record protecting consumers online, failing, for example, to ensure that consumer privacy is protected in its inadequate administering of the U.S.-European Union Safe Harbor agreement.¹³

100402174-0175-01," <http://www.ntia.doc.gov/comments/100402174-0175-01/> (all viewed 24 Jan. 2011).

¹⁰ For a brief history of the Children's Online Privacy Protection Act (COPPA), see Kathryn C. Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (Cambridge, MA: MIT Press, 2007): 141-177.

¹¹ Federal Trade Commission, "Privacy Initiatives: Unfairness & Deception Reports & Testimony," http://www.ftc.gov/privacy/privacyinitiatives/promises_reptest.html; Federal Trade Commission, "Online Profiling Public Workshop," Nov. 1999, <http://www.ftc.gov/bcp/workshops/profiling/index.shtm>; Electronic Privacy Information Center, "Group Letter on Online Profiling Agreement," 9 Aug. 2000, http://epic.org/privacy/internet/NAI_group_letter.html (all viewed 24 Jan. 2011).

¹² Jon Leibowitz, "FTC Chairman: 'Do Not Track' Rules Would Help Web Thrive," *US News and World Report*, 3 Jan. 2011, <http://www.usnews.com/opinion/articles/2011/01/03/ftc-chairman-do-not-track-rules-would-help-web-thrive-jon-leibowitz> (viewed 24 Jan. 2011).

¹³ World Privacy Forum, "The US Department of Commerce and International Privacy Activities: Indifference and Neglect," 22 Nov. 2010, <http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf> (viewed 24 Jan. 2011).

It was only through significant advocacy by privacy and consumer groups in the U.S. during the last few years, along with action by EU regulators and growing public concern, that the U.S. online ad marketplace has even begun to accept some responsibility. But as the online ad lobby's recent successful political effort to undermine the ability of the FTC to enact regulatory safeguards on privacy and consumer protection reveals, the digital marketing and data collection industry is afraid of allowing U.S. consumers to control what data can be collected from them.¹⁴ (It should be noted that the IAB, which led the fight against the proposed rules that would enable the FTC to protect consumers, has the leading online marketing companies on its board, including Google, Microsoft, AOL, Viacom, Comcast, and News Corps.)¹⁵

In light of its record on consumer privacy protection, we do not believe that the Commerce Department should establish a Privacy Policy Office. Nor should it attempt to assert greater control over U.S. consumer privacy issues. U.S. consumers require an independent agency to play the lead role developing and promoting privacy policy. The Department of Commerce has too many conflicting interests, given its mandate to serve the commercial and trade interests of U.S. businesses. Consumers require—and deserve—an agency that primarily focuses on their needs and experiences. Any framework designed to protect U.S. consumers' privacy and their transactions online should have at its foundation an independent governmental body whose primary responsibility is to consumer protection. As the Department must recognize, it is not structured—either historically or operationally—to operate as a consumer protection agency. Therefore, the Administration should ensure that the Federal Trade Commission and the newly established Bureau of Consumer Financial Protection are the primary policy and enforcement federal governmental entities on privacy.¹⁶

The FTC has already been accepted as a member of the leading global privacy regulatory organizations.¹⁷ The Department of Commerce can play a *subordinate*

¹⁴ Kate Kaye, "Ad Industry Fights to Stop Stronger FTC and Wins—For Now," ClickZ, 28 June 2010, <http://www.clickz.com/clickz/news/1721880/ad-industry-fights-stop-stronger-ftc-wins-for-now> (viewed 27 Jan. 2011).

¹⁵ IAB, "IAB Board Members," http://www.iab.net/about_the_iab/iab_board (viewed 27 Jan. 2011).

¹⁶ U.S. Department of the Treasury, "Bureau of Consumer Financial Protection (CFPB)," <http://www.treasury.gov/initiatives/Pages/cfpb.aspx> (viewed 27 Jan. 2011).

¹⁷ "US Federal Trade Commission Joins Asia Pacific Privacy Authorities Forum," 23 Sept. 2010, <http://privacy.org.nz/us-federal-trade-commission-joins-asia-pacific-privacy-authorities-forum/>; Boris Segalis, "Data Commissioners Conference in Jerusalem Focuses on Future of Privacy, Cooperation and Enforcement," Information Law Group, 2 Nov. 2010, <http://www.infolawgroup.com/2010/11/articles/recent-news/data-commissioners-conference-in-jerusalem-focuses-on-future-of-privacy-cooperation-and-enforcement/> (both viewed 25 Jan. 2011).

role, as it helps businesses address related privacy matters, but consumers would be poorly served by a new privacy policy role for the Department, which would place the special interests of commercial data collection industries over those of consumers.

Thus we call on the Obama administration to reverse the Commerce Department's expansionist plans, and ensure instead that an independent agency—one genuinely concerned about consumer needs and interests—will play the primary role in promoting online privacy. The attempt by Commerce in its green paper to relegate the FTC to privacy enforcement matters could be interpreted as a power grab designed to help powerful data collection interests. Many online marketers and lobbying groups support a stronger Commerce role precisely *because* they see it as an ally against the more thorough privacy framework recently proposed by FTC staff.¹⁸

Meaningful Fair Information Practice Principles (FIPPs) are required, but not based on a weak collection of self-regulatory codes that allow industry to continue its data-collection practices.¹⁹ Consumers would have been better served by the Department's privacy report had it developed its own comprehensive framework allowing individuals to have actual control over the data collection, profiling, and targeting process. A flimsy regime composed of "voluntary, enforceable privacy codes of conduct," as proposed by the report, illustrates that the Department's Internet Task Force is willing to place business-as-usual industry practices ahead of consumer concerns. Multi-stakeholder discussions and agreements should not replace public policy. While dialogue with industry is appropriate, the weak privacy proposals in the Commerce paper will set back true consumer privacy protection. If any such dialogues occur, moreover, they must be open and accountable to the public and ensure real parity among consumer and privacy groups and industry (with NGOs that receive industry funding playing only a limited role or counted as an industry participant. Academic experts should include those without funding or other conflicts of interest involving the online and data industry). Additionally, funding for research should be made available to the privacy and consumer groups, so they can muster adequate resources to respond to industry claims. In addition,

¹⁸ IAB, "IAB Responds to DOC Green Paper on Privacy," 16 Dec. 2010, http://www.iab.net/public_policy/1495162; Direct Marketing Association, "Direct Marketing Association Praises Department of Commerce Privacy Report," 16 Dec. 2010, <http://www.the-dma.org/cgi/dispanouncements?article=1514>; Federal Trade Commission, "FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers," 1 Dec. 2010, <http://www.ftc.gov/opa/2010/12/privacyreport.shtm> (all viewed 24 Jan. 2011).

¹⁹ For a discussion of inadequate FIPPs, see Fred H. Cate, "The Failure of Fair Information Practice Principles," in *Consumer Protection in the Age of the "Information Economy"* (forthcoming), http://www.hunton.com/files/tbl_s47Details/FileUpload265/1248/Failure_of_Fair_Information_Practice_Principles.pdf (viewed 24 Jan. 2011).

the Department's attempt to exempt companies from meaningful FTC enforcement actions if they adopt what will be weak and ineffective "safe harbors," is equally disturbing.²⁰ Such a proposal illustrates the Department's overall orientation that places the interests of the online data industry over consumer welfare. Any regime must ensure effective and flexible FTC and other regulatory action, given the growing data collection practices that will thrive within the boundaries of self-regulatory codes.

The U.S. should be a global leader in privacy.²¹ But the green paper proposes a "global interoperability" process in which a weak U.S. privacy regime would give U.S. online marketers and other data collection companies a free "you can collect data from the EU and Asia Pacific market" pass. This is one of the most problematic aspects of the green paper's proposal. It appears to be an attempt to undermine the notable EU regime on privacy, and set the stage for the growing Asia-Pacific (APEC) market as a consumer protection and privacy free zone.²²

Unfortunately, most Americans know very little about what the industry calls the new "media and marketing ecosystem."²³ The forms of advertising, marketing and

²⁰ Pam Dixon, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation," World Privacy Forum, Fall 2007, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (viewed 24 Jan. 2011).

²¹ See, for example, William E. Kennard, "Data Protection in a Transatlantic Perspective," Remarks of William E. Kennard, U.S. Ambassador to the EU Before the Committee on Civil Liberties, Justice, and Home Affairs, 25 Oct. 2010, <http://www.europarl.europa.eu/document/activities/cont/201010/20101027ATT90670/20101027ATT90670EN.pdf> (viewed 24 Jan. 2011).

²² Jeff Chester, "Statement of Jeff Chester on the Department of Commerce's Internet Policy Task Force Privacy and E-Commerce: a Bill of Behavioral Targeting 'Rights' for Online Marketers?" Digital Destiny, 16 Dec. 2010, <http://www.democraticmedia.org/jcblog/?p=1039>; Jeff Chester, "Digital Ad Lobby Plan for Commerce Privacy Approach: Sideline FTC and Stronger Consumer Protection Rules," Digital Destiny, 17 Dec. 2010, <http://www.democraticmedia.org/jcblog/?p=1040>; Jeff Chester, "Did the Commerce Dep't Give a Special Deal to the Online Data Collection Lobby?" Digital Destiny, 17 Dec. 2010, <http://www.democraticmedia.org/jcblog/?p=1041> (all viewed 24 Jan. 2011).

²³ There are a number of academic studies that should inform the current investigation of online privacy, including such essays as Aleecia McDonald, "Cookie Confusion: Do Browser Interfaces Undermine Understanding?" *Proceedings of the 28th International Conference Extended Abstracts on Human Factors in Computing Systems*, 2010, <http://people.mozilla.com/~faaborg/files/20100420-chi2010Firefox/cookieConfusion.pdf>; Aleecia McDonald and Lorrie Cranor, "Americans' Attitudes About Internet Behavioral Advertising Practices," *Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES, forthcoming)*, <http://www.aleecia.com/authors-drafts/wpes-behav-AV.pdf>; Aleecia McDonald and Lorrie Cranor, "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising," 38th Research Conference on Communication, Information and

selling that are emerging as part of the new media depart in significant ways from the more familiar commercial advertising and promotion we have seen in print and on television in the past. In today's digital marketing system, advertising, editorial content, data collection, measurement, and content delivery are increasingly intertwined. As a major advertising industry report on the future of marketing in the digital era explained, "The influx of data into marketing has been one of the biggest changes to players across the landscape.... Advertising strategies, campaigns, and distribution are increasingly based on predictive algorithms, spreadsheets, and math.... Every Web page's individual views, every word typed in a search query box (also known as the 'database of consumer intentions'), every video download, and even every word in an e-mail may create one more data point that a marketer can leverage and use to more precisely target the audience...."²⁴

Specifically, few U.S. consumers understand the power and intent of behavioral targeting, which, notes *eMarketer*,

segments the audience based on observed and measured data—the pages or sites users visit, the content they view, the search queries they enter, the ads they click on, the information they share on social internet sites and the products they put in online shopping carts. This data is combined with the time, length and frequency of visits.... Behavioral targets people, not pages. That is, behavioral uses the actions of a person to define its target, unlike contextual targeting, which serves ads based on a page's contents.... Behavioral information can also be merged with visitor demographic data—such as age, gender, and ZIP code.... Whether tracked by cookies or ISPs, the sort of user data that builds behavioral profiles takes in search queries, Web site visits, specific content consumed (such as clicks or playing a video), product shopping comparisons, product purchases and items placed in shopping carts but not bought.²⁵

Expressed another way, "Behavioral targeting customizes messages to individual consumers based on their specific shopping interests, and characteristics like

Internet Policy (Telecommunications Policy Research Conference, forthcoming), 16 Aug. 2010, <http://www.aleecia.com/authors-drafts/tprc-behav-AV.pdf>; Aleecia McDonald and Lorrie Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, 2008, <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>; and Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, and Chris Jay Hoofnagle, "Flash Cookies and Privacy," 10 Aug. 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862 (all viewed 24 Jan. 2011).

²⁴ Edward Landry, Carolyn Ude, and Christopher Vollmer, "HD Marketing 2010: Sharpening the Conversation," Booz/Allen/Hamilton, ANA, IAB, AAAA, 2008, http://www.boozallen.com/media/file/HD_Marketing_2010.pdf (viewed 12 Oct. 2009).

²⁵ David Hallerman, "Behavioral Targeting: Marketing Trends," *eMarketer*, June 2008, pp. 2, 11. Personal copy.

gender, age, and ethnicity. Behavioral targeting is a generic name for a series of technologies that collect and organize click stream data, develop data warehousing structures, apply data mining algorithms to uncover consumer browsing patterns, and serve targeted ads matched to an individual.”²⁶

Thus we are witnessing a dramatic growth in the capabilities of marketers to track and assess our activities and communication habits on the Internet.²⁷ Advertisers and marketers have developed an array of data collection and profiling applications, honed from the latest developments in such fields as semantics, artificial intelligence, auction theory, social network analysis, data-mining, and statistical modeling. Behavioral targeting is just one tool in the interactive advertisers’ arsenal. Social media monitoring, so-called “rich-media” immersive marketing, new forms of viral and virtual advertising and product placement, and a renewed interest (and growing investment) in neuromarketing, all contribute to the panoply of approaches that also includes BT. Behavioral targeting itself has also grown more complex. That modest little “cookie” data file on our browsers, which created the potential for behavioral ads, now permits a more diverse set of approaches for delivering “computational” advertising. We are being intensively tracked on many individual websites and across the Internet. Behavioral targeting and related technologies may provide “marketing nirvana,” as one company explained, but it leaves consumers unaware and vulnerable to an array of marketing communications that are increasingly tied to such inherently personal details as one’s health and finances.²⁸

Although discussions of consumer privacy in the digital age can be extraordinarily complex, we want to highlight five areas of concern—consumer tracking online, real-time ad auctions/exchanges, social media marketing, mobile/location marketing, and neuromarketing—that should have been discussed in the Commerce report for their impact on privacy.

1. Developments in consumer online tracking:

²⁶ Catherine Dwyer, “Behavioral Targeting: A Case Study of Consumer Tracking on Levis.com,” *Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, California August 6th-9th 2009*.

²⁷ For a useful online illustration on the data collection and targeting capabilities of online ad networks, see *Advertising Age’s* “Ad Networks+ Exchanges Guide. 2009. <http://brandedcontent.adage.com/adnetworkguide09/lobby.php?id=2> (viewed 14 June 2009).

²⁸ “The Rise of On-site Behavioral Targeting,” <http://www.omniture.com/offer/281> (viewed 14 June 2009). See, for example, Yahoo Research, “Computational Advertising,” http://research.yahoo.com/Computational_Advertising; Stanford University, “MS&E 239: Introduction to Computational Advertising,” <http://www.stanford.edu/class/msande239/>; “Welcome to MDMKDD 2010,” <https://sites.google.com/site/mdmkdd2010/> (all viewed 27 Jan. 2011).

As Yahoo's online ad auction service Right Media explains in a "primer" for marketers, "Data providers are changing the advertising landscape by focusing on who sees ads rather than where ads appear.... When consumers go to certain web sites, the page places a tag (or 'cookie') within the browser—tracking that a particular browser visited a particular site. In some cases, a data provider (which can also be described as a data 'collector') pays the web site for the ability to do this. The cookie enables the data provider to follow consumers and track their online 'behavior.'"²⁹ The growth of individual user tracking involving behavioral targeting and similar techniques underscores both the privacy threats consumers increasingly face and how industry claims they aren't targeting using "personal information," which should have been acknowledged by the Commerce report.

Commerce should have also sounded an alarm on behalf of consumers over the growing merging of offline and online data. Online tracking is now being combined with offline databases to create even more detailed profiles: "Digital-marketing companies are rapidly moving to blend information about consumers' Web-surfing behavior with reams of other personal data available offline," explained one of the dozens of new data tracking and profiling companies that have emerged in this era of "Big Data" consumer data collection. For example, eXelate, a behavioral targeting warehouse and "marketplace," ties "its data on more than 150 million Internet users to Nielsen's database, which includes information on 115 million American households, to provide more-detailed profiles of consumers. 'We can build [consumer] profiles from any building blocks,' [explained] eXelate.... 'Age, gender, purchase intent, interests, parents, bargain shoppers—you can assemble anything.'"³⁰ eXelate "gathers online consumer data through deals with hundreds of Web sites. The firm determines a consumer's age, sex, ethnicity, marital status and profession by scouring Web-site registration data. It pinpoints, for example, which consumers are in the market to buy a car or are fitness buffs, based on their Internet searches and the sites they frequent. It gathers and stores the information using tracking cookies, or small strings of data that are placed on the hard drive of a consumer's computer when that consumer visits a participating site. Advertisers, in turn, purchase cookie data from eXelate and use it to buy targeted online ads." eXelate's recent agreement with Nielsen will "will allow advertisers to go to eXelate to buy New York-based Nielsen's trove of data converted to a cookie-based digital format. That data comes from sources including the Census Bureau, the firm's own research and that of other consumer-research firms, such as Mediamark Research and Experian Simmons."³¹ The Commerce report should have analyzed the growth

²⁹ Right Media, "Data Providers," <http://rightmedia.yahoo.com/data-providers> (viewed 1 Apr. 2010).

³⁰ Emily Steel, "Exploring Ways to Build a Better Consumer Profile," *Wall Street Journal*, 15 Mar. 2010, <http://online.wsj.com/article/SB10001424052748703447104575117972284656374.html?KEYWORDS=exelate> (subscription required).

³¹ Steel, "Exploring Ways to Build a Better Consumer Profile."

of the online marketing data collection apparatus and discussed how consumer privacy is daily facing new risks.³²

The role of online lead generation (so-called “trigger leads”) and the use of behavioral targeting for mortgages and other loans represent a potentially critical threat to the privacy of digital consumers, whose data are used without their clear understanding, let alone control, of such surveillance. For example, Lightspeed Research promises marketers a “full wallet view across customers’ many financial services relationships,” providing “unparalleled insight into consumers’ use of credit, debit, banking and alternative payment products. We passively gather information from their financial accounts and merge it with third-party behavioral datasets, survey-based attitudinal insights, and industry expertise.”³³ Growing investment in behavioral and other online ad data collection practices also warrant a discussion by Commerce and a final report on their impact on consumer privacy.³⁴

Increasingly, these various targeting and profiling processes are carried out on the fly, thanks to sophisticated automation and optimization technologies. “The DataXu platform,” for example, “enables advertisers to measure, analyze and optimize digital media across the ad exchanges of Google, Yahoo and others. Unlike any other online advertising service, the DataXu platform values, bid manages and buys each ad impression individually, making real-time decisions on each ad opportunity, as it occurs. With the ability to process hundreds of thousands of ‘ad decisions’ a second—each returned in under 100 milliseconds—DataXu produces higher returns on media investments and lowers media costs by eliminating unnecessary impression spend.”³⁵ Google’s Teracent Mobile SmartAds, for example, “enable advertisers to customize creative to individual users in real-time with dynamically optimized ads based on user demographic and interest-based data, as well as factors such as location....”³⁶

³² For a map of the display ad technology marketplace, see Luma Partners, “Display Advertising Technology Landscape,” http://2.bp.blogspot.com/_-1K8To6cNmY/TQYxTMGxIOI/AAAAAABjHg/_Eu4WwBmPYo/s1600/ecosystem.jpg (viewed 27 Jan. 2011).

³³ Lightspeed Research, Financial Services Brochure, http://www2.lightspeedresearch.com/uploads/Financial_Services_Brochure.pdf (viewed 22 May 2009).

³⁴ “M&A & Venture Capital,” paidContent.org, <http://paidcontent.org/topic/ma-venture-capital/> (viewed 27 Jan. 2011).

³⁵ “DataXu Launches the First Real-Time Optimization Platform for Advertisers: Havas Digital Chooses DataXu as Optimization Partner,” 15 Sept. 2009, <http://www.dataxu.com/news/sample.php> (viewed 25 Oct. 2009).

³⁶ Teracent, “Mobile SmartAds,” <http://www.teracent.com/mobile.html> (viewed 26 Oct. 2009). Google acquired Teracent in 2009. Neal Mohan, “Displaying the Best Display Ad with Teracent,” Official Google Blog, 23 Nov. 2009,

2. Real-time auctions/exchanges:

Real-Time Bidding (RTB) “is the fastest growing segment of U.S. online advertising.... With RTB, advertisers have the great level of transparency available on the individual user in real-time.... Having greater transparency about the user in real-time provides great insights to advertisers, but it is the difference in how media is bought and sold with real-time bidding is the game changer....” RTB “can buy impressions to reach specific users or reject them as the campaign is in progress.”³⁷ The recent developments in online profiling and targeting represent a significant shift in how media for advertising is bought and sold: individual users, via impression targeting, can be purchased. The expansion of user targeting dramatically brings new threats to consumer privacy.

Recent press reports document these developments. As the *New York Times* described the real-time ad-bidding process, “Now, companies like Google, Yahoo and Microsoft let advertisers buy ads in the milliseconds between the time someone enters a site’s Web address and the moment the page appears. The technology, called real-time bidding, allows advertisers to examine site visitors one by one and bid to serve them ads almost instantly.... Using data providers like BlueKai or eXelate, AppNexus can add information about what a person has been doing online. ‘It’s a lot about being able to get the right users, but it’s also about passing on certain instances where we don’t think you’re in the market, based on what you’ve been doing in the past hour,’ Mr. Ackley [vice president for Internet marketing and advertising at eBay] said.... Until the arrival of real-time bidding, said Mr. Mohan of Google, ‘the technology hasn’t really been there to deliver on the promise of precise optimization, delivering the right message to the right audience at the right time’ in the display world.”³⁸ Ad exchange targeting also involves such sensitive areas as health and finance. Google’s DoubleClick Ad Exchange permits the targeting of a wide range of health and financial behaviors. These include arthritis, diabetes, GERD

<http://googleblog.blogspot.com/2009/11/displaying-best-display-ad-with.html> (viewed 25 Jan. 2011).

³⁷ Pubmatic, “Understanding Real-Time Bidding (RTB) From the Publisher Perspective,” Feb. 2010, http://www.pubmatic.com/wp-content/uploads/2010/02/PubMatic_RTb_White_Paper.pdf (viewed 1 Apr. 2010).

³⁸ Stephanie Clifford, “Instant Ads Set the Pace on the Web,” *New York Times*, 11 Mar. 2010, <http://www.nytimes.com/2010/03/12/business/media/12adco.html> (viewed 1 Apr. 2010). Microsoft, which acquired ad exchange company ADECN in 2007, is now in the process of “ramping” up its capabilities. Emile Litvak, “ADECN delivers – RTB goes live!” *The Turn Blog*, 17 Feb. 2010, <http://blog.turn.com/2010/02/17/adecn-delivers---rtb-goes-live/> (viewed 4 Apr. 2010).

and digestive disorders, migraines, sleep disorders, pain management, credit cards, loans and insurance.³⁹

Rubicon's "Targeted Audience Program" (TAP) "allows publishers to... [t]arget specific users on a publishers site." "The Data Intelligence layer of REVV™, upon which TAP is built ...aggregates data from a full spectrum of third-party data providers as well as site user and page data to create a holistic view of audience; Affinity Scoring drives insight into visitors' real interests and behavior, applying proprietary data mining algorithms to extract patterns and reveal audience insight...."⁴⁰ The monetization of our data and online behaviors is now being carried out in marketplaces that so far have been largely operating without the scrutiny of regulators or Congress.⁴¹

3. Social media marketing:

As social networks have become increasingly popular in recent years, social media monitoring, a form of online surveillance, has become a common practice. Social networks, it is clear, have taken behavioral targeting to another level, allowing marketers to target users based both on their online activities as well as on self-disclosed profile information. Few social media users understand the wide range of data tracking and targeting that operates on and via these networks. Our communications on blogs, social networks and other Web 2.0 media are now being analyzed, including for the purpose of targeting what are called key or "Alpha" influencers (people whose opinion sways their network of relationships). As the authors of one recent book on the social media marketing industry explained, "The digitally networked visitor to these social media forms leaves behind footprints, shadows and trails of his or her individual collective endeavours in the form of data; data that enables new type of marketing and communication between and within consumer communications.... Over time, this process will lead to an understanding

³⁹ DoubleClick, "Category Targeting Codes," <http://www.google.com/support/adxbuyer/bin/answer.py?answer=156178> (viewed 1 Apr. 2010). Angwin, "The Web's New Gold Mine: Your Secrets."

⁴⁰ "Audience-based Sales Now Drive 10% of Online Advertising Revenue For Web's Premium Publishers," 9 Dec. 2009, <http://www.rubiconproject.com/about/press/audience-based-sales-now-drive-10-of-online-advertising-revenue-for-webs-pr/> (viewed 1 Apr. 2010).

⁴¹ Center for Digital Democracy, U.S. PIRG, and World Privacy Forum, "In the Matter of Real-time Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy. Complaint, Request for Investigation, Injunction, and Other Relief: Google, Yahoo, PubMatic, TARGUSinfo, MediaMath, eXelate, Rubicon Project, AppNexus, Rocket Fuel, and Others Named Below," FTC filing, 8 Apr. 2010, http://www.uspirg.org/uploads/eb/6c/eb6c038a1fb114be75ecabab05b4b90b/FTCfiling_Apr7_10.pdf. See also AdExchanger.com, <http://www.adexchanger.com/> (both viewed 27 Jan. 2011).

of the participant's digital footprint."⁴² The privacy issues raised by Facebook, for example, require a critical analysis with a goal of consumer protection. Extensive data-mining and targeting techniques that claim to be permitted under an opt-in basis, for example, illustrate how contemporary data collection and online marketing practices require affirmative pro-consumer safeguards. Facebook and other social media marketing companies claim access to and use of the identities and online behaviors and relationships of their users, and embrace schemes and techniques to pry open even more information on consumers and their networks of family, friends, and associates.⁴³

The growth of social media surveillance requires the development of privacy safeguards supporting transparency and control by consumers. As the Department develops a white paper for the Administration, it should conduct a thorough analysis of the data collection and targeting strategies used by Facebook and similar social media companies (including locational techniques) and propose new public policies specifically designed to address the particular privacy and consumer protection implications.⁴⁴

⁴² Ajut Jaokar, Brian Jacobs, Alan Moore, and Jouko Ahvenainen, *Social Media Marketing: How Data Analytics Helps to Monetize the User Base in Telecoms, Social Networks, Media and Advertising in a Converged Ecosystem* (London: Futuretext, 2009), pp. 2, 19.

⁴³ See, for example, the "Facebook Marketing Bible," <http://gold.insidenetwork.com/facebook-marketing-bible/>; and Facebook, "Preferred Developer Consultant Program," Facebook Developers, <http://developers.facebook.com/preferreddevelopers> (both viewed 27 Jan. 2011).

⁴⁴ "More than 75 percent of all Americans are participating in some form of social media through blogs, forums, and sites like Facebook and Twitter," notes Visible Technologies, whose truCAST product suite includes social media monitoring and analysis applications." Visible Technologies, "ENGAGE Solutions," http://www.visibletechnologies.com/downloads/Solutions_ENGAGE.pdf (viewed 23 Oct. 2009). Collective Intellect, a market intelligence company, offers marketers "a real time 'listening' interface that's available 24x7 with automated alert emails. Each topic allows the tracking of activity, sentiment, author demographics, and emerging conversational themes. Sources currently include digital blogs, boards, news, and micro-blogs." Collective Intellect, "Real Time Topic-based Monitoring," <http://www.collectiveintellect.com/products/listen> (viewed 22 Oct. 2009). Offering both basic analytics (which "automatically derives general statistics for each topic being analyzed, across activity [number of conversations], sentiment [positive, negative, neutral], conversational themes, and the source of conversations") and advanced analytics (which "automatically identifies key influencers by topic, analyzes specific mentions and interactions with brands, campaigns, media, and provides micro-blog context"), Collective Intellect "helps market researchers understand what consumers like and dislike, and how a brand/product/show/event is perceived...." Among the factors that Collective Intellect analyzes are "Topic Attributes (tastes, features, etc.), Ritual Associations, Emotional and Rational Associations, Economic Associations, Quality Associations, [and] Unlimited Consumer Associations: Selection, Trust, Authenticity...." Collective Intellect, "Our Analytics," http://www.collectiveintellect.com/about/our_analytics (viewed 22 Oct. 2009).

4. Mobile/location marketing:

Many of the same consumer data collection, profiling, and behavioral targeting techniques that have raised concerns in the more “traditional” online world have been purposefully brought into the mobile phone marketplace. The mobile marketing industry has already developed extensive plans and techniques to help it collect and harvest the data from what it calls the “user journey” through the

Converseon offers a similar social media surveillance product, Conversation Miner, which “scours public, online discussion areas—including blogs, newsgroups, social media, and more—to capture, understand and report the issues, opinions and ideas that customers share between and among themselves.... Conversation Mining is an essential first step in developing an effective communications strategy to join and influence the conversation.”

Converseon, “Conversation Mining: Are Your Ears Buzzing?”

<http://www.converseon.com/conversation-mining.html> (viewed 22 Oct. 2009). Acxiom Relevance-X Social, similarly, “brings consumer data intelligence to online social marketing.... Acxiom Relevance-X Social helps you see the social networks of your customers and how many friends or contacts they may have within online communities, then compares this data against other markers....” “With Acxiom Relevance-X Social data, marketers can:

- Establish and maintain up-to-date social intelligence on their customers
- Interact with socially active brand advocates
- Create campaigns that solicit user-generated content or demonstrate brand enthusiasm
- Develop loyalty programs to reward segments
- Test products or services
- Plan media where your customers are socially active
- Invite, communicate and influence the influencers in a respectful and engaging way to drive purchase behavior.

Acxiom, “The Power of Direct Social Media Marketing,”

http://www.acxiom.com/products_and_services/Targeted%20Advertising/social_media/Pages/Social_Influencer.aspx (viewed 30 Oct. 2009). Products such as Nielsen’s

Buzzmetrics, BuzzLogic (“conversation ad targeting”), Ripple6 and Radian6 are part of this new digital data collection apparatus. See, for example, Radian6, “Social Media Monitoring and Engagement for Agencies and the Enterprise,”

<http://www.radian6.com/cms/solution> (viewed 14 June. 2009); BuzzLogic, “Get Your Ads in Front of Passionate Consumers,” <http://www.buzzlogic.com/advertisers/conversation-targeting.html>; Nielsen Online, “Millions of Consumer are Talking—Are You Listening,”

http://www.nielsen-online.com/products.jsp?section=pro_buzz (viewed 14 June. 2009);

Ripple6, “Revolutionizing Research Through Online Conversations,”

<http://www.ripple6.com/platform/socialInsights> (viewed 14 June. 2009).aspx; and Suresh Vittal, “The Forrester Wave: Listening Platforms, Q1 2009,” 23 Jan. 2009,

[http://www.nielsen-](http://www.nielsen-online.com/emc/0901_forrester/The%20Forrester%20Wave%20Listening%20Platforms%20Q1.pdf)

[online.com/emc/0901_forrester/The%20Forrester%20Wave%20Listening%20Platforms%20Q1.pdf](http://www.nielsen-online.com/emc/0901_forrester/The%20Forrester%20Wave%20Listening%20Platforms%20Q1.pdf) (viewed 14 June. 2009). The Interactive Advertising Bureau recently published

“Social Advertising Best Practices,” [http://www.iab.net/media/file/Social-Advertising-](http://www.iab.net/media/file/Social-Advertising-Best-Practices-0509.pdf)

[Best-Practices-0509.pdf](http://www.iab.net/media/file/Social-Advertising-Best-Practices-0509.pdf), which discusses some of the data capture that occurs within social media, and ways of informing users of these practices (viewed 14 June. 2009).

“mobile Internet.”⁴⁵ Many mobile marketers are eager to exploit what they correctly perceive as a unique opportunity to target consumers by taking advantage of our highly personal relationships with these extremely pervasive devices to provoke an immediate consumer response. Thus mobile devices, which know our location and other intimate details of our lives, are being turned into portable behavioral tracking and targeting tools that consumers unwittingly take with them wherever they go. Mobile marketers in the U.S. are already deploying a dizzying array of targeted marketing applications, involving so-called rich media, mobile video, branded portals, integrated avatars that offer “viral marketing” opportunities, interactive and “personalized wallpapers,” “direct-response” micro-sites, and a variety of social media tracking and data analysis tools. Technologies have also matured to now permit “the targeted and device-optimized insertion of any type of advertising (images, videos, logos, watermarks) on any type of mobile media consumer application (mobile TV, web browsing, MMS).”⁴⁶

“In addition to expanded mobile reporting capabilities,” notes *Mobile Marketing Watch*, “iPhone and Android mobile application developers can now also track how users engage with apps, just as with tracking engagement on a website. What’s more, for apps on Android devices, usage can be tied back to ad campaigns: from ad to marketplace to download to engagement.”⁴⁷

If behavioral targeting is a potent force in interactive advertising, the mobile marketplace increases the power of such targeting still further by pinpointing the

⁴⁵ As mobile marketer Amobee describes its various non-voice related applications and service offerings (including Web browsing, online games, and SMS and MMS messaging) to mobile operators, “Our unified solution allows the operator to manage user journeys across all these services in real time....” <http://www.amobee.com/main/operators.htm> (viewed 5 Dec. 2008).

⁴⁶ See, for example, “Mobile Rich Media Campaigns—A Quick Guideline,” <http://www.itsmy.biz/social>; “Vantrix Ad Booster,” <http://www.vantrix.com/products/Vantrix-Ad-Booster/> (both viewed 15 Sept. 2008). As Mobixel reveals in its product literature, “the opportunity to reach a large captive audience” through mobile advertising is “extremely enticing,” because “the mobile phone offers focused demographic, behavioral and contextual targeting and immediate engagement.” Using these capabilities, its Mobixel Ad-It service provides the tools for mobile network operators to “gather, quantify and analyze” a wide range of information about subscribers, including “demographic details, service profiles, behavioral patterns, as well as the real-time context of services, location and device and network capabilities.... It then uses this information, in real time, to make complex targeting decisions” on behalf of advertisers. “Mobixel Ad-It: Rich Media Multi-Channel Mobile Advertising Solution,” Feb. 2008, p. 2, [http://www.mobixel.com/data/uploads/Ad-It%20Brochure%20\(Feb%2008\).pdf](http://www.mobixel.com/data/uploads/Ad-It%20Brochure%20(Feb%2008).pdf) (viewed 8 Dec. 2008).

⁴⁷ “Google Expands Mobile Reporting In Analytics,” *Mobile Marketing Watch*, 22 Oct. 2009, <http://www.mobilemarketingwatch.com/google-expands-mobile-reporting-in-analytics/> (viewed 23 Oct. 2009).

precise location where various consumer behaviors take place. In the past, of course, marketers could determine the *approximate* location of mobile device users through a complex system of triangulation. But the latest generation of cellular phones, which are increasingly equipped with sophisticated global positioning capabilities, are taking all of the guesswork out of location-based targeting. Utilizing these advances in GPS technology, marketers can now determine the precise location of mobile users—within three feet.⁴⁸ As *Ad Age* noted, “Context-based banner ads now morph into GPS locators for the closest product from the user’s current location. Ads can initiate calls or purchase DVDs for instant viewing. Ads can incorporate audio, video and web browsing, and can also direct users to the iPhone App Store or iTunes.”⁴⁹ The rise of mobile/location marketing applications and coupons and accompanying data tracking and targeting, which incorporate incentives that are designed to pry more data from consumers, require special safeguards. Given that mobile marketers can now target a specific individual consumer in a specific neighborhood, location marketing requires local and state regulatory involvement as well.⁵⁰

5. Neuromarketing:

Online marketers are enhancing their data collection efforts through the purposeful use of tactics designed to take advantage of a consumers’ and citizens’ emotional and unconscious behavior. Many leading marketers are now drawing freely on the latest developments in neuroscience to drive their online and other advertising campaigns, zeroing in on our most intimate needs and vulnerabilities. Described by neuromarketing companies as a new form of “data collection,” the use of neuromarketing, “immersive,” and subliminal methods to foster consumer behavior and bypass rational decision-making is an important part of the privacy issue. As online marketers develop campaigns to take advantage of U.S. consumers’ subconscious minds to foster, for example, a willingness to opt-in, provide more data, and engage in other activities that they may not have done in the absence of such efforts, critical questions about the effectiveness of any self-regulatory or regulatory approach must be raised.⁵¹

⁴⁸ “Acuity Mobile Partners with AlphaTrek to Provide Advanced Location Targeting for Mobile Marketing Clients; Expands Patent Portfolio,” 22 Apr. 2008, <http://www.acuitymobile.com/docs/Press04222008.php> (viewed 8 Dec. 2008).

⁴⁹ Sherry Mazzocchi, “Marketers Start to Dial Up Ads for iPhone Apps,” *Advertising Age*, 24 July 2008, http://adage.com/digital/article?article_id=129861 (viewed 8 Dec. 2008).

⁵⁰ See, for example, Vertica, “Groupon Chooses Vertica for Real-Time Analytics,” http://www.vertica.com/company/news_press/95-groupon_chooses_vertica_for_real-time_analytics; Foursquare, “Foursquare for Business,” <http://foursquare.com/business/>; “Why Location Is About More than the Check-In,” *eMarketer*, 11 Jan. 2011, <http://www.emarketer.com/Article.aspx?R=1008161> (all viewed 27 Jan. 2011).

⁵¹ Robert Bain, “Duane Varan on Standards for Neuromarketing,” *Research*, 8 Oct. 2010, <http://www.research-live.com/features/duane-varan-on-standards-for->

The Nielsen Company, for example, already well established in the field of traditional audience measurement in more than 100 countries, has made a “strategic investment” in NeuroFocus, a firm that specializes in the application of brainwave research to advertising, programming, and messaging:

NeuroFocus uses established electroencephalography (EEG) technology to directly measure the brain’s reaction to a variety of stimuli.... NeuroFocus can precisely and instantaneously determine what parts of the messages they pay attention to; how they emotionally engage with them; and what is actually moved to memory. In addition, NeuroFocus blends eye tracking, galvanic skin response and other physiological parameters to provide a comprehensive solution that augments the brain wave analysis.⁵²

NeuroFocus uses “neurological testing [that] delves down to the subconscious mind,” far below such “corrupting factors” as education, language, and cultural variances, promising results that are “unambiguous, accurate, and actionable.”⁵³ In the words of NeuroFocus CEO A.K. Pradeep,

...[W]e have identified 67 specific ‘best practices’ that should be implemented when words and images are presented on a screen (any screen, from a TV or PC to a mobile phone or movie theater). They are the result of advanced neurological research into various brain functions, and especially research that has delved into the mysteries of diseases like Alzheimer’s, and brain conditions like ADD/ADHD, obsessive/compulsive behavior, and bipolar disorder.⁵⁴

neuromarketing/4003754.article; Advertising Research Foundation, “ARF Engagement Council,” <http://www.thearf.org/assets/engagement-council> (both viewed 27 Jan. 2011).

⁵² “Nielsen Makes Strategic Investment in NeuroFocus, An Innovative Leader in Neuromarketing Research,” press release, 7 Feb. 2008, http://www.nielsen.com/media/2008/pr_080207.html (viewed 24 Sept. 2008). David Penn, managing director of UK-based Conquest Research, one of the largest agencies specializing in brand and communications research, offers a more measured assessment of the potential of “neuromarketing”: “In fact, most of the exponents of neurological/biological measures are now quick to admit that their techniques are not alternatives, but complements to conventional research—either quantitative or qualitative.” David Penn, “Beyond Neuroscience—Whatever Happened to Neuromarketing?” *Admap*, Jan. 2008, www.warc.com/LandingPages/Generic/Results.asp?Ref=898 (purchase required).

⁵³ Jack Bush and A.K. Padreep, “Maximizing Message Impact for Alcon Laboratories,” presentation at the 2009 annual national conference of the PMRG, 8-10 Mar. 2009.

⁵⁴ A.K. Pradeep, “Absorption: How Messages Morph into Meaning and Value in the Mind,” Sept. 2008, http://www.neurofocus.com/pdfs/NeuroFocusWhitePaper_Absorption.pdf (viewed 16 Feb. 2010). Other companies have turned to such techniques, including functional magnetic resonance imaging (fMRI), in an effort to assess the effectiveness of various advertising campaigns. Marketers are particularly interested in research that

Studies Show the Public is Concerned about Online Privacy

Surveys conducted by reputable organizations have highlighted two important findings: Consumers highly value data privacy, but they are confused about the available protection of that privacy. Few consumers really understand the data collection system and targeted advertising environment online. A poll from the Consumer Reports National Research Center found that “72 percent are concerned that their online behaviors were being tracked and profiled by companies.”⁵⁵ Surveys by the University of Pennsylvania’s Annenberg School of Communication and the University of California at Berkeley Law School’s Samuelson Law, Technology & Public Policy Clinic also found confusion about customer data and customer privacy protections offered by businesses.⁵⁶ A 2008 Harris Interactive poll found that U.S. consumers “are skeptical about the practice of websites using information about a person’s online activity to customize website content.”⁵⁷

A June 2009 study from the UC Berkeley’s School of Information found that

... most of the top 50 websites collect information about users and use it for customized advertising. Beyond that, however, most contained unclear statements (or lacked any statement) about data retention, purchase of data about users from other sources, or the fate of user data in the event of a company merger or bankruptcy.

Sharing of information presents particular problems. While most policies stated that information would not be shared with third parties, many of these sites allowed third-party tracking through web bugs. We believe that this practice contravenes users’ expectations; it makes little sense to disclaim

addresses how “specific patterns of brain activation predict purchasing,” the potential “shopping centers in the brain,” and the neurological basis of purchasing. Brian Knutson, Scott Rick, G. Eliot Wimmer, Drazen Prelec, and George Loewenstein, “Neural Predictors of Purchases,” *Neuron* 53: 147-156; Alain Dagher, “Shopping Centers in the Brain,” *Neuron* 53: 7-8.

⁵⁵ Consumers Union, “Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy; Most Consumers Want More Control Over How Their Online Information Is Collected & Used,” 25 Sept. 2008, http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html (viewed 14 June 2009).

⁵⁶ Chris Jay Hoofnagle and Jennifer King, “Research Report: What Californians Understand About Privacy Online,” 3 Sept. 2008, http://www.law.berkeley.edu/clinics/samuelsonclinic/files/online_report_final.pdf (viewed 14 June 2009).

⁵⁷ Harris Interactive, “Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles,” 10 Apr. 2008, http://www.harrisinteractive.com/harris_poll/index.asp?PID=894 (viewed 14 June 2009).

formal information sharing, but allow functionally equivalent tracking with third parties.⁵⁸

More recently, another study (“the first nationally representative telephone survey that explores Americans’ opinions about behavioral targeting”) found that 66 percent of Americans “do not want online advertisements tailored by marketers to their specific interests.... Not only that, when informed of specific behavioral targeting techniques that marketers employ to create the ads, even higher percentages— between 73 percent and 86 percent—oppose tailored advertising. Those techniques include tracking behavior on websites and in retail stores.”⁵⁹ It seems clear, in other words, that if consumers were genuinely *aware* of the invasive marketing practices common on the Internet today, the vast majority of these Americans would have the same response: “No thanks.”

Consumers would welcome, on the other hand, a “Do-Not-Track” policy that would “allow Web browsers to opt out of all online tracking by third-parties. Gallup found that 67% of consumers said advertisers should not be allowed to present ads based on their Internet use, while only 30% said marketers should be allowed to do so. Thirty-five percent said tracking by marketers is justified because it allows free access to websites, and 61% said free access was not worth the loss of privacy.”⁶⁰

In light of these findings, we urge the adoption of regulations that will ensure that consumer privacy online is protected. The foundation for such protection should be the implementation of Fair Information Practices for the digital marketing environment. While the recent Commerce report embraces a Fair Information Principles regime, this framework is only as effective as the regulations and laws that actually create and implement privacy safeguards. The principles can be used to justify widespread data collection practices, unless they are bounded by strict policies that actually limit collection, ensure meaningful transparency (such as the FTC’s “Just-in-Time” privacy notice proposal), and ensure consumer choice and control. The so-called Notice and Choice [regime], which has been the basis of the self-regulatory system, is a failure. Despite industry efforts at self-regulation for more than a decade in the U.S., what we have witnessed is steadily increasing data collection and use—all without the real, informed understanding and consent of

⁵⁸ “Consumer Advocacy Group Comments In the Matter of a National Broadband Plan for Our Future,” Center for Digital Democracy, Privacy Rights Clearinghouse and U.S. PIRG, FCC Docket 09-51, June 2009, <http://www.democraticmedia.org/node/405> (viewed 14 June 2009).

⁵⁹ “Americans Reject Tailored Advertising: Study Contradicts Claims by Marketers,” 30 Sept. 2009, <http://www.asc.upenn.edu/news/NewsDetail.aspx?nid=612> (viewed 29 Oct. 2009).

⁶⁰ Mercedes Cardona, “Gallup: Two-thirds of consumers would back ‘Do-Not-Track,’” *Direct Marketing News*, 22 Dec. 2010, <http://www.dmnews.com/gallup-two-thirds-of-consumers-would-back-do-not-track/article/193260/> (viewed 23 Jan. 2011).

users.⁶¹ The failure to adequately regulate the financial sector greatly contributed to the worst economic crisis since the Great Depression. In the new online world, where we conduct our financial, health, and personal affairs online and via mobile devices, we must strive to develop the most effective means of safeguarding privacy. Online commerce and publishing will thrive even more as consumers are assured their privacy has been effectively safeguarded.

We call on the Department of Commerce to revise its analysis and recommendations as it develops the final white paper on privacy. It should incorporate recommendations from the FTC's recent "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"; utilize comments from consumer and privacy groups filed in both proceedings; reflect the analysis done by the international Article 29 Working Group (including reviewing and embracing that regulatory body's informed-consent discussion on behavioral targeting); make a commitment to support the EU data protection regime and to seek a strong framework for APEC; promote the role of the FTC and other independent agencies (such as the CFPB for consumer financial privacy online) as the lead privacy policy organizations; support meaningful protections for children, adolescents, and other vulnerable users; affirm the need for strong regulatory rules on sensitive information; and revise its framework to address contemporary digital and offline data collection practices more effectively. Additionally, the Obama administration should make it a high priority to ensure meaningful affirmative consent prior to data collection, including in social media and mobile applications.

We reject the notion that protecting privacy will somehow undermine the "health" of the Web by restricting advertising. Conflating the Internet and democratic discourse with the contributions from online ad revenues, as the industry lobbyists frequently do, reflects a cynical attempt to scare Internet users into accepting invasive advertising practices. The Web is more than simply the sum of its commercial parts. Online ad revenues are important, certainly, and they will continue to grow as the new media displace the old in the advertising landscape. But this growth need not come at the expense of consumer privacy and welfare. In the absence of data protection and consumer rules, in fact, a number of online ad applications—for example those involving online lead generation, digital financial marketing, and so-called "e-pharma"—can actually incur real harm and economic loss.⁶²

⁶¹ Industry, moreover, has played a role in misleading consumers in the area of online privacy. See, for example, Pedro Giovanni Leon, Lorrie Faith Cranor, Aleecia M. McDonald, and Robert McGuire, "Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens," Carnegie Mellon University CyLab, 10 Sept. 2010, http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab10014.pdf (viewed 24 Jan. 2011).

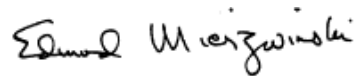
⁶² Center for Digital Democracy, U.S. PIRG, Consumer Watchdog, and World Privacy Forum, "In the Matter of Online Health and Pharmaceutical Marketing that Threatens Consumer Privacy and Engages in Unfair and Deceptive Practices. Complaint, Request for

The uncertainty over the loss of privacy and other consumer harms will continue to undermine confidence in the online advertising business. That's why the online ad industry will actually *benefit* from privacy regulation. Given a new regulatory regime protecting privacy, industry leaders and entrepreneurs will develop new forms of marketing services where data collection and profiling are carried out in an above-board, consumer-friendly fashion. Consumer and privacy groups have already pledged to work closely with Congress to help draft a law that balances the protection of consumers with the interests of the online marketing industry, and CDD will submit more a detailed analysis of online privacy in response to the FTC's request for comments in mid-February 2011.

Respectfully submitted,



Jeff Chester
Executive Director
Center for Digital Democracy
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009



Ed Mierzwinski
Consumer Program Director
U.S. PIRG
218 D St. SE
Washington, DC 20003

The Center for Digital Democracy is a nonprofit group working to educate the public about the impact of digital marketing on public health, consumer protection, and privacy. It has played a leading role at the FTC and in Congress to help promote the development of legal safeguards for behavioral targeting and other online data collection practices.

U.S. PIRG serves as the federation of non-profit, non-partisan state Public Interest Research Groups. PIRGs are public interest advocacy organizations that take on powerful interests on behalf of their members. For twenty years, U.S. PIRG has been concerned with privacy and compliance by governments and commercial firms with Fair Information Practices.

Investigation, Public Disclosure, Injunction, and Other Relief: Google, Microsoft, QualityHealth, WebMD, Yahoo, AOL, HealthCentral, Healthline, Everyday Health, and Others Named Below."