Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	**)**	
	)	
A Preliminary FTC Staff Report on	**)**	**File No. P095416**
Protecting Consumer Privacy	**)**	
in an Era of Rapid Change:	**)**	
A Proposed Framework for	**)**	
Businesses and Policymakers	**)**	

COMMENTS OF

The Center for Digital Democracy
and
U.S. PIRG

18 February 2011

The Center for Digital Democracy (CDD) and U.S. PIRG (US Public Interest Research Groups) supports the Federal Trade Commission staff's call for the establishment of a comprehensive "framework for how companies should protect consumers' privacy." We urge the Commission to incorporate suggestions made in this Comment, as well as other recommendations that will strengthen the practical impact of the new framework. The Commission staff report demonstrates that the FTC has made significant strides toward a better understanding of how contemporary digital marketing practices both threaten personal privacy as well as affect the consumer's ability to engage autonomously in transactions that touch on their finances, health, families, and other personal matters. The staff has accurately understood that "changes in technology and the emergence of new business models also have new implications for consumer privacy." The Commission must now act swiftly to finalize and implement the staff report's recommendations. It is aware, of course, of the important investigative findings of the *Wall Street Journal*, which, in its "What They Know" series, declared that "one of the fastest-growing businesses on the Internet… is the business of spying on Internet users."[1] U.S. consumers should not be placed at risk any longer from a commercial surveillance system that disregards their personal privacy.

It is the Commission's role and responsibility to protect U.S. consumers—and it must continue on a course that addresses the serious threats that much of online data collection embodies. The staff's multi-dimensional framework, given the right mix of implementation requirements, would significantly safeguard consumers online. The Commission staff is correct in asserting, from evidence provided through the FTC privacy roundtables, that the consumer has a "lack of understanding about the collection and use of their personal data, and the corresponding inability to make informed choices." Few consumers fully understand how online data collection works as part of contemporary digital marketing practices, although, as a recent Gallop/USA poll indicated, the majority of the public oppose being tracked and targeted online with behavioral ads.[2] Today's consumers should not be expected to be able to make informed decisions about how to protect their privacy in a system intentionally shaped to foster data collection through "360-degree" and other invasive digital marketing strategies.[3] Indeed, how online marketing and data

---

[1] 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/ (viewed 10 Feb. 2011).

[2] Jack Marshall, "U.S. Users Opposed to Behavioral Targeting, Gallup Poll Suggests," ClickZ, 21 Dec. 2010, http://www.clickz.com/clickz/news/1934047/users-opposed-behavioral-targeting-gallup-poll-suggests (viewed 10 Feb. 2011).

[3] Advertising Research Foundation, "360 Media and Marketing Council," http://www.thearf.org/assets/360-media-council; Advertising Research Foundation, "The ARF Inaugural NeuroStandards Retreat," http://www.thearf.org/assets/neurostandards-meeting both (viewed 10 Feb. 2011).

collection operate is purposefully hidden from consumers (and policymakers). The "Notice and Choice" regime used today fails to accurately inform users about the various methods used to solicit and use their data. The "Harms" approach can play an important role—but it is really only recently that the Commission has even begun to address how the dynamics of online marketing can threaten consumer welfare. One of the key challenges to the FTC is to require that online marketers accurately inform consumers, via the proposed "Just-in-Time" notices and new forms of opt-in control, exactly what they tell their clients and prospective clients about how the system *actually* works.

Through the Commission's series of roundtables it has identified many of the outstanding problems that it must now address in a final report and plan. These include "the ubiquitous collection and use of consumer data," "consumers' lack of understanding and ability to make informed choices about the collection and use of their data," "the importance of privacy to consumers," and the "blurring of the distinction between personally identifiable information and supposedly anonymous or de-identified information." We concur that the Commission's new framework should apply to both "online and offline commercial entities that collect, maintain, share or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device."

CDD and U.S. PIRG urge the Commission to help bring new standards of candor to the so-called "privacy-by-design" approach. Indeed, that approach has many limitations, given the far-reaching nature of contemporary data targeting. Many marketers desire to capture and harvest user data on a continual basis, beyond a "specific business purpose." Vast amounts of user data are now regularly mined and stored in behavioral targeting warehouses and other databases—and used in an instant to update online targeting profiles. Any privacy-by-design regime truly committed to privacy will limit such ongoing data collection and use. The Commission should create guidelines to help direct the "privacy by design" field. One crucial element is a requirement that a commercial website that collects data must clearly and prominently tell a consumer exactly what is actually being collected, what methods are used, and how the data will be used—a process that is practically nowhere to be found online today. A privacy-by-design system must inform users that techniques such as landing-page optimization, eye-tracking, viral and rich-media applications, and data collected via behavioral "intent" warehouses have been incorporated into a website's strategic data collection approach.[4]

---

[4] See, for example, Experian, "Digital Advertising," http://www.experian.com/business-services/digital-advertising.html?cat1=marketing-services; DataXu, "Who We Partner With," http://www.dataxu.com/we-work/who-we-partner-with/; SiteSpect, "Benefits of Behavioral Targeting," http://www.sitespect.com/behavioral-targeting.shtml; Enquiro, "Research Services," http://www.enquiro.com/services/research.php (all viewed 12 Feb. 2011).

We also agree with the Commission staff recommendation that "companies provide choices to consumers about their data practices in a simpler, more streamlined way…." The "Just-in-Time" notice is an appropriate method that can ensure that a consumer receives accurate and timely information about the data collection process. But it must convey an accurate statement on the process—otherwise the site should be held to Commission action under Section 5 as unfair and misleading. The current self-regulatory icon-based scheme now being implemented by the online ad industry is both insufficient and unreliable as a method to inform a consumer of the privacy implications of a given site. The industry is going to need the guidance of the Commission and the input from consumer and privacy groups in order to identify which practices require meaningful consent and safeguards.

Do Not Track

We fully support the implementation of a Do-Not-Track system that provides consumers with a powerful and more reliable tool to help protect their privacy While ad industry lobbyists dismiss the need for DNT because they claim they don't track individuals, the IAB's own definition of behavioral targeting ("A method that enables advertisers to show an ad specifically to visitors based on their Targeting shared behavioral, demographic, geographic and/or technographic attributes") makes clear that specific individual consumers *are* being tracked and targeted online, claims to the contrary notwithstanding.[5] The IAB defines a "behavioral event" as a "user-initiated action which may include, but [is] not limited to: searches, content views, clicks, purchases, form-based information and other interactions."[6]

We will discuss below how the growing integration of first- and third-party data illustrates that a consumer's relationship with a frequently used website requires new forms of privacy safeguards. Today, most privacy policies fail to accurately disclose a site's or service's data collection practices. Privacy policies must acknowledge contemporary digital marketing and data collection techniques. The Commission should develop a new standard for privacy policies that will ensure their intellectual rigor and honesty. We concur that meaningful "transparency" is required and that consumers should have the right to access and edit any files containing data collected about them online.

---

[5] IAB, "Networks & Exchanges Quality Assurance Guidelines," June 2010, http://www.iab.net/media/file/NE-QA-Guidelines-Final-Release-0610.pdf (viewed 10 Feb. 2011).

[6] The IAB also defines "Attribute [as a] …single piece of information known about a user and stored in a behavioral profile which may be used to match ad content to users. Attributes consist of demographic information (e.g., age, gender, geographical location), segment or cluster information (e.g., auto enthusiast), and retargeting information (e.g., visited Site X two days ago). Segment or cluster information is derived from the user's prior online activities (e.g., pages visited, content viewed, searches made and clicking and purchasing behaviors). Generally, this is anonymous data (non-PII)." IAB, "Networks & Exchanges Quality Assurance Guidelines."

The Contemporary Digital Marketing Landscape

No discussion of privacy can occur without understanding the overall context of how online marketing actually operates. There has been a serious lack of scholarly research on the "digital marketing ecosystem," as the industry calls it, and its impact on consumer welfare—including privacy. Much of the research cited (and often funded) by industry to support the behavioral targeting and consumer data collection status quo suffers from a lack of analysis of the real dimensions of interactive advertising. As we have stated elsewhere in academic journals and other publications, "Digital marketing departs in significant ways from traditional forms of marketing, challenging the prevailing theories and methods that have guided media research in the past…. In the digital marketing environment, advertising, editorial content, and measurement have been completely intertwined."[7] Consumers need to be explicitly informed how much of online marketing has been structured to facilitate the collection of use of consumer data. Today, a consumer has to navigate through a system that provides nearly ubiquitous connectivity—including location-oriented services—and that has data collection at its core. Online marketing campaigns are designed to foster forms of "engagement," creating deeper emotional and other connections that promote interactions between brands, products, and users. Online marketers also facilitate the data collection process using methods involving so-called "user-generated content" that makes a consumer an active—but largely unaware—participant in the data collection process. "Personalization" is used by digital marketers to make "personalized marketing and sales appeals based on a customer's unique preferences, behaviors, and psychological profile." Harnessing the "social graph"—one's connections of friends and networks via the myriad of social media marketing techniques—permits marketers to collect a wealth of consumer data. The purposeful use of "immersive" environments, including sites developed using rich media and neuromarketing (implicit persuasion), are designed to promote new methods of data collection that bypass the rational decision-making process of a consumer.[8] New privacy regulations must be grounded in a more complete understanding of contemporary online marketing.

We understand and appreciate the benefits to online consumers, publishers, and others connected to the digital marketing system. Online marketing provides significant opportunities for consumers to become better informed and to engage in

---

[7] Kathryn Montgomery, Sonya Grier, Jeff Chester, and Lori Dorfman, "A Conceptual Framework for Food Marketing in the Digital Age," 2011, unpublished manuscript.

[8] Montgomery, Grier, Chester, and Dorfman, "A Conceptual Framework for Food Marketing in the Digital Age"; Jeff Chester and Kathryn Montgomery, "Interactive Food & Beverage Marketing: Targeting Children and Youth in the Digital Age," May 2007, http://www.digitalads.org/documents/digiMarketingFull.pdf (viewed 15 Oct. 2008); Kathryn Montgomery and Jeff Chester, "Interactive Food & Beverage Marketing: Targeting Adolescents in the Digital Age," *Journal of Adolescent Health* 45, n. 3, Suppl. (Sept. 2009): S18–S29.

a broader range of transactions. Online ad revenues are an important source of funding for publishers, other content sites, and advertising and marketing companies. But it is very disturbing that a number of digital marketing industry representatives and lobbying groups—with a vested interest in maintaining the digital data collection and online interactive marketing status quo—disingenuously claim that if consumer privacy is respected and protected the Internet will succumb to a "digital depression." There is absolutely no serious evidence presented by the industry—and most of the academic research they have funded—that such would be the case. The Commission (and other policymakers) should reject these scare tactics. Online marketing is growing as an industry not because of the increasing behavioral targeting and other forms of data collection it has embraced. The growth of online advertising is primarily due to the significant changes in consumer media usage—more and more people are online and using various digital channels and devices, most notably mobile phones.[9] The flow of revenues into online advertising is a reflection that today's users—especially young people—are fully connected to the digital marketplace. Online marketers developed behavioral targeting and many other forms of online consumer data collection without ever taking privacy in mind. While such digital data collection tactics generate additional revenues, they do so at the expense of privacy and impose other costs on consumers. No one has suggested that digital marketing be prohibited—just that a consumer be able to make informed decisions about the process.

Ironically, just three years ago, the Interactive Advertising Bureau—the online ad industry's principal trade association—denied there was an online privacy problem at all. Forced to address the issue because of pressure from the European Union, the FTC, and congressional leaders from both parties, as well as from the growing public concern about privacy (including from the *Wall Street Journal* and state attorneys general), the IAB and others now admit privacy is a concern. But these lobbying groups still cling to a flimsy argument that the economic health of the Internet will be jeopardized if the FTC imposes reasonable consumer privacy safeguards. Some of the research conducted and cited by industry, such as the work of Avi Goldfarb and Catherine E. Tucker, which offer claims that privacy safeguards diminish online ad revenues, do not hold up to review.[10] Indeed, online ad revenues in the EU (the focus

---

[9] Kathryn Zickuhr, "Generations Online in 2010," Pew Research Center, 16 Dec. 2010, http://pewresearch.org/pubs/1831/generations-online-2010; Microsoft Advertising, "Understanding the Digital Audience: Reaching Youth," http://advertising.microsoft.com/uk/reaching-youth (both viewed 12 Feb. 2011).

[10] See, for example, Avi Goldfarb and Catherine E. Tucker, "Advertising Bans and the Substitutability of Online and Offline Advertising," *Journal of Marketing Research* (forthcoming), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600221 (viewed 15 Feb. 2011); Avi Goldfarb and Catherine E. Tucker, "Online Display Advertising: Targeting and Intrusiveness," *Management Science* (forthcoming), http://www.rotman.utoronto.ca/~agoldfarb/GoldfarbTucker-intrusiveness.pdf; Avi

of Professors Tucker's and Goldfarb's "Privacy Regulation and Online Advertising") have been robust—and the growth of behavioral targeting has been largely unaffected by its data privacy regime.[11] Similarly, Howard Beales, in work funded by online marketers, misinterprets the nature of behavioral advertising and its actual costs for consumers.[12]

Based on the polls and surveys done by independent experts, including UC Berkeley and the University of Pennsylvania, the Commission should reject this assertion. Ensuring consumer privacy will only boost e-commerce and online marketing, as the public is assured that their dealings online are being handled with the care they deserve.[13]

The Need to Protect Consumer Privacy in the "Big Data" Era

Goldfarb and Catherine E. Tucker, "Search Engine Advertising: Pricing Ads to Context," *Management Science* (forthcoming).

[11] Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," *Management Science* 57, n. 1, (Jan. 2010): 57-71, http://mansci.journal.informs.org/cgi/rapidpdf/mnsc.1100.1246v1; IAB Europe, "AdEx—The Definitive Guide to the Size and Scale of European Online Advertising," http://www.iabeurope.eu/research/adex-%E2%80%93-the-definitive-guide-to-the-size-and-scale-of-european-online-advertising.aspx; Robert Andrews, "Forecast: Online Will Take More Ad Dollars Than Newspapers By 2015," paidContent:UK, 8 Dec. 2009, Forecast: Online Will Take More Ad Dollars Than Newspapers By 2015; Karin von Abrams, "Online Ad Spending in Western Europe," eMarketer, Oct. 2009, http://www.emarketer.com/Reports/All/Emarketer_2000609.aspx; Karin von Abrams, "Western Europe Online Ad Spending: Leading the Recovery ," eMarketer, Oct. 2010, http://www.emarketer.com/Report.aspx?code=emarketer_2000724; Microsoft Advertising—Europe, "Audience Targeted Ads," http://advertising.microsoft.com/europe/audience-targeted-ads; Google for Advertisers—UK, "Success Story Archive," https://services.google.com/advertisers/uk/success/archive?sort=date; and Chris Morrison, "Europe's Facebook Growth Moved East in June 2010," Inside Facebook, 6 July 2010, http://www.insidefacebook.com/2010/07/06/europes-facebook-growth-moved-east-in-june-2010/ (all viewed 12 Feb. 2011).

[12] Howard Beales, "The Value of Behavioral Targeting," 2010, http://www.scribd.com/doc/29301297/The-Value-of-Behavioral-Targeting (viewed 12 Feb. 2011).

[13] Eric Eldon, "November 2010 Facebook Traffic: Usual Growth Worldwide, Slower in US, Measurement Firms Show," Inside Facebook, 3 Jan. 2011, http://www.insidefacebook.com/2011/01/03/november-2010-facebook-traffic/; Randall Rothenberg, "War Against the Web," Huffington Post, 21 Apr. 2008, http://www.huffingtonpost.com/randy-rothenberg/war-against-the-web_b_97811.html (both viewed 12 Feb. 2011).

Both the privacy and welfare of consumers in the U.S. are being placed at risk every day, by what online marketers refer to as the era of "Big Data."[14] Consumers today confront a powerful and far-reaching data collection and targeting system that uses advanced and largely stealth means to extract information and influence their decisions—including for sensitive transactions involving finance, health, and families. Consumers are unaware of the data optimization and "self-tuning" algorithms, predictive targeting, the use of "Intent" and "unique personal" data from outside databases, re-targeting, cross-channel targeting, and "real-time bidding" systems that play a growing role in shaping their online experience.[15]

As we have previously explained to the commission, the fundamental foundation of online marketing is the one-to-one marketing paradigm, first discussed in the mid-1990's.[16] Some in the online marketing industry claim, disingenuously, that steady advances in online marketing-related data collection practices pose an obstacle to sensible privacy safeguards. Nothing could be farther from the truth. The over-arching goal is the collection and use of ever-greater amounts of a consumer's information, across all platforms and many applications. In our comments, CDD and U.S. PIRG will review some of the most recent developments in the "Big Data" era, and how they affect consumers' privacy and their transactions.

As a January 2011 report from Econsultancy explains, "Data has become one of the most valuable commodities in the real-time bidding system. There is a fundamental shift in media buying from buying placements to buying audiences."[17] As we noted in our April 2010 FTC complaint, individual consumers are now being bought and sold via online ad exchanges and other services so they can be targeted with interactive advertising.[18] A complex array of data is collected and used for consumer profiling, tracking, and targeting on these "exchange" and "demand-side" platforms. Data collected on an individual user, including via behavioral tracking, "intent" data warehouses, and outside databases, are used to determine the value of an individual

---

[14] James Hutchinson, "Big Data to Get Even Bigger in 2011," *InfoWorld*, 20 Jan. 2011, http://www.infoworld.com/d/data-explosion/big-data-get-even-bigger-in-2011-064 (viewed 15 Feb. 2011).

[15] Econsultancy, "Demand-Side Platforms Buyer's Guide," 2011, p. 41, http://econsultancy.com/us/reports/dsps-buyers-guide (purchase required).

[16] Don Peppers and Martha Rogers, *The One to One Future* (New York: Random House, 1999).

[17] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 3.

[18] 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," Federal Trade Commission filing, 8 Apr. 2010, http://www.democraticmedia.org/real-time-targeting (viewed 9 Feb. 2011).

targeting "impression." In the words of computational advertising company Rocket Fuel, companies can buy "individual impressions of the users that matter most—the ones …determined [to] fit [a] customized data-driven audience profile."[19]

Consumers don't understand—nor should they be expected to understand—a "custom targeting" system that uses wide-ranging data sets to determine "the absolute value of each impression" for an advertiser. A consumer is tracked beyond the click, including content they access via "brand pages," as well as what they download, forms filled out, etc. For example, how and why should any user have to know how a data-targeting "demand-side platform" operates and will impact their privacy and consumer decision-making? As Econsultancy recently explained, a demand-side platform

- Connects to multiple inventory sources (e.g. ad exchanges, optimizers), creating a significant pool of impressions.
- Calculates the value of an impression relative to its characteristics in real time.
- Makes decisions on what impressions to bid for and what price to bid for each in real time…
- Enables data integration with third party data providers, agencies, analytics companies and clients.
- Integrates data, targeting, optimization, analytics, impression attribution and reporting…
- Makes the media and data buying process more transparent and efficient.
- Enables media buyers to manage and optimize their campaigns in real time though a single interface.
- Provides better insight into users' behavior and allows retargeting across numerous platforms.[20]

Econsultancy explains that "Ad exchanges, demand-side platforms and supply-side platforms… [provide] efficiency, transparency, lower transaction costs and better targeting."[21] DataXU's Mike Baker notes that "demand-side platforms that can automatically process data to discover new audiences at scale, optimize performance, and uncover unique insights into consumer behavior will attract more and more of the growing digital ad budgets currently flowing through the ad networks."[22] Indeed, the rise of techniques heavily harvesting identifiable data sets for user targeting moves online marketers away from what is now being called a more "black box approach" from online ad networks.[23]

---

[19] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 92.

[20] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 10.

[21] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 13.

[22] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 13.

[23] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 14.

Among the benefits to online publishers, marketers, and data brokers from ad exchange-related services is the ability to better target a user. One can now "precisely identify and target desired audiences and behavior, without using content as a proxy"; use "Impression-level-bidding [to] make cookie retargeting more scalable and powerful; Execute cross-sell, up-sell and retention campaigns by leveraging customer relationship management databases and third-party data."[24] In deciding which advanced online targeting technology company to use, marketers are told they should ask themselves a range of data-related questions, including "Who are their data partners; Is the company able to integrate and manage first-party data as well as third-party data sources? Can you use data from any third-party provider or are you limited to certain providers only? What types of data can the platform integrate, e.g., intent data, unique personal data? Does the platform have predictive targeting… capabilities? Are cross-platform buying capabilities (e.g., Facebook, Google Adwords) offered?" Questions that should be asked on "targeting and optimization" include: "Is the optimization approach rules-based or algorithmic-based?; Are the algorithms static or dynamic?; Does the DSP offer real-time assessment, page-level optimization and automated optimization? …What targeting approaches does the DSP offer (e.g., demographic, contextual, behavioral, geo-targeting, retargeting, multivariate targeting)?"[25]

Many of the data targeting companies involved in today's behavioral profiling marketplace incorporate so-called "intent data" from companies such as BlueKai, eXelate, and AlmondNet, along with "unique personal data" from vendors that include TARGUSinfo and Experian.[26] Demand -side platform company DataXU explains that it has moved "beyond the limitations of… [purchasing] audiences using cookies …[to] impression level decisioning… across mobile, video and online channels."[27] Online behavioral profiling companies have assembled a long list of data partners for their targeting infrastructure, including Yahoo!, Bizographic, Acxion, Datalogic, Lotame, Magnetic, Nielsen, Quantcast, AdMeld, AdBrite, Pubmatic, Rubicon and many others.[28] A publisher or advertiser can bring their own data into the targeting mix, including the use of "tracking beacons" and other data sets.[29]

But while online marketers and publishers have greater transparency and control over the targeting process, consumers do not. The Commission must force open the privacy-threatening practices of the digital wizards of data Oz operating behind the

---

[24] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 23.

[25] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 33.

[26] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 44.

[27] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 53.

[28] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 61.

[29] Econsultancy, "Demand-Side Platforms Buyer's Guide," pp. 67, 82.

exchange, demand, and supply-side curtains.[30] The need to establish privacy and other consumer safeguards across platforms should be one of the highest FTC priorities. Mobile, video, and social media are increasingly being integrated into the data collection and targeting real-time bidding apparatus.[31] Growing investment in online marketing and data collection companies is expanding the field's capacity to deliver advertising based on the harvesting of a users' online data. But while the data targeting industry is expanding through investment and acquisitions, consumer privacy protections are failing to keep up with the market.[32]

Opt-in, First- and Third-Party sites

Consumers should be accorded the same kind of user opt-in control on first-party and third-party sites alike. First-party sites, it is clear, engage in a wide range of data collection and targeting approaches unknown even to their regular visitors, and user consent for these practices should be required. In addition, as first-party publishers increasingly engage in forms of data sales and sharing for the purposes of consumer tracking and targeting, the distinctions between first and third parties are eroding. As we explained in our FTC complaint on online ad exchanges, it's increasingly not a case of *where* one is online, but rather *who* one is that ignites and informs the data collection, profiling, and targeting process.[33]

For example, many first-party sites are now using SiteCatalyst (and its behavioral targeting product) as a means of adding external databases to the mix of personal data used for targeting purposes. As LUMA Partners' Terence Kawaja recently observed about Adobe Systems' acquisition of data management provider Demdex, "…. Advertisers will be able to combine its first-party SiteCatalyst data with third party data to identify and categorize the site visitors, and then effectively target

---

[30] Adnetik, "How it Works," http://www.adnetik.com/how-it-works/ (viewed 15 Feb. 2011).

[31] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 7.

[32] See, for example, Devindra Hardawar, "Google Acquires Invite Media to Help Users with Ad Exchanges," VentureBeat, 2 June 2010, http://venturebeat.com/2010/06/02/google-acquires-invite-media-to-help-users-with-ad-exchanges/; David Kaplan, "VC Money Keeps Pouring In For Ad Targeters: Turn Raises $20 Million," paidContent.org, 5 Jan. 2011, http://paidcontent.org/article/419-vc-money-keeps-pouring-in-for-ad-targeters-turn-raises-20-million/ (both viewed 15 Feb. 2011).

[33] 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," Federal Trade Commission filing, 8 Apr. 2010, http://www.democraticmedia.org/real-time-targeting (viewed 9 Feb. 2011).

high-value audience segments with display advertising campaigns."[34] And according to John Mellor, Adobe Omniture's vice president of marketing, "We have seen that the buying and selling of online ads has undergone dramatic changes in the past 18-24 months that put data at the center of buying and selling decisions. With real-time bidding exchanges and similar technologies, an advertiser can decide at the point of impression whether or not it's valuable...."[35]

Underscoring the need for immediate FTC and other federal action are the growing privacy and other threats to consumers from the real-time auctions of individuals online, which are said to be evolving at "lightning speed." As a new report on the "Mechanics of Real-Time Bidding" illustrates, the extensive system of online tracking and targeting permits an ad to be "delivered to the user within milliseconds" after an auction of that person is done online. "Advertisers are granted unprecedented access to the users they're trying to target," notes the report, "while removing the users they'd rather ignore." Such Real-Time buying and selling of users was expected to account for "20% of all display advertising spend" in 2010. The report makes clear that consumers are increasingly vulnerable to having their data made available to marketers: "Buyers have greater access to audience, and most critically, highly targeted audiences, than they ever did before."[36] Consumer privacy is also at risk, through the growth of "data leakage," where "advertisers will capture information about users they are interested in targeting on one site, then go out and find cheaper inventory through which to access the same users."[37]

---

[34] "LUMA Partners' Kawaja On Demdex Sale To Adobe," AdExchanger.com, 3 Feb. 2011, http://www.adexchanger.com/venture-capital/luma-partners-demdex-adobe/ (viewed 9 Feb. 2011).

[35] "Adobe Omniture VP Mellor Reviews Acquisition Of Data Platform Demdex," AdExchanger.com, 18 Jan. 2011, http://www.adexchanger.com/online-advertising/adobe-omniture-demdex/. For its part, Demdex makes clear its data acquisition capabilities:

> Capitalize on all your audience & demographic data.
> SegmentID is a turn-key audience data management solution that empowers you to cost-effectively create a "Data Bank" of audiences and integrate them into all your online efforts. It also manages the third party data you buy from data exchanges or other data sellers to ensure you get the maximum benefit from your data. The result is a central repository of data that will dramatically improve all your targeting, segmentation, or analytic efforts.

Demdex, http://www.demdex.com/index.html (both viewed 9 Feb. 2011).

[36] The Rubicon Project, "Mechanics of Real-Time Bidding," 2011, http://www.rubiconproject.com/market-intelligence-download (registration required).

[37] "Here's how that risk comes into play: during the bid process, some quantity of publisher and user information is sent to each bid partner. Only one bid partner will ultimately pay for that impression, but even non-winning bid partners are exposed to the data (non-PII) and know that user (identified by a non-PII, numeric ID) visited the publisher's web site. Also, DSPs will often do a cookie pairing to insert their unique user identifier into the publisher or ad serving platform's cookie. This allows the token to be retrieved when an ad request is

Behavioral Targeting and Data Mining

The failure of the FTC and other policymakers to act to protect a consumer's privacy has led to the emergence of behavioral targeting warehouses and "co-ops." Online marketers appear to believe that they have been given free license to stealthily collect and then financially benefit from an individual consumer's personal information. For example, Akamai says it "operates the industry's only online shopping data co-op" that harvests data of "140 million U.S. consumers... made up of over 550 multi-channel retailers, product manufacturers, travel, and telecom websites who contribute data representing $13.5 billion worth of quarterly ...consumer shopping transactions. This unique data set makes it possible for Akamai ADS to understand the distinctive behavioral patterns shoppers exhibit leading up to a purchase—and thus identify in-market consumers with accuracy."[38] Among the areas Akamai targets are "health and wellness seekers, college students, moms with kids."[39]

BlueKai, meanwhile, claims to be "operating the largest data exchange focused on identifying consumer intent in the advertising world as well as bringing to market the most advanced data management platform available to marketers."[40] According

---

made by that user. That token is passed, as part of the bid request, back to the DSP. The auction identifier and the publisher's user identifier are often incorporated into each bid request as well. If these two elements of the bid request are not encoded in such a way that is unique to each bid partner they can act as naked foreign keys that allow otherwise disparate bid partners to merge their data. In other words, this data appending is a subtle type of unintentional data leakage by the publisher." Rubicon Project, "Mechanics of Real-Time Bidding." For another report on consumer data "leakage," see "Krux Digital Study: Significant Data Skimming Leads to Revenue Loss for Premium Publishers," 9 Nov. 2009, http://www.kruxdigital.com/news/press-release-significant-data-skimming-leads-to-revenue-loss.html (viewed 10 Feb. 2011).

[38] Akamai, "ADS Predictive Segments," http://www.akamai.com/html/solutions/ads_predictive_segments.html (viewed 9 Feb. 2011).

[39] Akamai also explains that its "Shopographics—audience segmentation based on shopping data—yields better ad targeting response than demo-, psycho-, or geographics, combined! How people spend their money is the most accurate descriptor of who they are and what they're likely to be interested in — more so than what they read, watch, or like online. That's why Akamai ADS operates the world's only online shopping data cooperative, representing an estimated $15 Billion in U.S. consumer spend quarterly and nearly 100% of online shoppers." Akamai, "ADS Descriptive Segments," http://www.akamai.com/html/solutions/ads_descriptive_segments.html (viewed 9 Feb. 2011).

[40] BlueKai, "Jobs: Client Service Manager," http://www.bluekai.com/aboutus_jobs.php#account_executive_chicago_nyc (viewed 9 Feb. 2011).

to BlueKai, the company has taken us from the "Data Dark Ages" to the "Data Renaissance": "For the first time in history, advertisers can target individual consumers independent of their media choices. At the heart of this vision is a simple, but proud truth: Data is king. True audience targeting is driven by superior data. By decoupling media from targeting data, we've created an enlightened data economy that compensates data sellers with maximum yields and buyers with performance-driven data that delivers consistent results. This vision makes it possible to reach anyone, anywhere on the web."[41] BlueKai assures prospective clients that they will be able to "[a]ccess actionable audience data on more than 200 million users. That's over 80% of the entire US Internet population at your fingertips.... BlueKai Exchange offers more than 30,000 data attributes to power any branding or direct marketing initiatives you can imagine. The BlueKai Exchange transacts over 75 MM auctions daily."[42] BlueKai offers marketers the ability to track and target a consumer's financial interests through the sale of their data related to credit cards, mortgages and refinancing, retirement, and other financial service products. Data targeting college and private school students, as well as their parents, are also offered. Among BlueKai's data partners are Fox, DataXU, Microsoft, Yahoo, and Valueclick.[43]

eXelate, similarly, enables "data buyers [to] build an instant behavioral targeting function and optimize their campaign delivery, while data sellers gain direct control over their audience data distribution.... The eXchange includes over 50 top ad network, agency and demand-side platform buyers and dozens of leading publishers, who deliver targeting data on nearly 200 million U.S. unique users in verticals including Business-to-Business, Auto, Travel, Finance, Shopping and registration-based Demographics."[44] A consumer's data are trafficked and sold, including for targeting relating to race or ethnicity, financial interests, political views, health concerns, and big-ticket purchases. The company explains that "Each month we capture rich targeting data on over 150M U.S. UV [unique visitors] via a rigorous set of data collection, filtering, segmentation and normalization procedures.... All of eXelate's online-based activity data is directly sourced from online publisher partners via tags located on web pages in which consumers interact with relevant content or queries. Via this tag, eXelate is able to drop a 'targeting cookie' which collects relevant activity...." The company uses a consumer's data for targeting that "may be limited to a specific deep action (such as a shopping search, or lead generating auto interaction), while in others, such as age or gender,

---

[41] BlueKai, "About Us," http://www.bluekai.com/aboutus.php (viewed 9 Feb. 2011).

[42] BlueKai, "The BlueKai Exchange," http://www.bluekai.com/exchange.php (viewed 9 Feb. 2011).

[43] BlueKai, "Intent Data," http://www.bluekai.com/intentdata.php; http://www.bluekai.com/intentdata_bluekaiinside.php (both viewed 9 Feb. 2011).

[44] eXelate, "eXelate Launches Premier Media Partnership," 18 Jan. 2011, http://www.exelate.com/home/inside-press-releases-28.html (viewed 9 Feb. 2011).

multiple registration-based data points may be accumulated on the user in the segment."[45] Nor is the online advertising industry standing still in its capacity to collect and analyze data for consumer targeting, as the recent Knowledge Discovery and Data Mining conference makes clear.[46]

Big Data and Big Lies

The FTC should immediately adopt a policy that makes it clear that information on a unique user collected via a unique identifier and other tracking technologies is by its very nature "personally identifiable." Online marketing companies continually claim that they collect and use only non-personal information. However, even a cursory

---

[45] eXelate, "Data 101 FAQs," http://www.exelate.com/home/advertiser-data-101-faqs.html (viewed 9 Feb. 2011).

[46] KDD-2010, "Workshop 8: The Fourth International Workshop on Data Mining and Audience Intelligence for Online Advertising (ADKDD'10)," 25 July 2010, http://kdd10.crowdvine.com/talks/14075. At this data mining and web analytics workshop, held last July in Washington, DC, the following areas of study, illustrative of the wide-ranging inquiry of the field, were identified:

Mining for Ad Relevance and Ranking
- Ad relevance measurement
- Ad ranking algorithms
- Ad text creation and evaluation

Audience Intelligence & User Modeling
- Understanding user intent
- Modeling online user behaviors for targeted advertisement
- User segmentation and profiling
- Demographics & location prediction
- Personalized advertising

Content Understanding
- Content-targeted advertising
- Opinion/sentiment mining
- Web scale information extraction for online advertisement
- Text mining techniques such as named entity extraction, query classification, keyword extraction, and other topics
- Understanding multimedia content for online advertisement

Search Engine Marketing, Optimization (SEMs, SEOs)

Other Topics in Advertising
- Advertising through social networks and microblogging (such as facebook and twitter)
- Advertising on new channels such as mobile devices
- Measurement of online advertising effectiveness
- Consumer privacy and data use policy
- Privacy preserving data mining approaches
- Fraud and spam detection & prevention in online advertisements.

ADKDD2010, "Call forPapers," http://adlab.microsoft.com/adkdd2010/Call_for_Papers.html (both viewed 9 Feb. 2011).

examination of online ad companies that say they incorporate "Unique personal data" into their targeting reveals a "non-PII" privacy smokescreen that must be rejected by the FTC framework. Among the companies incorporating such "unique personal data" are AdBuyer.com, Adnetik, Efficient Frontier, Infectious Media, Invite Media, Media Innovation Group, mediaMath, mexad, Rocket Fuel, SearchIgnite, The Trade Desk, Triggit, Turn, and XA.Net. These same companies also use "Intent Data" from behavioral targeting warehouses such as BlueKai and eXelate.[47]

Turn, for example, operates a "data-driven" ad-targeting platform that "crunches 2000+ behavioral, contextual, inventory, and ad selection variables within 25 milliseconds… all to determine the right ad, right time, right price, and right audience." [48] "Turn operates one of the largest marketing platforms on the Internet… ranked 6th in US audience reach, just behind companies like Google…."[49] A recent research paper by TURN discusses how its "data mining solution enables marketers to cost-effectively identify interactions and variables of thousands of data points. It also allows them to look at the entire user profile at the time of impression receipt and do a thorough analysis of the impact of all the variables on a campaign (including latent variables which go beyond the audience segmentation and are often times overlooked)."[50] Turn explains that its "secret sauce" is a "scalable infrastructure [that] enables us to read an individual user's data profile from among hundreds of millions of profiles within a very small time frame, generally 2 or 3 milliseconds. And, we do this over 100,000 times a second (8+ billion times a day)."[51]

In its privacy statement, Turn cites its membership in the Network Advertising Initiative (NAI), its work with the IAB on the new self-regulatory icon-based program, its membership in the Hunton and Williams LLP Center for Information Policy Research, work with Evidon (formerly "Better Advertising"), and adherence to the US/EU data Safe Harbor as evidence of its commitment to the "highest consumer privacy and data policy standards and practices." The company says in that statement that it "does not collect PII," while saying that the following is only non-personal information: "…the IP address used to access the Internet, the type of browser used, which and how many Business Partner web pages have been viewed,

---

[47] Econsultancy, "Demand-Side Platforms Buyer's Guide," p. 41. DataXU says that it uses such intent data.

[48] Turn, "Turn Media Platform Overview," http://www.turn.com/?p=3055 (viewed 15 Feb. 2011).

[49] Turn, "The Ingredients of Our Secret Sauce: Part 1," http://www.turn.com/?p=5973 (viewed 15 Feb. 2011).

[50] Turn, "Mining Data for Digital Advertising," http://www.turn.com/?p=4014 (viewed 15 Feb. 2011).

[51] Turn, "The Ingredients of Our Secret Sauce: Part 1."

search terms entered on Business Partner websites, referring/exit pages, and the date and time a Turn Ad was viewed." In its discussion of the use of cookies and Web beacons, the company claims that such tracking and analysis isn't personally identifiable. But the privacy policy and the claim that its targeting is all based on non-PII dta flies in the face of what its long list of "data partners" provide (let alone its own pronouncements on the ability to track and target an "entire user profile"). Its data partners include Bizo, IXI, TARGUSinfo, Polk, Datalogix, Almondnet, Bluekai and eXelate.[52]

Bizo data provides "business demographics of a person which may include, but is not limited to job function, seniority, company size, industry, geography, etc."[53] IXI's digital ad data enables online marketers to "target only the consumers that have the right financial profile for each offer and brand…. [with] real-time user classification capabilities…. [that] ranks online consumers based on their expected ability to pay their financial obligations… [and] provides a powerful, complete and accurate estimate of your prospects' and customers' total household income… [along with an] estimate of a household's spending after accounting for the fixed expenses of life (housing, utilities, public transportation, personal insurance and pensions)."[54] TARGUSinfo's data includes "names, addresses, landline phone numbers, mobile phone numbers, email addresses, IP addresses and predictive attributes" (continually updated "10 times daily").[55] TARGUSinfo also facilitates the collection of "audience targeting data high-quality, offline attributes—including demographics, shopping behaviors, lifestyles, preferences and brand affinities—that are verified… to accurately identify Internet users and link them to attributes—such as demographics, buying behaviors and attitudes—in a real-time… manner…. enabling you to target the most relevant ad to every user regardless of location or media buying methodology."[56] "AdAdvisor services use cookies that give you a window to

---

[52] Turn, "General Info," http://www.turn.com/?page_id=532; Turn, "Info Collection & Use," http://www.turn.com/?page_id=536; Turn, "Site Privacy Policy," http://www.turn.com/?page_id=534; Turn, "Data Partners," http://www.turn.com/?p=1392 (all viewed 15 Feb. 2011).

[53] Bizo, "Bizo Membership Agreement," http://www.bizo.com/partner/membership_terms (viewed 15 Feb. 2011).

[54] IXI Corporation, "Solutions for Advertisers and Agencies," http://www.ixicorp.com/ixi-digital/solutions-for-advertisers-and-agencie; IXI Corporation, "AudienceIXInsights," http://www.ixicorp.com/ixi-digital/solutions-for-advertisers-and-agencies/audienceixinsights/; IXI Corporation, "IXI Digital Targeting Options," http://www.ixicorp.com/ixi-digital/ixi-digital-targeting-options/ (all viewed 15 Feb. 2011).

[55] TARGUSinfo, "About Us: Our Data," http://www.targusinfo.com/about/data/ (viewed 15 Feb. 2011).

[56] TARGUSinfo, "Solutions: On-Demand Scoring: Display Advertising Optimization," http://www.targusinfo.com/solutions/scoring/optimization/default.aspx (viewed 15 Feb. 2011).

rich, predictive data on **over 50 million unique US users**."[57] Polk can provide "consumer detail (e.g., age, household income, gender), phone numbers, email addresses," along with "comprehensive customer profiles with unique automotive variables…. The number of registered vehicles in a household, When a household will likely be in the market for their next vehicle purchase, How much will likely be spent on the next vehicle purchase," and "reliable and extensive ethnic data including those with the highest levels of purchasing power—Hispanics and Asians."[58] Datalogix, "a source for real-world data for online targeting" uses "tens of millions of …Affiniti Cookies to support online targeting."[59] "DataLogix' audience platform is powered by a database with over $1 trillion dollars in consumer spending behavior."[60] "Available data spans hundreds of product categories and a host of recency, frequency and monetary value data elements."[61] AlmondNet "partner(s) with Data-Owners & Media-Owners to facilitate the delivery of relevant, targeted (based on recently-conducted searches for products/services) ads to consumers wherever they go…," "…based on their observed online behavior wherever they may be found."[62] "[O]ur technology collects information about Users from our data partners, and from Users as they visit our partner web sites."[63] The data collected and sold by both BlueKai and eXelate are discussed in this submission

---

[57] TARGUSinfo, "Solutions: On-Demand Scoring: Advertisers," emphasis in the original, http://www.targusinfo.com/solutions/scoring/optimization/advertisers.aspx (viewed 15 Feb. 2011).

[58] R.L. Polk & Co., "Data Enhancement Services," http://usa.polk.com/Industries/Dealers/Communicate/DataEnhance/; R.L. Polk & Co., "Profiling," http://usa.polk.com/Industries/Finance/Analyze/Profiling/; R.L. Polk & Co., "Targeted Marketing Lists," http://usa.polk.com/Industries/Media/Communicate/TargetMkt/ (all viewed 10 Feb. 2011).

[59] Datalogix, http://affiniti.datalogix.com/; Datalogix, "DLX Platform," http://affiniti.datalogix.com/what-is-dlx-platform (both viewed 15 Feb. 2011).

[60] Datalogix, "Datalogixtm Taps Consumer Packaged Goods and Retail Vet David Sommer as General Manager Of Datalogix CPG," 24 Jan. 2011, http://www.datalogix.com/assets/files/press/Datalogix-Sommer-final.pdf (viewed 15 Feb. 2011).

[61] Datalogix, "Data Append," http://nextaction.datalogix.com/index.php?id=93 (viewed 15 Feb. 2011).

[62] AlmondNet, http://www.almondnet.com/Home.aspx; AlmondNet, "AlmondNet Partners with Invite Media," 25 May 2010, http://findarticles.com/p/articles/mi_m0EIN/is_20100525/ai_n53774289/ (both viewed 15 Feb. 2011).

[63] AlmondNet, "Technology Privacy Policy," http://www.almondnet.com/privacy-center/technology-privacy-policy.aspx (viewed 15 Feb. 2011).

as well. Increasingly, such data are collected across platforms, with tracking occurring on mobile, social media, search, and other online content.[64]

The growth of third-party data integration used for behavioral targeting and other interactive marketing poses significant privacy concerns. Companies such as Experian, arguing for self-regulation, claim that "the collection and sharing of third-party data… provides numerous significant benefits to consumers and businesses…. The result is lower prices, enhanced competition, and increased consumer convenience…. Third-party data also facilitates the relevancy of first-party marketing efforts…. Even large first-party marketers with extensive customer databases depend on third-party data…."[65]

Experian and other third-party data brokers working in the online marketing environment fail to inform the Commission of the significant developments in digital profiling and targeting that warrant meaningful consumer protection safeguards under the new framework. A far-reaching system that instantly integrates a wide range of data profiling sources for tracking and targeting—now used for real-time auctions of a single user—illustrates why the Commission's approach must place limits on how third-party data can be utilized. Consumers should both know of and approve, via Just-in-Time Notices and new standards for data collection and use, the precise use of third-party data. As the recent Econsultancy demand-side platform report makes clear, Experian is part of a "Data Partner" online marketing chain that includes Bluekai, eXelate, Bizo, Rapleaf, AlmondNet, TARGUSinfo, eBureau, Datalogix and Acxiom.[66] Experian, in its recent Comment to the Commerce Department's privacy proceeding, was less than forthcoming about its data collection practices for online marketing. For example, Experian should have stated that its "Audience IQ" is a "turn-key" solution that provides far-reaching profiling for consumer targeting capabilities, including "Direct Data Matches." The company also reveals in marketing documents that "Audience IQ uses advanced methodologies that predict the location of the consumer at a resolution that varies from five-digit ZIP Code to household. Once Experian has geographically located the consumer, it is able to link the

---

[64] TURN cites all these data partners, but neither CDD/U.S. PIRG nor consumers know exactly what data sets and information they use for their targeting service. We use TURN only as an example. Our comments could have examined other companies, who operate in the same non-transparent and purposefully misleading manner about what they collect and how they target an individual.

[65] NTIA, "Information Privacy and Innovation in the Internet, Docket # 101214614-0614-01: Comments of Experian," 28 Jan. 2011, http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=A276913A-A0FC-44B7-8054-520C4A609181 (viewed 12 Feb. 2011).

[66] Monica Savut, "Demand-Side Platforms Buyer's Guide," Jan. 2011, http://econsultancy.com/us/reports/dsps-buyers-guide (viewed 12 Feb. 2011).

marketer's selected data elements and deliver those back in real time…."[67] Such digital data targeting by Experian can be used for both PC and mobile platforms.

Online/Offline Data Combined

Consumers who were victimized during the subprime mortgage era, or those who were sold unaffordable loans for education, should not have to remain vulnerable to new forms of unfair database marketing that combine offline and online data, such as that of the new partnership involving eBureau and BlueKai. eBureau engages in online lead generation and digital marketing in such sensitive consumer markets as "Higher education, Insurance, Financial Services, Collections, Automotive," and online retail.[68] The company claims to have an "online data warehouse" with 300 Billion records," or nearly 1,000 records for every man, woman, and child in the U.S.[69] As the two companies explained in a recent announcement,

> Through this partnership, marketers are no longer forced to make a tradeoff between precision and scale. Because eBureau Custom Audiences are built using tens of thousands of predictive factors to identify ideal customers and new prospects, the addressable audience is dramatically larger than a simple demographic approach. To build a Custom Audience, a marketer defines their customer profile, using input from their historical performance data, customer lists or demographic and/or psychographic criteria. eBureau's predictive analytics platform amasses the client data with eBureau's extensive amount of offline data to define the marketer's unique target market. The results are distilled into a single, custom targeting attribute representing the Custom Audience and made available only to those clients through the BlueKai Platform.[70]

Mobile Advertising

Special safeguards are needed for small-screen devices, where icons and other graphic elements are apt to be overlooked. Advances in mobile advertising,

---

[67] Experian, "Audience IQ for Display Advertising," http://www.experian.com/marketing-services/online-display-advertising.html?cat1=customer-acquisition&cat2=digital-marketing; Experian, "Audience IQ for Customer and Website Experience," http://www.experian.com/marketing-services/customer-experience.html?cat1=customer-acquisition&cat2=digital-marketing (both viewed 12 Feb. 2011).

[68] eBureau, "Industries," http://www.ebureau.com/industries (viewed 9 Feb. 2011).

[69] eBureau, "Solution Brief: Auto Lead Quality Scoring," 2010, http://www.ebureau.com/sites/default/files/file/ebureau-solutionbrief_automotive.pdf (viewed 9 Feb. 2011).

[70] "eBureau and BlueKai Partnership Provides New Level of Targeting Precision at Scale for Digital Advertisers," Business Wire, 8 Dec. 2010, http://www.businesswire.com/news/home/20101208005581/en/eBureau-BlueKai-Partnership-Level-Targeting-Precision-Scale (viewed 9 Feb. 2011).

moreover, and in the ability to design applications to capture user data more effectively, require the Commission's framework to specifically address the privacy and consumer protection issues for the mobile Web era. For example, the recently created Open Rich Media Mobile Advertising (ORMMA) initiative is setting a new standard for the creation and delivery of interactive mobile marketing applications that have a direct impact on privacy. As the new project explains, "Mobile Rich Media ad units are mobile compatible ad units with various measurable, interactive options which drive greater brand engagement and messaging across to end-users compared to basic banner ads…. Optionally, the ad unit can capture information from the end-user to continue engagements at other times or via other media…. [and] can be dynamically composed so the ad content is targeted to the end-user."[71] The impact on consumer privacy of such technologies as mobile "ad controllers" on wireless devices is another reason for the Commission to quickly adopt the staff report and proceed with defining consumer safeguards.

That framework, moreover, must address the unique nature of mobile marketing, as illustrated in a recent SEC filing from mobile marketer Velti:

> According to ABI Research, mobile marketing and advertising spending is expected to increase from $1.64 billion in 2007 to nearly $29 billion in 2014.... Unlike other media platforms, mobile devices cover a very large installed base and enable access to consumers virtually anytime and anywhere, allowing real time interaction and engagement. By using a mobile device, campaigns can be further targeted to consumers based on interest, demographic profile and behavioral characteristics, thereby enabling brands, advertising agencies, mobile operators and media companies to effectively engage consumers in interactive, measurable advertising and marketing campaigns.[72]

---

[71] Google, "ORMMA: Description of Issues And Solutions," http://code.google.com/p/ormma/wiki/Description (viewed 16 Feb. 2011).

[72] "Measure the consumer engagement. Unlike other media platforms, the mobile device is used by the consumer more frequently and over longer periods, providing greater opportunities to generate data on where, when and how a consumer responds to a marketing or advertising message. Brands, advertising agencies, mobile operators and media companies can leverage this data to motivate a specific consumer action (e.g., a product purchase) at critical moments (e.g., when choosing between products) or at a distinct location (e.g., a nearby retailer)....

"The Velti mGage Interact's CRM capability provides a mechanism for tracking customer information by enabling campaign management functions including:

- identifying target groups within the customer base according to selected criteria or demographics;
- sending mobile campaign-related material (such as information on special offers) to selected recipients; and

The Growth of Ad Agency Data Targeting Services

There is an ever-growing number of companies buying and selling consumer data for online targeting, including major ad agencies, behavioral targeting warehouses, and ad exchanges. For example, WPP's "Zeus Advertising Platform" (ZAP) enables its clients to use advanced data-mining techniques "to track the effectiveness of each individual digital marketing element in the purchase funnel; to identify precisely which factors affect their audience at what times, and if/how they ultimately lead to conversion. ZAP provides a holistic view of *site analytics and campaign data for a comprehensive understanding of every individual consume*r…. within many live campaigns that reach hundreds of millions of unique users per month, and the solution is expanding in both data volumes and capabilities."[73] Reflective of the growing ease with which online marketing companies can seamlessly integrate diverse datasets across many platforms for myriad applications, ZAP permits "custom data integration." Through the "Zeus data warehouse, advertisers can action consumer and advertising data as well as integrate and action external data…. Third party data is layered on top of aggregated user level data… to form a record for each user, marrying audience data with performance metrics."[74] Last November, Google extended its digital ad targeting partnership with agency giant Publicis and its "VivaKi Nerve Center Trading Desk." They are buying video and mobile ads via Google Doubleclick's ad exchange for data targeting.[75]

- tracking, storing and analyzing campaign statistics, including tracking responses and analyzing trends.

"The Velti mGage Interact CRM functionality includes tools to enable marketers to extend their online and offline CRM strategies to mobile applications. It provides for the easy creation of finely segmented mobile CRM databases, automated segmentation based on historic customer responses, and member registration via multiple channels, including messaging, Internet and mobile internet....

"Velti mGage Measure provides end-to-end tracking and reporting of consumer behavior and engagement across media platforms, including traditional, online and mobile. "Customers are able to view the entire breadth of consumer engagement and then make data-driven decisions to refine their execution of marketing and advertising campaigns." Velti, "SEC Filing Pursuant to Rule 424(b)(1), Registration No. 333-166793," http://www.sec.gov/Archives/edgar/data/1490412/000104746911000342/a2201716z424b1.htm#ea45601_business (viewed 10 Feb. 2011).

[73] Netezza, "Media Innovation Group Case Study," 2009, emphasis added, http://www.netezza.com/documents/MIG_CaseStudy.pdf. See also Media Innovation Group, http://www.themig.com/mobile/zap.php (both viewed 15 Feb. 2011).

[74] Econsultancy, "Demand-Side Platforms Buyer's Guide," pp. 76-77.

[75] "Google Extends VivaKi Partnership," Warc, 8 Nov. 2010, http://www.warc.com/LatestNews/News/ArchiveNews.news?ID=27471 (viewed 16 Feb. 2011).

The Role of Innovation in Online Marketing and Privacy

As during the 1990's, when the online marketing industry opposed consumer privacy rules at the FTC and elsewhere, once again digital advertising companies disingenuously claim that enacting appropriate privacy safeguards will (as Google puts it), "thwart the ability of companies to develop new services and tools, and in turn make U.S. Internet companies less competitive globally and make the Internet a less robust medium…. [A]n anti-innovation framework would counterproductively choke off the development of new tools and services to protect personal privacy."[76] The facts—as Google undoubtedly knows—show this not to be the case. First, online marketers did not build serious privacy and consumer protection safeguards into their online marketing products. All the innovation has been, and continues to be, focused on expanding the data collection, profiling and targeting of users, across multiple platforms and applications. Google, Yahoo, Microsoft, ad agencies and digital marketing companies have significantly invested in creating new forms of digital data collection and new ways to measure it. That point is something that the industry doesn't volunteer and that regulators and policymakers should recognize. It has taken a global public uproar and governmental pressure to force Google, Facebook and the entire online ad industry to acknowledge and respond to concerns regarding privacy practices. (In fact, it was only after pressure brought by CDD, EPIC and our colleagues opposing Google's acquisition of DoubleClick that the FTC felt compelled to issue new staff proposals for behavioral advertising and privacy).

The U.S. is the global leader in developing and deploying online advertising applications and data targeting technologies. It sets the standard in the EU, Asia Pacific, South America, and elsewhere. Once the FTC establishes its new framework, and as the EU revises its own to reflect contemporary online commercial data collection techniques, U.S. online marketers can engage in the same spirit of innovation that will make their online products and practices truly privacy friendly. The FTC should not permit Google and other digital marketers to invoke the term "innovation" as if it were some magic political talisman that automatically chokes off reasonable consumer privacy policy safeguards. In its final report, we expect the FTC to set aside the self-serving claims that privacy safeguards will undermine innovation. Indeed, it is common sense to admit that once consumers know that their privacy is respected, there will be greater confidence in e-commerce and online marketing generally.[77]

---

[76] Google, "Comments re. Information Privacy and Innovation in the Internet Economy," Department of Commerce filing, 28 Jan. 2011, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/FINALCommentsonDepartmentofCommercePrivacyGreenPaper%20(3).pdf (viewed 16 Feb. 2011).

[77] See, for example, Advertising Research Foundation, "Councils," http://www.thearf.org/channels/councils; ESOMAR, "Online Research 2010: E-Universe: The Power of Listening," http://www.esomar.org/index.php/online-research-2010-programme.html; Microsoft Research, "Online Services and Advertising,"

Social Media Marketing

The Commission's framework has to ensure that the country's users of social media receive privacy and consumer protection. As we have discussed in other filings at the FTC, social media marketing has developed as an extensive but too little scrutinized digital data collection apparatus. Companies such as Facebook suggest that somehow consumers of what they call the "social web" operate with a different set of expectations for privacy. As Facebook recently explained, "certain aspects of the social web…exist precisely because people want to share rather than limiting the sharing of their information to others…. [I]mposing burdensome privacy restrictions could limit Facebook's ability to innovate, making it harder for Facebook to compete in a constantly evolving industry."[78]

Facebook, as the Commission knows, has been continually prodded and forced to change and improve its privacy practices—especially given the company's strategy of pushing its ability to harvest its member data (since the introduction of its now well-known "Beacon" and Facebook Advertising in 2007). Facebook has failed to ensure that its 149 million active U.S. users have control over the data collection and targeting practices related to its digital advertising and marketing system. Facebook is engaged in extensive data mining of its users for advertising purposes, which enables it to serve the interests of its major advertisers and other marketers on the platform. Facebook reportedly made $1.86 billion from advertising in 2010 (and that excludes revenues from sales of virtual currency) and delivered 1 billion ads on

---

http://research.microsoft.com/en-us/groups/osa/; "First International Workshop on Social Media Engagement (SoME 2011), http://wwwhome.math.utwente.nl/~volkovichyv/some2011; Katitza Rodriguez, "European Privacy Officials: Google, Yahoo, and Microsoft Are Still Breaking European Privacy Law," 10 June 2010, http://www.eff.org/deeplinks/2010/06/european-officials-google-yahoo-microsoft-breaking-law; Federal Trade Commission Closes Google/DoubleClick Investigation: Proposed Acquisition 'Unlikely to Substantially Lessen Competition,'" 20 Dec. 2007, http://www.ftc.gov/opa/2007/12/googledc.shtm; Electronic Privacy Information Center, "Facebook Privacy," http://epic.org/privacy/facebook/; Warwick Ashford, "Revised EU Privacy Laws to Demand Greater Transparency on the Web," 5 Nov. 2010, http://www.computerweekly.com/Articles/2010/11/05/243767/Revised-EU-privacy-laws-to-demand-greater-transparency-on-the.htm; Google, "Price Testing with Google Website Optimizer," Conversion Room Asia-Pacific Blog, 8 Feb. 2011, http://conversionroom-japac.blogspot.com/; Microsoft Advertising, "Microsoft Advertising Europe," http://advertising.microsoft.com/europe/home (all viewed 12 Feb. 2011).

[78] Facebook, "Comments re. 'Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," 28 Jan. 2011, http://www.scribd.com/doc/47918734/Facebook-Comments-Commerce-Dept-Dynamic-Privacy-Framework (viewed 10 Feb. 2011).

its platform.[79] That's one reason why Facebook is currently expanding its already five-football-field-large data center in the U.S.[80]

Facebook is a valuable service to its users and is a business success. But such qualities should not be at odds with consumer privacy—especially when a consumer entrusts the site with abundant amounts of personal and collective behavioral information. The Commission's framework must apply to social media marketing, including the data collected and used by Facebook. We urge the FTC to ensure that the framework informs a user about the various techniques used to solicit data in the social media marketing system. There are a host of techniques applied to Facebook and other similar services that rely on forms of stealth targeting designed to elicit data and other behavioral information to be captured by digital marketers. For example, the Facebook Marketing Bible recently explained how advertisers can take advantage of the user data available via Facebook's "user profile design:

> The December user profile redesign leads users to provide more personal information which can be targeted through Facebook ads….
>
> Previously, personal info was only shown in the secondary Info tab, meaning users and their friends rarely saw it during typical browsing. Users would often go months or years without updating their information to reflect changes in location or employer. Others who only entered the required name, gender, email, and date of birth when signing up for Facebook had little to encourage or remind them to list additional information.
>
> Accurate and plentiful personal information allows advertisers to target users with more relevant ads. Here are the ways in which the new redesign coaxes additional information out of users:
>
> - The Profile Info Summary makes personal info more visible to a user and their friends
> - Users see prompts to add missing information on their own Profile Info Summary
> - The Featured Friends panel prominently displays a user's significant other and family members

---

[79] Jolie O'Dell, "Facebook's Ad Revenue Hit $1.86B for 2010," Mashable, 20 Jan. 2011, http://mashable.com/2011/01/17/facebooks-ad-revenue-hit-1-86b-for-2010/ (viewed 15 Feb. 2011).

[80] John Letzing, "Facebook Data Center Is Boon for Oregon Town," *Wall Street Journal*, 21 Jan. 2011, http://online.wsj.com/article/SB10001424052748704881304576094222157412808.html (viewed 15 Feb. 2011).

- The enhanced Work and Education section encourages users to add their employers and schools
- The Likes and Interests section now shows images for each Like
- The new "Sports You Play" Likes category could become a targeting parameter in the future

Profile Info Summary

The Profile Info Summary appears in the top center of the profile, and lists in paragraph form the following data:

- Job position and employer
- Concentration or major and university
- Current city
- Relationship status
- Languages spoken
- Hometown
- Birthday

This data is so prominently displayed to a user's friends that they will strive to keep it accurate by updating when changes occur. When users see that their friends have listed this info, they will be more inclined to do so as well. When users browse to their own profiles, they'll notice if their information is out of date and correct it…. Users can now list additional information about their work, such as projects they've undertaken and friends who helped them, and about their education, such as classes and classmates… *This information can be a strong indicator of socioeconomic class*.[81]

Individual Facebook users should be informed, for example, that they are targeted via the keywords they may list on their profiles "based on interests, activities, favorite books, TV shows, movies, and job titles." And that they are targeted "based on stage of life," including whether they say they are in high school or college, for example. Targeting can also be focused on a whether someone is primarily Spanish-speaking in the U.S. Facebook and numerous third-party developers have refined strategies to engage users in "conversations" and then solicit and track a range of actions—in order to take advantage of the viral nature of the service feeds. Users can be tracked based on data collected on them that measures their "Viralocity," (viral coefficient), whether they are "social influencers," "daily active users," and other social engagement metrics.[82] One technique used by Facebook and its advertisers to elicit data is "incentivizing social action with rewards." Such

---

[81] "Facebook Marketing Bible," emphasis added, http://gold.insidenetwork.com/facebook-marketing-bible/?p=3096 (viewed 3 Jan. 2011).

[82] Refresh Partners, "Refresh Analytics: Facebook Application Demographics," http://refreshpartners.com/products; Kontagent, "The Kontagent Fact Sheet," http://www.kontagent.com/about/ (both viewed 15 Feb. 2011).

techniques can use third parties to install "tracking pixels" on a Facebook page, which "automatically contact[s] and rewards users when pixels are triggered or activity is observed."[83]

Consumers should also know and be able to control the role of "Third-Party Facebook Platform Analytics Providers" that track their behaviors. For example, Adobe's Omniture SiteCatalyst incorporates a range of "social media analytics" for Facebook marketers, so they can "gain deeper insights into user behavior" and "understand how apps 'go viral' amongst… users."[84] Facebook and other social media users need to understand the privacy implications when they are being stealthily targeted using forms of "incentives" designed to elicit data. As one Facebook marketing publication explains,

> By offering something the user values in return, they're much more likely to follow your call to action…. Many of these incentive promotions can be conducted manually by community or social media managers. They can monitor who takes action and manually enter them into your sweepstakes, contact them and transfer Facebook Credits to them, repost their content, or record their name on a list for discounted admission.
>
> Other programs can be built into your Page or website, either through embeddable widgets, by your team, or by a boutique Page or site management company. Your Page can be designed to only show a video player to those who've liked the Page, or to send an email with an MP3 download link to those who join your email list.
>
> Incentivizing action can be further automated using a third-party incentive system which installs tracking pixels on your site or Page, or which monitors your Page, Twitter account, or other property for activity. It then automatically contacts and reward users when pixels are triggered or activity is observed. One company offering such an incentive system is ifeelgoods.[85]

We suggest that the Commission take Facebook at its word when, in recent Comments filed with the Department of Commerce" it said that "companies should provide a combination of greater transparency and meaningful choice… in which

---

[83] Josh Constine, "Incentivizing Social Action with Rewards," Facebook Marketing Bible, Dec. 2010, http://gold.insidenetwork.com/facebook-marketing-bible/?p=2815 (viewed 12 Jan. 2011).

[84] Justin Smith, "Analytic Tools for Developers," Facebook Marketing Bible, Sept. 2010, http://gold.insidenetwork.com/facebook-marketing-bible/?s=Third-Party+Facebook+Platform+Analytics+Providers (viewed 12 Jan. 2011).

[85] Constine, "Incentivizing Social Action with Rewards."

information is collected."[86] Such a principle should be operationalized under the FTC's imminent new framework.

The Limits of Self-regulation and Voluntary Codes in the Absence of a Comprehensive Policy Framework

Any student of self-regulation and media/telecommunication in the U.S. will recognize that self-regulation is only as effective as the laws and regulatory policies it is designed to implement. In privacy, such as with the Children's Online Privacy Protection Act (COPPA), the federal statute and implementation rules of the FTC set the parameters of various self-regulatory approaches for the market. Without COPPA's statutory requirements, children would be subject to an even greater array of behavioral targeting and interactive marketing practices, and there would be no effective self-regulation addressing their privacy. Self-regulation of online marketing to protect consumer privacy has been a failure from the start, as research makes clear. Indeed, there hasn't been a meaningful incentive for the online targeting industry to ensure there is an adequate mechanism for self-regulation in behavioral and other digital targeting approaches. Until the FTC adopts its proposed framework, along with action by other regulators and Congress, the online consumer data targeting industry will continue to expand its capabilities without regard to privacy.[87]

Voluntary privacy codes must also reflect actual contemporary digital marketing data collection and targeting practices. The new icon-based program implementing the July 2009 Self-Regulatory Principles for Online Behavioral Advertising, developed by the DMA, IAB, and others, fails to effectively empower and protect consumer privacy online. One has only to examine how the "Principles" fail to protect a U.S. consumer's most sensitive information, including data related to the finances, health and families. Under the woefully inadequate "Sensitive Data Principle" they include children who are *already* protected by the legal requirements of COPPA. The Principles also reflect the narrowest range of sensitive information, requiring consent "for the collection of financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual for online behavioral advertising purposes." The principles embraced this limited definition of sensitive information in order to ensure that consumer data can continually be collected without consent for the online marketing of financial and health products (as well as adolescents, racial/ethnic groups and others who rightly should have their information classified as sensitive). Online marketers spent some $1 billion targeting online users seeking medical

---

[86] Facebook, "Comments re. 'Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."

[87] Pam Dixon, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation," World Privacy Forum, 2 Nov. 2007, http://www.worldprivacyforum.org/behavioral_advertising.html (viewed 17 Feb. 2011).

condition and health-related information last year, and more than $2 billion for financial digital advertising during the first half of 2010 alone.[88]

The Evidon site (formerly "Better Advertising"), which implements the new self-regulatory program for the "Digital Advertising Alliance" (4As, AAF, DMA, IAB), says it has created the equivalent of a nutrition food label for online privacy. But an informed examination will discover they have left out significant information. It's as if that soup can failed to inform a consumer about the salt, fat, and additive content used to make the product. Evidon's self-regulatory system relies primarily on a graphical triangulated icon that appears on display ads and is called "Ad Choices." No information on the actual techniques used to collect data is generated by the icon. Nor does this self-regulatory approach address the likely inability of even noticing the icon, as a consumer is encouraged to engage with various interactive design techniques (such as rich media, online video, etc.). As the Evidon site illustrates, if a user clicks on a Bank of America ad, they first read this purposefully vague statement: "This ad has been matched to your interests. It was selected for you based on your browsing activity." A further click of the overlay generates a headline reading: "how data powers your experience."[89]

If a user seeks to learn from Evidon "How Interest Based Advertising Works," one sees a presentation that does not comport to many of the techniques used for behavioral and digital marketing. Nor does the section candidly discuss the privacy and consumer protections concerns. Instead Evidon uses such inadequate phrases as "Some companies collect data and sell it to other companies; being familiar with company privacy policies helps people protect their privacy…. Companies usually provide their own opt-out mechanisms through their web sites. A good place to start is a company's privacy policy."

Through its "Open Data Partnership" Evidon allows users to eventually use an ad preference manager system. But this service also fails to effectively inform a consumer on how its partners collect and use data. For example, if one links to BlueKai's Evidon section a consumer is confronted with a description lifted out of obtuse privacy policies: "BlueKai operates an auction based, online data exchange… provider of marketplace connecting advertisers to ad networks and data aggregators (online and off), often facilitating multiple connections and bidding process… collects data from online publishers and provides data to advertisers directly or via exchange…. Anonymous (ad serving domains, browser type, language

---

[88] "Internet Ad Revenues Break Records, Climb to More Than $12 Billion for First Half of '10," IAB, 12 Oct. 2010, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-101210 (viewed 17 Feb. 2011).

[89] Evidon, "Build Trust. Grow Your Business," http://www.evidon.com/solutions/overview (viewed 17 Feb. 2011).

settings, operating system, page views, search terms, time/date), Pseudonymous (Clickstream data, IP address)…. Anonymous data is shared with third parties….” Then one has to click to learn what profiling categories one was placed in, in order to decide whether to edit them. A consumer would be better informed if they were told, for example, what BlueKai tells its clients, that BlueKai has ushered in a “Data Renaissance.” “For the first time in history, advertisers can target individual consumers independent of their media choices… real-time data from top tier websites with unique access to purchase, shopping comparison, and product research behavior from their users…. BlueKai Exchange offers more than 30,000 data attributes… a marketer defines their customer profile, using input from their historical performance data, customer lists or demographic and/or psychographic criteria. eBureau’s predictive analytics platform amasses the client data with eBureau’s extensive amount of offline data to define the marketer’s unique target market. The results are distilled into a single, custom targeting attribute representing the Custom Audience and made available only to those clients through the BlueKai Platform.”[90]

Research on the new self-regulatory system indicates that few consumers ever proceed with opting out, illustrating its ineffectiveness.[91] “The pilot test data shows that consumers want to learn more about behavioral advertising but that only a small percentage, once informed, will change their preferences,” said Fran Maier, President of TRUSTe. “This low rate of preference change indicates that an effective ad notice may actually increase trust without any negative impact on advertising revenues.”[92]

Another Evidon data partner is Lotame, described in a deliberately opaque manner: “Lotame is an online ad network that uses ‘Crowd Control’ technology to build customized consumer audiences based on social activity using implied or stated interests. Their technology is specifically designed to take full advantage of the unique attributes of social data using participation and user generated content…. Anonymous (browser information, page views, time/date, ‘user interest expressed

---

[90] Evidon, “About BlueKai,” http://info.evidon.com/companies/bluekai (viewed 17 Feb. 2011).

[91] Jack Marshall, “Few Opt Out of Behavioral Ads,” ClickZ, 20 Dec. 2010, http://www.clickz.com/clickz/news/1933561/opt-behavioral-ads; “RESEARCH: Consumers Feel Better about Brands that Give Them Transparency and Control Over Ads,” Evidon’s Corporate Blog, 3 Nov. 2010, http://blog.evidon.com/2010/11/10/research-consumers-feel-better-about-brands-that-give-them-transparency-and-control-over-ads/ (both viewed 16 Feb. 2011).

[92] “Consumers Find Behavioral Advertising Choices Compelling With TRUSTe TRUSTed Ads Privacy Platform,” 16 Nov. 2010, http://www.marketwire.com/press-release/Consumers-Find-Behavioral-Advertising-Choices-Compelling-With-TRUSTe-TRUSTed-Ads-Privacy-1354242.htm (viewed 16 Feb. 2011).

or implied at social networking sites'), IP address…."[93] Lotame tells its clients another story: "Lotame's Audience Builder collects billions of data points each day from Lotame's audience and organizes them into a taxonomy of human behavior…. Precise and transparent online advertising solutions derived from over 240 billion monthly collected interests, actions, and attributes. Armed with our data on how people behave…."[94] Undoubtedly a user of Evidon's ad preference system should be empowered to decide whether they wish to be identified by one of Lotame's "Data Solutions" for targeting, including segments called "Arcade Addict: People who play video/online games and use multi-player environments"; "Couch Potato: People who spend their time seeking/generating content surrounding TV programs (current and re-runs), networks, and actors/actresses"; or "Teeny Boppers: The lifestyles, activities and interests of teens (13-19 years)."[95]

The current self-regulatory program fails to reflect the actual contemporary digital marketing practices involved in data collection. The Commission should reject this most recent attempt by the online marketing industry to thwart federal consumer privacy rules by the FTC.[96]

---

[93] Evidon, "About Lotame," http://info.evidon.com/companies/lotame (viewed 17 Feb. 2011).

[94] Lotame, "Advertiser Solutions," http://www.lotame.com/solutions/advertisers/ (viewed 17 Feb. 2011).

[95] Lotame, "Data Solutions," http://www.lotame.com/solutions/datasolutions/ (viewed 17 Feb. 2011).

[96] Without COPPA, for example, there would be no effective self-regulation on children's privacy. Another example is the Children's TV Act rules set by the FCC. See: http://mitpress.mit.edu/catalog/item/default.asp?ttype=2&tid=11125; http://www.caru.org/about/index.aspx; http://www.truste.com/privacy_seals_and_services/enterprise_privacy/childrens-online-privacy-seal.html; www.worldprivacyforum.org/.../WPF_NAI_report_Nov2_2007fs.pdf; www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf; http://ir.library.oregonstate.edu/xmlui/handle/1957/19453. Even the law firm of Wiley, Rein recognizes that "Threat of Legislation Drives Self-Regulation of "Behavioral Advertising." http://www.wileyrein.com/publications.cfm?sp=articles&id=5072; http://www.marketwire.com/press-release/Pharma-Industry-Ups-Digital-Ad-Spending-1310194.htm; http://www.iab.net/AdRevenueReport; http://www.google.com/doubleclick/gallery/features/data_capture.html; http://creativezone.mediamind.com/; http://blog.greystripe.com/2010/07/introducing-greystripes-immersion-ads.html; http://www.evidon.com/assurance_platform; http://info.evidon.com/about_behavioral_advertising/section1?n=103; http://info.evidon.com/companies/bluekai; http://www.bluekai.com/; http://info.evidon.com/companies/lotame; For an overview of the data collection system generally, see, for example: http://digitalads.org/

The TRUSTe icon, unfortunately, try as it might to masquerade as a kind of Good Housekeeping Seal of Approval for privacy protection, is simply no substitute for transparency, clarity, and choice. That icon relies on a small graphic device  that fails to convey what's really going on behind the scenes, and is also linked to the same notice-and-choice privacy policy regime that has proven again and again to be inadequate. Industry's description of the TRUSTe program, moreover, is little more than an apologia for behavioral targeting, which it describes in the most glowing terms, while neglecting to explain how BT may affect the consumer in such critical areas as finances and health.[97] This is not to suggest, however, that TRUSTe is not an eminently effective enterprise. From all reports, it has been notably successful at its central mission, which is providing "…agencies, advertisers, networks and publishers a turnkey solution to provide evidence of compliance with … FTC guidelines."[98] TRUSTe, in other words, which started out as a nonprofit organization before deciding in 2008 to become a for-profit, provides corporate websites with an out-sourced, streamlined means of assuaging privacy concerns that might be raised by consumers or policymakers.[99]

CDD and U.S. PIRG provide the following comments in response to the questions raised by the report.

1. U.S. PIRG and CDD strongly support the Commission staff's important recommendation to redress a longstanding failure of the agency—to ensure that the reams of data on a user that online marketers claim aren't personally identifiable—are protected. As the Commission explained, roundtable experts supported addressing this digital data "loophole," by recognizing that the distinctions made by industry to separate so-called PII from non-PII are antiquated. The online targeting industry has developed a range of

---

[97] TRUSTe, "TRUSTed Ads," http://www.truste.com/privacy_seals_and_services/enterprise_privacy/trusted-ads.html (viewed 10 Feb. 2011).

[98] "Consumers Find Behavioral Advertising Choices Compelling with TRUSTe TRUSTed Ads Privacy Platform."

[99] According to TRUSTe CEO Chris Babel, "We currently offer a full end-to-end compliance solution that starts with an ad tag insertion, then delivers the industry "forward i" icon, the interstitial notice upon icon click, and finally additional information and the consumer preference manager. As we only have contracts directly with our clients as opposed to being an industry watchdog, we provide each client a full set of reporting on a real-time and monthly summary basis and it is up to them to share this data with regulators or industry associations. We price on a CPM basis with a basic service which is upgradeable to include additional consumer interface customization and advanced reporting and we are offering free trials to customers in this initial phase of market implementation." "TRUSTe CEO Babel Discusses The Business Of The Trusted Intermediary As Privacy Concerns Swirl,"AdExchanger.com, 31 Jan. 2011, http://www.adexchanger.com/data-exchanges/truste/ (viewed 10 Feb. 2011).

techniques and methodologies to impose data tracking identifiers on a specific user, and then measure that user throughout what is described as the "online journey." Such tracking of a single user is increasingly cross-platform, including PCs and mobile devices. The online marketing industry has developed such measures, in part, to determine which online entities should receive financial compensation for securing the "conversion" and other measureable impacts. The Commission should also review contemporary digital marketing practices, especially social media and mobile/location advertising, to identify the data sets that should be incorporated into the safeguards provided by the new framework.[100]

2. The Commission should ensure that companies provide to the consumer, via Just-in-Time notices, precise and accurate information on the "specific business purpose" or "need" for which their data are being collected. Data should only be retained for that specific purpose—and require an affirmative opt-in if they are to be used or stored for more than 24 hours. Most of the data for behavioral targeting-related applications have a fairly short lifespan, while other products, such as for automotives, have a longer "in-market" buying cycle. The Commission should articulate reasonable limits to govern the use and retention of behavioral data and profiles in order to protect and empower consumer privacy.

3. The concept of "commonly accepted" practices requires review in order to protect consumer privacy. The placement of cookies and other tracking and profiling techniques, along with the sale of those user cookies for subsequent targeting, for example, should not be accepted as a routine practice. The relationships between so-called first- and third-party sites are blurring, as online marketing is conducted through ad exchanges and other mechanisms for data transfer and sale. A first-party site must be required to operate under the proposed framework—with meaningful and affirmative choice concerning data collection and usage practices controlled by the consumer.

4. Informed consent in the digital marketing era requires, as we have mentioned, a new commitment to candor and honesty from the online marketing industry. It needs to clearly explain to the user how the data are collected and used, and no longer rely on disingenuous and misleading privacy statements and public assurances. For mobile applications, the Commission should ensure that its framework clearly articulates the need for providers (network, content, marketing apps) to develop a mechanism

---

[100] See, for example, Microsoft Advertising, "Engagement Mapping," http://advertising.microsoft.com/engagement-mapping ; TagMan, "What is TagMan?" http://www.tagman.com/index.php/what-is-tagman.html (both viewed 10 Feb. 2011).

through which a consumer both understands and consents to the range of tactics used to facilitate data collection.[101]

5. A consumer should not have to confront a "take-it-or-leave-it regime." The Commission should incorporate into its framework a provision that users receive fair compensation for the use of their data. Given the increasing revenues for online publishers and marketers from the harvesting of users' data without their consent, new forms of compensation are required.[102]

6. Sensitive data and "sensitive users" require the Commission framework to articulate important safeguards. Consumers are increasingly at risk today regarding the information and offers they receive for such critical matters as mortgages, credit, insurance, private college loans, and health information. As we have said previously, no consumer can be expected to understand—let alone control—the array of sophisticated and pervasive data mining and personalized targeting techniques that confront them in today's online digital marketplace. A new report by Admeld illustrates one aspect of this threat related to sensitive data. Companies engaged in financial marketing, including GEICO, Microsoft, H&R Block, State Farm Insurance, Traveler's Insurance, American Express US, Safeco, Turbo Tax, Capital One, Vanguard, and 21st Century Insurance, are using real-time bidding online targeting services. Health and medical real-time targeting is being conducted by AstraZenica/Symbicort. Other advertisers using real-time online tracking and user profile auctions that can involve substantial financial transactions made by a consumer include those involving autos, travel, and telecommunications services.[103]

   Given the array of data a company can easily (and non-transparently) compile on a single user to be used for profile-based targeting, which can include their race or ethnicity, presence of children, financial status, political interests, and many other variables, the combination of such information can affect users differently. CDD and U.S. PIRG have already filed complaints with the Commission on the targeting of consumers for pharmaceutical and health

---

[101] See, for example, "Action Initiation" (Section 6.3.2) in Mobile Marketing Association, "Mobile Advertising Guidelines," Feb. 2011, p. 19, http://mmaglobal.com/policies/committees/mobile-advertising (viewed 10 Feb. 2011).

[102] See, for example, "The Rubicon Project Publishes 'Mechanics of RTB' White Paper," 9 Feb. 2011, http://www.rubiconproject.com/about/press/the-rubicon-project-publishes-mechanics-of-rtb-white-paper/ (viewed 10 Feb. 2011).

[103] Admeld, "Download: Agency RTB Landscape," http://www.admeld.com/agencyrtbmap/ (viewed 12 Feb. 2011).

products and services.[104] Other scholarly research on social networking sites covering medical issues and the lack of meaningful privacy safeguards underscore the need for effective Commission safeguards for sensitive information/sensitive users under the new framework.[105] We have also raised in our behavioral targeting complaints the sale of subprime mortgages and other financial products that harmed consumers.[106] The Commission framework should acknowledge that higher standards are necessary for information that a consumer would reasonably deem sensitive, including services that affect their finances and health. We strongly believe that the following sensitive information categories, as proposed by privacy legislation just introduced by Rep. Bobby Rush, be included in the Commission's framework: "race, ethnicity, religious beliefs and affiliations, sexual orientation or sexual behavior, precise geolocation information and any information about the individual's activities and relationships associated

---

[104] 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).

[105] Elissa R Weitzman, Emily Cole, and Liljana Kaci, et al, "Social but Safe? Quality and Safety of Diabetes-related Online Social Networks," *Journal of the American Medical Informatics Association* (2011), http://jamia.bmj.com/content/early/2011/01/24/jamia.2010.009712.full.html (subscription required).

[106] Center for Digital Democracy and U.S. PIRG, "Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices. Federal Trade Commission Filing," 1 Nov. 2006, http://www.democraticmedia.org/files/pdf/FTCadprivacy.pdf; 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," Federal Trade Commission Filing, 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"; 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; 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 (all viewed 12 Oct. 2009).

with such geolocation."[107] The Commission's framework must ensure that issues related to the targeting of an individual by race or ethnic data is classified as sensitive and subject to greater privacy safeguards. (In separately filed comments, we address the issues related to adolescents as sensitive users).

Given the state of the online industry, including the growth of third-party data sharing and sales for targeting with first parties (and the use of other interactive data techniques described earlier), we believe that the traditional first- vs. third-party distinctions are no longer clear. More publishers will see ad inventory using real-time bidding methods. See, for example the Open RTB Consortium and the establishment of "private ad slots" reserved for premium like ad buys.[108] All websites should be required to implement principles and practices under a comprehensive framework that places maximum practical control of the decision-making process in the consumer's hands.[109]

7. Consent requires a consumer being accurately informed about the data collection process and practices prior to any significant use. As we stated previously, the Commission's framework must ensure a new level of honesty and transparency that informs a consumer about the process and its implications. This can be handled through a combination of new uniform standards articulated by the framework for addressing sensitive information and sensitive users, "Just-in-Time" notices, new approaches to providing in-

---

[107] Wendy Davis, "Rush Privacy Bill Reintroduced," MediaPost Raw, 10 Feb. 2011, http://www.mediapost.com/blogs/raw/?p=5661 (viewed 12 Feb. 2011).

[108] "IDG Introduces Real-time Bids for Ad Space," 20 Jan. 2011, http://www.mad.co.uk/Main/News/Articlex/5ddf938733fa4fb6bbcfa7c5b4d2212f/IDG-introduces-real-time-bids-for-ad-space.html; DataXu, "Real Time Bidding Grows Up," 4 Feb. 2011, http://www.dataxu.com/2011/02/real-time-bidding-grows-up/; "Industry Leaders Team to Drive New Open RTB Standards," 13 Dec. 2010, http://www.marketwire.com/press-release/Industry-Leaders-Team-to-Drive-New-Open-RTB-Standards-1367683.htm (all viewed 15 Feb. 2011).

[109] Center for Digital Democracy, "April 2010 Complaint—Real-time Targeting & Auctioning, Data Profiling, Optimization, And Economic Loss To Consumers & Privacy," Apr. 2010, http://www.democraticmedia.org/real-time-targeting; Center for Digital Democracy, "Testimony on Behavioral Advertising: Industry Practices and Consumers' Expectations," 18 June 2009, http://www.democraticmedia.org/doc/cdd-testimony-20090618; Emily Steel and Julia Angwin, "The Web's Cutting Edge, Anonymity in Name Only," *Wall Street Journal*, 4 Aug. 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html ; "What They Know," *Wall Street Journa*l, Dec. 2010, http://online.wsj.com/public/page/what-they-know-digital-privacy.html (all viewed 12 Feb. 2011).

depth privacy information, limitations on the data collection process that users expect under the framework, and a serious new approach to "privacy by design." In another words, we call on the Commission to enact a framework that fundamentally transforms the privacy equation and places the control back in the hands of a consumer. As we discussed earlier, the icon-based system is an inadequate and purposefully misleading approach to ensuring consumers have autonomy over their privacy. Mobile applications require commensurate safeguards to address both the physical limitations of phone screens and also the range of digital marketing applications—including behavioral and location targeting—applied to the mobile marketing system.[110]

8. CDD and U.S. PIRG urge the Commission to oppose any use of deep-packet inspection by network operators. A one-stop shop that permits 24/7 user surveillance of all their transactions and that can take advantage of real-time/demand-side data profiling severely threatens consumer privacy. The Commission should hold workshops and hearings on deep-packet inspection and privacy, as part of a fact-finding and consumer education process that will inform the development of specific principles for the new framework.

9. Under the Commission's framework, we expect that all data partners involved in online data collection and targeting that don't directly interact with a consumer will be required to follow the framework. They and their clients that work with consumers will have to engage in practices that conform to the new provisions. The same creativity that has gone into integrating reams of disparate consumer information in real-time from diverse sources for targeting can be applied to privacy.

10. CDD and U.S. PIRG strongly support the FTC's leadership role in implementing a Do-Not-Track system. Many of our colleagues from the consumer and privacy community are submitting to the Commission specific recommendations on the technological and policy issues. The FTC should

---

[110] "New Mobile-Only, Display Ad Ecosystem Map From AdMeld VP Theermann," AdExchanger.com, 19 Dec. 2010, http://www.adexchanger.com/mobile/display-ad-ecosystem-map/; NAVTEQ Media Solutions, "Mobile Marketing Services," http://navteqmedia.com/mobile/marketing; NAVTEQ Media Solutions, "LocationPoint Advertising," http://navteqmedia.com/mobile/advertising/locationpoint-advertising; Smaato, "Mobile Advertising Optmization," http://www.smaato.com/adnetworks; AdMob, "AdMob for Advertisers," http://www.admob.com/advertise; "MMA Releases Whitepaper on Rich Media Mobile Advertising," http://mmaglobal.com/news/mma-releases-whitepaper-rich-media-mobile-advertising; John Constine, "Facebook Acquires Hyper-Local Mobile Advertising Startup Rel8tion," Inside Facebook, 25 Jan. 2011, http://www.insidefacebook.com/2011/01/25/acquires-mobile-advertising-rel8tion/ (all viewed 12 Feb. 2011).

recommend to Congress that it enact legislation that would empower the Commission to oversee the development and implementation of Do-Not-Track. While recent Do-Not-Track applications offered by various browser companies are a step forward, consumers should have the assurance that such systems operate in ways that truly protect privacy. The Commission needs to help develop the standards for Do-Not-Track and have regulatory responsibility for ensuring they protect privacy. The more granular policy safeguards and new industry standards as proposed by the framework, when combined with a universal opt-out system, will be a major step towards addressing privacy issues in the digital era.

11. Consumers should have access to all the data collected about them, including the right to edit and challenge information they believe to be misleading, incorrect, or harmful. We call on the online marketing field—which is working together on the implementation of its icon-based program—to work with both consumer and privacy groups and the FTC to develop a system designed to provide consumers with access to and control of their digital data.

12. Consumer/Commission Education: The Commission must do a better job in educating itself on how online advertising and data collection work before it engages in public education. While the staff report illustrates the Commission has made significant advances in understanding many aspects of the contemporary digital marketing system, it's clear they still have too narrow an understanding. In order to protect consumer privacy, the FTC has to engage in a focused effort that analyzes the relationship between the modes and methodologies used by digital marketing and the techniques and technologies of "computational" advertising. The Commission should better integrate the work of its Advertising Practices and Privacy Divisions, and create a plan to ensure that the staff and the Commission understand and can respond to current and emerging practices. While we approve of the Commission's recent hire of technology experts (which we urged the agency to do), it must understand that the issues raised by technological approaches are just one part of a multi-dimensional system that involves a wide range of academic and other disciplines. Once the Commission has a more informed analysis of the issues and threats raised, for example, by social media or location-based marketing, it can then develop consumer education materials that will assist the public.[111]

---

[111] For an example of the various fields the Commission should assess and analyze as it develops a more thorough assessment of the consumer and privacy impact, see Google Research, "Publications by Googlers in Artificial Intelligence and Data Mining," http://research.google.com/pubs/ArtificialIntelligenceandDataMining.html; Yahoo Research, "Computational Advertising," http://research.yahoo.com/Computational_Advertising; Microsoft, "adCenter Labs—

The Commission should reject calls made by some governmental entities and online marketers, such as Google and Facebook, that propose the U.S. engage in negotiations designed to undermine the strong privacy and civil liberty protections enacted by the European Union.[112] The FTC has a crucial responsibility, as both an independent consumer protection agency and also as a member of international privacy organizations, to ensure that the U.S. respects and supports the EU framework; that it lead the development of privacy safeguards for this country that match or exceed what has been articulated by the EU; and that it play a leadership role supporting a privacy policy regime for the Asia-Pacific market that reflect the highest possible standards for consumer privacy protection.[113]

CDD and U.S. PIRG strongly support the FTC's critical leadership role on consumer privacy, including on proactively developing public policy and also ensuring enforcement. Consumers require an independent agency to ensure their interests are represented. The FTC and the new Bureau of Consumer Financial Protection should be in the forefront of ensuring that consumer privacy is safeguarded, and that online transactions involving sensitive information and posing significant costs are structured in a fair and transparent manner. The framework should support meaningful protections for children, adolescents, and other vulnerable users; affirm the need for strong regulatory rules on sensitive information; and ensure consumers can control contemporary digital and offline data collection practices more effectively. Additionally, the FTC should make it a high priority to ensure meaningful affirmative consent prior to data collection, including in social media

---

Innovations in Digital Advertising," http://adlab.msn.com/; Microsoft, "ADKDD 2010," http://adlab.microsoft.com/adkdd2010/; Chuck Hemann, Lauren Vargas, and Teresa Basich, "Defining and Measuring Influence," Radian 6 Community E-book, Jan. 2011, http://pages.radian6.com/e/3652/11-01-Radian6-JAN2011-Book-pdf/57BZN/102972791; Google Research, "Google and WPP Marketing Research Awards," http://research.google.com/university/marketingresearchawards/index.html; Eric Litman, "Ad Metrics, Evolved," 2 Feb. 2011, http://www.digidaydaily.com/stories/ad-metrics-evolved/; Michael J. Scialdone, "Establishing Best Practices for Scholarly Research Based on the Tenets of Human-Computer Interaction," AIS Transactions on Human-Computer Interaction, 2010, http://aisel.aisnet.org/thci/vol2/iss4/3/; Advertising Research Foundation, "Direct Engagement Initiative," http://www.thearf.org/assets/research-arf-initiatives-future-direct-engagement (all viewed 12 Feb. 2011).

[112] NTIA, "Information Privacy and Innovation in the Internet, Docket # 101214614-0614-01: Comments of Google Inc.," 28 Jan. 2011, http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=10FE3003-691B-4E2E-9685-87D7DB413C1D (viewed 12 Feb. 2011).

[113] Center for Digital Democracy and U.S. PIRG, "CDD and U.S. PIRG Urge Commerce Department to Protect Consumers Online," 28 Jan. 2011, http://www.democraticmedia.org/information-privacy-and-innovation-in-the-nternet-economy (viewed 16 Feb. 2011).

and mobile applications. We urge Chairman Leibowitz and the other commissioners to ensure that staff promptly make the necessary revisions that will strengthen its new framework and pass the document as soon as possible. The Commission should also recommend to Congress that legislation be enacted, including the establishment of a Do-Not-Track system supervised by the FTC.

Respectfully submitted,

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

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