Safe Harbor Draft Complaints

14 August 2014

The Center for Digital Democracy examined the EU Safe Harbor certification documentation of a number of industry-leading U.S. companies involved in digital profiling and online targeting and identified 30 of them that we believe are in violation of that framework. (See attached legal analysis for a more detailed discussion of Safe Harbor generally and the groupings of the specific violations that we found.) Although the companies on our list differ in the details of their various approaches to the digital data collection and profiling and targeting of individuals, five broad themes emerged in the course of our investigation, trends that underscore the fundamental weakness of the Safe Harbor in its current incarnation.

First, privacy policies in general, and Safe Harbor declarations in particular, fail to meet the needs of EU consumers. The shortcomings of corporate privacy policies are well known: they are too long, too arcane, and most consumers refuse to read them. Additionally, most of these policies fail to disclose adequately the companies' actual data-collection and consumer-targeting practices. The contrast between a company's description of its services in a corporate privacy policy, and what the company actually does in terms of its real-world consumer data collection practices, is stark, and figures prominently in the complaints presented here. Even the clearest, most concise of the policies we examined tended to cover data collection on the corporate website that few consumers were likely to visit rather than the data-driven advertising products and applications that they were likely to encounter on websites, mobile devices, and other platforms.[1]

Safe Harbor declarations, in contrast, which in our study ranged from eight words to eight sentences, are too short, too vague, and are shared in a manner—on the DOC's safeharbor.export.gov website and buried within corporate privacy policies—that few EU consumers are likely to see. This combination of faulty disclosure, alternately difficult to read and difficult to find, falls far short of adequately serving EU consumers seeking guidance on Safe Harbor and the privacy implications of these companies' actual data practices, which these companies readily reveal to their own corporate customers. Such admissions, offered by the companies themselves in their product literature and financial reporting, reveal the extent to which they are engaged in the very acts of data collection and consumer tracking that their Safe Harbor and privacy statements attempt to disavow.

Second, most of the companies we analyzed insist that they are "data processors" rather than "data controllers"—with the former ostensibly relieved of the obligation of upholding some Safe Harbor principles. The organization that engages the services of the online marketing specialist (or purchases its applications) is ultimately responsible for meeting the Safe Harbor requirements on behalf of all of these "processors" regardless of their data practices, or so the argument runs. But this assertion of "processor" status, of legal importance to EU consumers, is contradicted by the companies' own statements, which we quote at length in the summaries that follow. These statements, gleaned from corporate websites, product

data sheets, and financial reports to the SEC and others, are replete with references to the power and precision of the latest online advertising technologies—showing these companies have sufficient power over user data to make them data "controllers" under the applicable definition. For example, companies summarized here that create profiles on consumers from different data sets are "controllers" according to the applicable definition in the EU Safe Harbor agreement, and all of the companies at issue here determine the "means" of processing—sufficient dominion over EU personal information to become a data controller.[2]

Third, the environment in which these companies operate is nothing less than an "online marketing ecosystem" that continues to grow more complex and more powerful with every new breakthrough in "Big Data" technology and every new partnership and alliance, merger and acquisition. Many of the companies on our list, for example, have been materially affected by these changes to corporate structure in recent years, and even those that have remained more or less independent readily boast of their ability to "onboard" vast quantities of consumer data from a wide variety of sources, online and off. Nowhere in the Safe Harbor documentation or privacy statements that we examined, however, are such developments mentioned and clearly explained, even in passing. Nor is real-time bidding (RTB), or programmatic buying, the increasingly prevalent data-targeting industry practice that U.S. companies have promoted in the EU, in which millions of individual users (whose personal profiles are stored in targeting databases) are effectively "auctioned off" to the highest bidders (companies that want to reach particular audience segments with their advertising) in the milliseconds before a given web page loads. All of this personal data flows from the EU to the U.S. in a fraction of a second—without the knowledge or consent of the consumer whose profile is being traded.[3]

Fourth, most of the companies we cite do not provide meaningful opt-out mechanisms that EU consumers can find and use to remove themselves fully from privacy-harming data collection and processing. Opt-out mechanisms are more often than not available only on U.S. corporate websites that EU consumers are unlikely to visit, while the outsourced, third-party mechanisms that many companies employ turn out to be questionably effective cookie-based solutions to cookie-based profiling. Such opt-outs are ineffective in many popular technologies that do not include cookies.[4] In many instances, moreover, it is not clear whether consumers are actually opting out of data collection and processing covered by Safe Harbor Choice obligations, or simply getting less targeted advertising that results from such invasive practices. As consumers are increasingly tracked and targeted across various devices and applications, tagged with a variety of orchestrated cookie and non-cookie unique identifiers, EU (and other) consumers require greater transparency and control—safeguards that are not offered by the companies we identify in this complaint.[5]

Finally, while the companies on our list use terms like "anonymity" and "non-personally identifiable" ("non-PII") with abandon, they operate in a manner (again, based on their own statements) that is quite the opposite. The reality, as our

complaints make clear, is that dozens if not hundreds of companies alternately compete and cooperate in collecting detailed information about individual consumers, processing that data for the insights therein, and then transferring those insights to their partners and affiliates for the purposes of targeted marketing and advertising. The oft-expressed claim of "anonymity," ironically, is based simply on the absence in these digital consumer dossiers of any given names or government ID numbers (which have been discarded in favor of a more precise alphanumeric IDs in any case). But with a sufficient number of details about personal needs and interests, employment and social status, location and income, antiquated PII data concepts are not needed to track and target particular individuals. And neither—thanks to inadequate provisions of the Safe Harbor, inadequate FTC enforcement, and cynical corporate implementation of the Safe Harbor—is that consumer's permission.

---

[1] Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," I/S: A Journal of Law and Policy for the Information Society," (2008): 540-565, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf (viewed 15 July 2014).

[2] See discussion of Article 29 guidance on the definition of "controller" in accompanying legal analysis document.

[3] See, for example, "Criteo Gets Great Results Retargeting Audiences at Scale with Real-Time Bidding," DoubleClick Advertiser Blog, 1 June 2011, http://doubleclickadvertisers.blogspot.com/2011/06/criteo-gets-great-results-retargeting.html; "Creatives Meet Coders: Pierre Naggar, Turn Europe," Turn, http://www.turn.com/news/creatives-meet-coders-pierre-naggar-turn-europe; Jay Stevens, "Summary of IAB Italy Seminar on RTB: 'Keep Calm, Test & Learn,'" Rubicon Blog, 8 July 2013, http://www.rubiconproject.com/blog/summary-of-iab-italy-seminar-on-rtb-keep-calm-test-learn/ (all viewed 10 July 2014).

[4] Increasingly, and especially as mobile Web traffic grows, companies are turning to non-cookie-based approaches to profile consumers, through device-identification technology and device fingerprinting, with varying impacts on consumer privacy.

[5] Gavin Dunaway, "ID Is Key: Unlocking Mobile Tracking & Cross-Device Measurement, Part 2," AdMonsters, 3 Aug. 2013, http://www.admonsters.com/blog/id-key-unlocking-mobile-tracking-cross-device-measurement-part-2; Joanna O'Connell Luca S. Paderni, Samantha Merlivat, and Collin Colburn, "Solving the Cross-Platform Targeting Puzzle," Forrester, Aug. 2013, http://www.acxiom.com/resources/solving-cross-platform-targeting-riddle/ (both viewed 15 July 2014).

Acxiom Corporation

Complaint number	1
Company profile	Acxiom Corporation is a data broker engaged in digital data profiling of individual consumers. According to a recent FTC report, "Acxiom provides consumer data and analytics for marketing campaigns and fraud detection. Its databases contain information about 700 million consumers worldwide … ."[1]
Main website	www.acxiom.com/
Safe Harbor/privacy statements	Claiming to be a "Processor on Behalf" with regard to the personal information it receives from the EU/EEA and/or Switzerland, Acxiom also admits in its Safe Harbor certification statement that it serves as well as a "Data Controller … provid[ing] business and consumer information products designed to help companies market more successfully, integrate and improve the accuracy of their customer information and reduce the operational costs of processing customer data."[2] The company's Safe Harbor privacy policy elaborates still further on this point: Acxiom pledges to conduct its business according to the EU Safe Harbor Principles and the frequently asked questions (FAQs) issued by the U.S. Department of Commerce on July 21, 2000. … Acxiom … provides business and consumer information products designed to help companies market more successfully integrate and improve the accuracy of their customer information and reduce the operational costs of processing customer data. In this function, Acxiom acts as a data controller of the personal information contained in these information products. To the extent required by local law, Acxiom subsidiaries located in the member states act as the data controller with respect to personal data collected, processed and stored. … **Notice** Prior to the transfer of any non-public personal information from the EU to the United States, Acxiom requires contractual confirmation from the EU controller from whom Acxiom acquired the information that the personal data has been provided to Acxiom in accordance with the applicable EU Member State Data Protection law, thereby ensuring the data subjects have been provided with proper notice regarding how their

	personal data will be used. In addition, when personal data is collected directly from data subjects, Acxiom provides the data subject with notice regarding the manner and circumstances in which the personal data will be used and transferred to third parties. **Choice** Prior to the transfer of any non-public personal information from the EU to the United States, Acxiom requires contractual confirmation from the EU controller from whom Acxiom acquired the information that the personal data has been collected in accordance with applicable EU member State Data Protection law, thereby ensuring the data subjects have been provided with the proper choice regarding how their personal data may be used. In addition, when personal data is collected directly from the data subjects, Acxiom provides the data subject with a choice regarding the manner and circumstances in which their personal data may be used and shared with third parties. In addition to choice regarding the use of information, Acxiom will remove an individual's name and related information from its direct marketing information products.[3] In addition to this Safe Harbor privacy statement, Acxiom's website includes 18 other privacy statements (including separate policies for France, Germany, Poland, and the UK, as well as four non-EU countries and five U.S. privacy statements).[4] Although one of these statements, "Consumer Data Information," includes online options to opt out of both targeted online advertising as well as direct mail, email, and telemarketing advertising, the aforementioned EU Safe Harbor privacy statement offers a somewhat more cumbersome form of opt-out: "Consumers may request an opt-out form by writing Acxiom at the address below, leaving a message on our Consumer Advocate Hotline at 501-342-2722 (toll free 1-877-774-2094) or sending an e-mail to us at safharboroptout@acxiom.com."[5] Another one of its 19 privacy documents, "Acxiom Data FAQ," provides further insight into the company's data-collection practices: The data we collect helps companies market more effectively and reduces fraud and identity theft. Our data also helps people find businesses or other people

	through our directory services. … Acxiom's data consists of publicly available information, information from surveys and data from other providers. While all of our data collection complies with laws and industry best practices, our marketing data adheres to an even higher standard. We review our marketing data suppliers' online privacy policies to determine whether individuals are notified that information will be shared for marketing purposes and that people have a choice about such sharing. We do not work with data suppliers whose policies do not meet our strict standards. … … Acxiom does not collect cross-domain web browsing activity, but we do work with clients and partners who wish to use web browsing activity and our data to present more relevant advertising. When we do this, we comply with all applicable laws and the higher standards established by industry trade associations like the Direct Marketing Association, the Interactive Advertising Bureau and the Digital Advertising Alliance. … Acxiom collects three types of data – data that helps companies market more effectively, data that helps reduce fraud and identity theft and data that helps people find businesses or other people through our directory services. We allow individuals to see and correct the data we have about them.[6]
Non-compliance/ false claims	In none of this material, however—neither its Safe Harbor statement nor any of its privacy policies—does Acxiom make clear—as it does repeatedly in its own descriptions of its services elsewhere, that in its work on data profiles it integrates considerable amounts of sensitive first- and third-party data. Its Safe Harbor disclosures only hint at the company's practices without making clear to consumers the vast scope of the data collected and processed into intimate profiles. According to Scott Howe, Acxiom's president and CEO, "… through Acxiom … marketers are able to fully leverage all kinds of data—first-party, transactional, digital, social, mobile and other audience information."[7] Acxiom introduced its Audience Operating System (AOS) in 2013, describing it as "… the world's most powerful marketing platform. … [which] allows you to utilize the world's largest collection of consumer data from a cross-section of online and offline sources and types to further enhance and model your first-party CRM data."[8]

	"For the first time ever," Acxiom explains, "marketers, agencies and publishers can plan, buy and optimize audiences across channels, devices and applications, with precision and scale. One integrated platform that ties all the disparate sources of media channels and technology together. An open platform so flexible it can support virtually any application you can imagine."[9]AOS services combine a powerful set of its own Big Data targeting capabilities with outside partners, offering "unprecedented power to leverage the most important marketing databases … ."[10] Acxiom's data partners for AOS include some of the biggest online ad companies—Adometry, Affinity Solutions, Aggregate Knowledge, Alterian, AOL, AppNexus, Audience Science, BlueKai, Cisco, Collective, Comcast Media 360, DataXu, Ebay, Facebook, Hewlett Packard, IBM, PayPal, Rocket Fuel, TiVo, TURN, Twitter, and Yahoo—none of which is identified to consumers as AOS participants.[11] Acxiom also works with partners like eBay in what it calls "Direct Matching" (which "… connects eBay's transactional-level data with Acxiom's access to third-party datasets, as well as brands' own customer and prospective databases to identify potential matches for targeting purposes.").[12] Acxiom was one of nine companies that received an "Order to File Special Report" from the FTC in connection with the commission's recent report, "Data Brokers: A Call for Transparency and Accountability." Even though, as that report notes, "Acxiom … launched a new website that allows consumers to access, correct, and opt out of having information about themselves included in certain marketing products," we remain convinced that the company's digital data profiling practices continue to pose a threat to the privacy of consumers in the EU.[13]
FTC action on possible violations	FTC should investigate and seek appropriate remedies against this company for its failure to clearly notify consumers of the depth and sophistication of its profiling practices. Acxiom likely fails to fulfil its Notice and Choice duties to consumers concerning (1) the full range of its data-mining and ad-targeting technologies, (2) the number and identity of other companies that contribute consumer data to its AOS platform, and (3) the extent to which it commingles EU citizen data across its clients' data sets and resells that information as marketing products. As the FTC Data Broker report found, in its coverage of Acxiom and the company's practices, this company lacks transparency and

	an effective opt-out mechanism—both of which are required by the Safe Harbor framework.

[1] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," May 2014, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (viewed 29 May. 2014).

[2] Acxiom, Safe Harbor Organization Information, expires 5/28/15, http://safeharbor.export.gov/companyinfo.aspx?id=23039 (viewed 11 Aug. 2014).

[3] Acxiom, "EU Safe Harbor," http://www.acxiom.com/about-acxiom/privacy/eu-safe-harbor/ (viewed 21 May 2014).

[4] Acxiom, "Privacy," http://www.acxiom.com/about-acxiom/privacy/ (viewed 11 June 2014).

[5] Acxiom, "EU Safe Harbor."

[6] Acxiom, "Acxiom Data FAQ," http://www.acxiom.com/about-acxiom/privacy/acxiom-data-faq/ (viewed 11 June 2014).

[7] "Acxiom Releases Audience Operating System," Destination CRM.com, 30 Sept. 2013, http://www.destinationcrm.com/Articles/CRM-News/Daily-News/Acxiom-Releases-Audience-Operating-System-92294.aspx (viewed 22 Apr. 2014).

[8] Acxiom, "AOS for Marketers," http://aos.acxiom.com/marketers/ (viewed 5 Apr. 2014).

[9] Acxiom, "AOS: Audience Operating System," http://aos.acxiom.com/ (viewed 5 Apr. 2014).

[10] Acxiom, "AOS for Developers," http://aos.acxiom.com/developers/. "Yesterday, no one could effectively target the identical set of consumers on and offline," observes Acxiom's Nada Stirratt. "Today, with AOS, you can. In the online arena, we know relying on pixels leads to inaccurate data. AOS allows the use of consumer data that has been anonymized for true synchronized online and offline targeting, optimization and distribution across channels and devices. … Because of its integrated outlook, AOS can provide insight into targetable audiences across multiple channels. Acxiom focuses on partner networks where known audiences exist, not just cookie pulls. And we support analyzing all types of data (i.e. offline conversion data) in the platform, not just media-related data. … If a customer has access to other 3rd party data via their marketing database, we can take advantage of that by onboarding it to the online space and making it available for segmenting." "Acxiom's Nada Stirratt on the Game Changing Acxiom Audience Operating System (AOS)," The Makegood, 1 Nov. 2013, http://www.the-makegood.com/2013/11/01/acxioms-nada-stirratt-on-the-game-changing-acxiom-audience-operating-system-aos/ (both viewed 15 July 2014).

[11] Acxiom, "Partners," http://acxiom.com/partners/ (viewed 5 Apr. 2014).

[12] Michael Gorman and Geene Rees, "Harnessing the Power of Social Intelligence," Acxiom, http://www.nuibooks.com/power-of-social-intelligence-PDF-36694140/?rf=4 (registration required).

[13] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability."

Adara Media

Complaint number	2
Company profile	Adara Media uses proprietary data from its travel industry partners' search, purchase, and loyalty programs to profile and pinpoint specific individuals for targeted advertising.
Main website	www.adaramedia.com/
Safe Harbor/privacy statements	Adara Media admits in its Safe Harbor certification statement to being "… a global leader in helping consumer brands find new customers using advanced precision-targeting technology powered by Big Data sourced from the world's leading travel and hospitality companies," and to offering "…unparalleled access to first-party data combined with proprietary technology [that] enables advertisers to execute and optimize highly effective display, mobile, video, and social media ad campaigns."[1] Its corporate privacy statement, on the other hand, simply states that "Adara, Inc, complies with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. Adara has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[2] Additionally. as part of its "Privacy Promise," Adara offers a "Definition of Terms" section that appears to be at odds with the more rigorous interpretation of personal information and the use of cookies and other online tracking in the EU: **Personally Identifiable Information ("PII")** PII means your name, home and work address, telephone number, URL, email address and any other information that identifies you personally. **Non-Personally Identifiable Information** Non-Personally Identifiable Information means information that does not identify you personally. This information is anonymous, i.e. it does not identify you personally, and only includes information such as your computer's Internet Protocol ("IP") address, browser type, and activity on our Marketing Partners' websites. Non-Personally Identifiable Information may be collected by both Adara and its Marketing Partners. …

	Cookies Like many websites, we use "cookies" to collect information. A cookie is a small data file that we transfer to your computer's hard disk for record-keeping purposes. We use cookies to personalize your experience on our Site and to keep track of advertisements we believe are relevant to you. We set our cookies to expire after two years, however, as is the normal practice in our industry the two year expiration date is extended each time the cookie we gave you encounters our server. We do not use cookies to obtain PII. We do not link the information we store in cookies to any PII you submit while on our Site. In addition to Adara cookies, we may transfer Marketing Partner or other third party cookies to you to make it easier for you to navigate and make full use of our Site and the websites of said Marketing Partners and other third parties. Other than transferring Marketing Partner and other third party cookies to you when requested to do so Adara has no access to or control over these cookies. Adara uses a third-party tracking service that uses cookies, web beacons and log files to track Non-Personally Identifiable Information such as visitor traffic patterns on our site in the aggregate. We analyze this information to understand how many people visit our site in aggregate. This privacy statement covers the use of cookies by http://www.adaramedia.com only and does not cover the use of cookies by Marketing Partners or other third parties. … **Information Collection and Use** Adara is in the business of providing Services to its Marketing Partners. When collecting consumer information through the use of Cookies or obtaining consumer information from our Marketing Partners we do not attempt to collect PII, nor do we deliver ads to consumers based upon PII. We only collect, analyze and use Non-Personally Identifiable Information for the purposes of providing Services to our Marketing Partners. [3] While some of its definitions may differ from EU standards, Adara does provide users with a means of opting out from targeted advertising on its website: "You may Opt-Out of

	Adara's Services and Site at any time. If you prefer not to receive relevant advertising from us, simply click on the following link to Opt-Out."[4] That link, however, simply places an Adara opt-out cookie on the respondent's computer, and since most EU consumers will come in contact with Adara's targeted advertising through a hotel or airlines loyalty program, it is not clear that any of these consumers will ever see Adara's opt-out page.
Non-compliance/ false claims	In neither its Safe Harbor statement nor its Privacy Promise, does Adara disclose its ability—claims of "anonymity" notwithstanding—to identify specific individuals for personalized targeting, which the company readily discusses on its corporate website. "Adara uses exclusive, private data to connect online advertisers with customers," the company explains. "Our relationships with trusted data partners allow us to access hundreds of millions of data points that can pinpoint online buyers. We don't look for people who browse online—we've found the shoppers."[5] In describing its data management platform, moreover, the company tells it clients that the "Adara Audience Platform accesses premium, proprietary 1st party data—information that comes directly from the primary source—to connect your advertising with known online shoppers at scale. … Adara and our data partners have created a portfolio of premium consumer data, with hundreds of millions of pieces of data. Personal information stays private, while purchase and profile data is available to advertisers. Actual purchase patterns, life stages, lifestyle, and demographics are all at your fingertips."[6] Adara has access to over 250 million unique traveller profiles every month, provided by more than 70 data partners.[7] Remarkably, despite such precise tracking and targeting of consumers, the company nonetheless claims that it handles only "anonymous" data: "Adara brings consumers to advertisers with explicit, yet anonymous, purchase data. It works like this: From the millions of people browsing online … Adara's data partners deliver valuable profile information about proven buyers and qualified prospects—their purchase patterns, preferences, and demographics. Advertisers then use that information to create unique campaigns that specifically target that buyer—and others who fit the profile or target."[8] In the face of the evidence present in this complaint, Adara's claim of respecting consumer anonymity is misleading, and should be

	investigated.
FTC action on possible violations	Despite vague statements to DOC that this company helps to "find" customers and "optimize … campaigns," it fails to make clear to consumers, both by ambiguity and omission, its tracking and profiling of individuals. FTC should investigate and sanction Adara for failing to provide adequate Notice to consumers concerning (1) the full range of its data-mining and (2) the precision of its ad-targeting technologies, both of which operate at the individual level and track EU consumers based on their online identity, as well as (3) the selling of consumers full purchase profiles and other identifiable information that is not anonymized sufficiently to satisfy EU consumer expectations. FTC should investigate whether Adara's opt-out mechanism is ineffective in light of customers' lack of knowledge of Adara's existence and practices. Since the company fails to anonymize data before selling it to other companies, FTC should also investigate Adara for unauthorized Onward Transfer without consumers' consent.

[1] Adara Media, Safe Harbor Organization Information, expires 5/29/14, http://safeharbor.export.gov/companyinfo.aspx?id=20867 (viewed 8 Apr. 2014).

[2] Adara, "Adara Privacy Policy," http://adaramedia.com/privacy-promise (viewed 21 May 2014).

[3] Adara Media, "Privacy Promise," http://adaramedia.com/privacy-promise (viewed 11 June 2014).

[4] Adara Media, "Privacy Promise."

[5] Adara Media, "About Us," http://adaramedia.com/about-us (viewed 11 Apr. 2014).

[6] Adara Media, "What We Do," http://adaramedia.com/what-we-do (viewed 11 Apr. 2014).

[7] "Adara and Havas Media Announce an Agreement to Help Havas Media Reach Travelers Worldwide," 28 Apr. 2014, http://adaramedia.com/about-us/news-and-views-details/adara-and-havas-media-announce-agreement-to-help-havas-media-reach-traveler. Adara also has an advertising partnership with Twitter. Abhishek Shrivastava, "More Relevant Ads with Tailored Audiences," Twitter Advertising Blog, 5 Dec. 2013, https://blog.twitter.com/2013/more-relevant-ads-with-tailored-audiences (both viewed 15 July 2014).

[8] Adara Media, "What We Do—How It Works," http://adaramedia.com/what-we-do/how-it-works (viewed 11 Apr. 2014).

Adobe Systems

Complaint number	3
Company profile	Adobe Systems is a software company whose products range from publishing and design applications to online marketing services. It is the latter that are at issue here, including a data-driven marketing suite that collects, analyzes, and makes personal data "actionable" in its efforts to provide "a 360-degree view of the customer."
Main website	www.adobe.com/
Safe Harbor/privacy statements	"In Adobe's capacity as a data processor," the company writes in its Safe Harbor declaration, "Adobe acts on the instructions of [its EU/EAA] customers and does not own the personal information it may process on the customers' behalf."[1] Adobe's Safe Harbor Privacy Policy makes a similar claim: Adobe Systems Incorporated may receive personal information from Adobe subsidiaries …, our corporate customers, and other business partners in the EEA and Switzerland, such as name, email address, company name, title, postal address, telephone number, and preferences regarding our applications and websites. Any personal information sent to us may be used by Adobe Systems Incorporated and its subsidiaries and their agents and business partners for the purposes described at the time the information was collected. … Adobe Systems Incorporated provides hosted services to companies **…** . As part of providing these hosted services, Adobe Systems Incorporated may receive and process your personal information if you are a customer of one of these companies. When Adobe Systems Incorporated provides these services, we are referred to as a data processor. As a data processor, Adobe Systems Incorporated acts on the instructions of these companies and uses reasonable physical, electronic, and administrative safeguards to protect this personal information from loss; misuse; or unauthorized access, disclosure, alteration, or destruction. Companies that use an Adobe hosted service are responsible for complying with all other obligations in relation to the personal information they may collect from you.[2] In another statement, "Advertising Services," which

	appears in the Adobe Privacy Center section of its corporate website, Adobe discloses the kinds of information it collects on behalf of a company that uses Adobe's digital marketing services: When a company uses Adobe's advertising services, that company chooses how to implement and utilize Adobe's tools to determine what type of information to have Adobe collect on its behalf and what information to send to Adobe advertising services. The following are examples of the type of information these companies may choose to collect: • Where you go and what you do on that company's website, apps, or social media • Your browsing activity, including the URL of the web page you are visiting • The URL of the page that showed the link you clicked on that brought you to that company's website • The search you performed that led you to that company's website • Information about your browser and device, such as device type, device identifier (as it relates to mobile and table devices), operating system, connection speed, and display settings • Your IP address, which Adobe may use to approximate your general location • Information you may provide on that company's website or when interacting with that company within social media, including information on order and registration forms and information tied to your profile on social media accounts • Details relating to the types of products and services you have bought from that company • Ad campaign success rates, such as whether you clicked on a company's ad and whether viewing or clicking on the ad led you to purchase that company's products Examples of the type of information these companies may provide to Adobe advertising services are: • Email addresses

	• Phone numbers • Physical addresses • Details relating to the types of products and services you have bought from that company[3] This document also includes a discussion of Adobe's and its clients' use of cookies, as well as a mechanism (also cookie-based) to opt-out of Adobe advertising.
Non-compliance/ false claims	Adobe's discussion of its data-driven business practices in other contexts is much more revealing, depicting a company that is able to collect, combine, and analyze data about individuals in a powerful and precise data-mining apparatus. "Marketers finally have a complete, integrated solution for all their marketing efforts," Adobe declares on its website. "Analytics, social, media optimization, targeting, web experience management—and now cross-channel campaign management with Adobe Campaign—Adobe Marketing Cloud does it all. … Adobe Marketing Cloud pulls all your data together—including email, point-of-sale, CRM, third-party data, and more. With a single source of truth, you'll have powerful new ways to monitor and adapt campaigns, accurately assign attribution, and make informed decisions based on powerful, predictive logic."[4] That "single source of truth," however, comes at the expense of consumer privacy, consolidating as it does "… audience information from all available sources. It identifies, quantifies, and optimizes high-value target audiences, which can then be offered to advertisers … [using] First-party data (analytics and registration), Second-party data (strategic partners), and Third-party data (data vendors)."[5] According to Forrester, "What really set Adobe AudienceManager apart was the integration with Adobe Marketing Suite. With the additional acquisitions of buying platform Efficient Frontier, campaign management system Neolane, and tag management system Satellite, Adobe is well down the road in building out a marketing technology stack that broadly addresses data intelligence and audience delivery."[6] Adobe Social, moreover, enables the company's clients to make "real customer connections" and use "buzz-monitoring data to identify trends, opportunities, and threats."[7] According to Adobe, with this product companies can "[a]uto-generate and append unique tracking codes to social posts and apps" as well as

	"[m]onitor over 100 engagement metrics across your entire social presence and drill down for performance at the property, audience, or post level"—all of which involves tracking individuals across the Internet and monitoring their online actions to build detailed personal profiles.[8] The result of such efforts, and a primary reason for our challenge of Adobe's Safe Harbor certification, is the "… comprehensive and actionable view of an individual customer" that Adobe promises its clients.[9] Adobe's new Exchange, for example, makes available to the company's clients hundreds of third-party apps (including seoClarity for Adobe Analytics, Sina Weibo for Adobe Social, and Demandbase for Audience Manager), which collectively enable fine-grained targeting of specific individuals.[10] And Adobe is an active participant in these practices. "We see Adobe Consulting as an extension of our team," explained a spokesperson for the Milano, Italy-based UniCredit Group, "and they help us take a 100% data-driven approach, with every recommendation backed by industry best practices and years of experience."[11]
FTC action on possible violations	Adobe should be investigated by the FTC in light of the company's failure to provide adequate Notice to consumers concerning (1) the full range of its data-mining, (2) consumer profiling using various undisclosed data sources, and (3) precision ad-targeting technologies, all of which operate at the individual level. Instead the company's disclosure paints it as a passive vendor of tools, not profiles, and lists possible data collection by third parties without explaining the purposes for which Adobe collects and uses consumers' personal information. The omission of these practices from a Safe Harbor Notice statement greatly misleads consumers. Adobe's retention of consumer profile information and use of that data for new purposes makes it a responsible controller with full Safe Harbor duties. Although Adobe may not be using some of its cloud-services clients' data to target consumers with advertising, its omission of full disclosure of its data processing practices to EU citizens makes it impossible for them to understand or choose to avoid its set of powerful data profiling and targeting applications.

[1] Adobe, Safe Harbor Organization Information, expires 3/2/15, http://safeharbor.export.gov/companyinfo.aspx?id=21625 (viewed 8 Apr. 2014).

[2] Adobe, "Adobe Safe Harbor Privacy Policy," http://www.adobe.com/content/dotcom/en/privacy/safe-harbor.html (viewed 21 May 2014).

[3] Adobe, "Adobe Privacy Center: Advertising Services," http://www.adobe.com/content/dotcom/en/privacy/advertising-services.html (viewed 11 June 2014).

[4] Adobe, "Adobe Marketing Cloud," http://www.adobe.com/solutions/digital-marketing.html (viewed 29 May 2014).

[5] Adobe, "Adobe AudienceManager," http://www.adobe.com/il_en/products/audiencemanager.html (viewed 24 Apr. 2014). The Adobe Marketing Cloud Exchange, for example, includes links to some 40 third-party data providers, including Nielsen, MasterCard, Experian, Neustar, Acxiom, and eXelate. Adobe, "Exchange: Data," https://marketing.adobe.com/resources/content/resources/en/exchange/marketplace/data.html (viewed 1 July 2014).

[6] Joanna O'Connell, "The Forrester Wave: Data Management Platforms, Q3 2013," http://www.forrester.com/The+Forrester+Wave+Data+Management+Platforms+Q3+2013/fulltext/-/E-RES99501 (purchase required).

[7] Adobe, "Adobe Social," http://www.adobe.com/solutions/social-marketing.html. Adobe recently added a Facebook app to its Adobe Social service. Adobe, "Facebook for Adobe Social," https://marketing.adobe.com/resources/content/resources/en/exchange/marketplace/apps/facebook-for-adobe-social.html (both viewed 2 July 2014).

[8] Adobe, "Adobe Social: Solution Overview," July 2013, http://success.adobe.com/assets/en/downloads/product-overviews/24408_adobe_social_solution_overview_ue_v2.pdf (viewed 15 July 2014).

[9] Adobe, "Profile Management," http://www.adobe.com/solutions/digital-marketing/profile-management.html. (viewed 25 Apr. 2014).

[10] Adobe, "Exchange: All Applications," https://marketing.adobe.com/resources/content/resources/en/exchange/marketplace/apps.html (viewed 13 July 2014).

[11] Adobe, "UniCredit Group: Taking the European Market by Storm," Apr. 2013, http://wwwimages.adobe.com/content/dam/Adobe/en/customer-success/pdfs/unicredit-case-study.pdf (viewed 15 July 2014).

Adometry

Complaint number	4
Company profile	Adometry collects and processes data from a variety of online, offline, and mobile sources in order to provide its clients with a detailed view of the consumer purchase path. (Adometry was recently acquired by Google, and did not renew its Safe Harbor certification, which expired on 25 July 2014.)
Main website	www.adometry.com/
Safe Harbor/privacy statements	In its Safe Harbor certification statement, Adometry admits to collecting "… online advertising data as a data processor," but claims that it "… will only process the personal information it has collected from residents of the EEA and Switzerland on behalf of and under the instructions of its clients."[1] The company's privacy policy simply states that "Adometry complies with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland, and has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[2] Adometry's privacy policy also discusses the company's and its clients' use of cookies, the cookie-based opt-out mechanism that it offers, and a section on "Customer Policies," which indicates that Notice and Choice concerning Adometry's advertising services may be left to the discretion of its clients: > We strongly recommend that our customers, as data controllers (in the EU context), add statements or clauses to their privacy policies specifically describing their use of third party hosted optimization products and services (such as those provided by Adometry) and describing the details of such third party products and services (such as the use of cookies and clear gifs/web beacons). Further, we strongly recommend that each of our customers provide their visitors with information regarding the ability to opt-out of session data aggregation and analysis (see opt out section above).[3]
Non-compliance/ false claims	Nowhere in its Safe Harbor statement or in its privacy policy, however, is there a candid discussion of Adometry's role in a collaborative data-mining process that captures

	(as it boasts elsewhere) "Online exposure data at individual user level."[4] Adometry has "… partnerships with LiveRamp [now owned by Acxiom] and Datalogix [that] allow its customers to connect digital transactions to offline sales," as well as "… relationships with marketing data and technology companies such as Acxiom, which helps Adometry integrate more customer-centric behavioral data into its attribution model. This provides its attribution approach with a multidimensional view of the customer purchase path, including motivational behavior."[5] The true extent of Adometry's aggressive data-gathering efforts is clear from its product literature, which explains that the company "… processes and analyzes tens-of-billions of impressions and advertising transactions per month to identify the true consumer purchase-decision journey … ."[6] Its "Adometry Attribute Offline Connector allows marketers to create the linkage between online and offline consumer behavior, matching offline purchases to online marketing. … Adometry evaluates every single offline action to get the most accurate results for analysis."[7] And its Programmatic Connector uses "… Adometry's standard first- or third-party tags to collect impression and click data at the most granular level."[8] Adometry's "Audience & Data Partners" include Acxiom, Neustar, Adobe, Bizo, Datalogix, Digital Envoy, eXelate, IXI, LiveRamp, Nielsen, and Zvelo, giving the company access to vast amounts of detailed consumer data and allowing it to track individual's online and offline activities.[9]
FTC action on possible violations	Adometry should be investigated and sanctioned by FTC in light of the company's material omissions, comprising a failure to provide adequate Notice to consumers concerning (1) the full range of its data-mining and the precision of its tracking and targeting technologies, both of which operate at the individual level, (2) the company's use of individual's offline data in online advertising profiling, (3) its ability to track customers throughout the Internet in order to profile them for further marketing, and, in relation to its Consent Decree (4) its recent acquisition by Google.[10] The company's failure to renew its Safe Harbor certification without any communication to users about the deletion of their personal information seemingly is a clear violation of FAQ 6 of the Safe Harbor. Concerning the control over the purposes for data use that Adometry exercises (not to mention its exclusive control of the means of processing

	and its custom of combining personal information from numerous sources), the company's self-characterization as a processor appears to be a material misrepresentation. The fact that Adometry suggests, but does not require, companies it deals with to add disclosures that would cover some of Adometry's practices (but, for some reason not its underlying purposes) shows that it is aware of its duties but only regards them as suggestions rather than mandatory commitments it has made.

[1] Adometry, Safe Harbor Organization Information, expires 7/25/14, http://safeharbor.export.gov/companyinfo.aspx?id=19054 (viewed 8 Apr. 2014).

[2] Adometry, "Privacy Policy," http://www.adometry.com/privacy.php (viewed 21 May 2014).

[3] Adometry, "Privacy Policy."

[4] Adometry, "Ease of Onboarding," http://www.adometry.com/technology-services/ease-of-onboarding.php (viewed 30 Apr. 2014).

[5] Tina Moffett, "Quick Take: Google Acquires Adometry," Forrester, 8 May 2014, http://www.forrester.com/Quick+Take+Google+Acquires+Adometry/fulltext/-/E-RES116601 (viewed 2 July 2014)

[6] Adometry, "Corporate Fact Sheet," 2012, http://www.adometry.com/cms-assets/documents/68055-180526.adometry-backgrounder.pdf (viewed 30 Apr. 2014).

[7] Adometry, "Adometry Attribute Offline Connector," 2013, http://www.adometry.com/assets/files/resources/uploads/adometry-offline-connector.pdf (viewed 30 Apr. 2014).

[8] Adometry, "Programmatic Connector," https://www.adometry.com/assets/files/resources/uploads/Adometry_Programmatic_Connector.pdf (viewed 7 July 2014).

[9] Adometry, "World Class Partners," http://www.adometry.com/partners/audience-and-data-partners.php (viewed 29 May 2014).

[10] Mike Shields, "Google to Acquire Online Attribution Firm Adometry," *The Wall Street Journal*, 6 May 2014, http://blogs.wsj.com/cmo/2014/05/06/google-to-acquire-online-attribution-firm-adometry/ (viewed 29 May 2014).

Alterian

Complaint number	5
Company profile	Alterian was a UK-based supplier of marketing automation software and services before its acquisition by SDL International in December 2011.
Main website	www.alterian.com/
Non-compliance/ false claims	Alterian's Safe Harbor certification is still listed as "current" (through 13 August 2015), even though (1) the company was acquired by SDL in early 2012, six months *before* its most recent certification; (2) the privacy policy to which it directs users on its Safe Harbor page belongs to SDL; and (3) the website URL that it lists on that page—"www..com"—doesn't work at all.[1] (The company's erstwhile domain, alterian.com, simply redirects to sdl.com.) Alterian has apparently failed to comply with Safe Harbor FAQ 6.[2] The fact that it has failed to make meaningful disclosures to EU consumers about whether personal information was deleted or segregated, or whether the merged company has sought re-certification under the Safe Harbor demonstrates a material omission in violation of Notice and Choice obligations. Even if both companies were Safe Harbor members before a merger, the combination of the two cannot satisfy requirements that EU consumers be notified of data uses and given the chance to opt out of Onward Transfer that was not disclosed at the time personal information was collected.
FTC action on possible violations	Because both Alterian and its parent company, SDL (see complaint no. 26, below) failed to handle their 2012 merger properly with regard to the required Safe Harbor documentation, FTC should investigate and sanction the companies accordingly.

[1] "SDL's Acquisition of Alterian Further Demonstrates SDL's Commitment to Drive the Global Customer Experience," 30 Jan. 2012, http://www.sdl.com/aboutus/news/pressreleases/2012/sdl-acquires-alterian.html (viewed 17 May 2014); Alterian, Safe Harbor Organization Information, expires 8/13/15, http://safeharbor.export.gov/companyinfo.aspx?id=23958 (viewed 11 Aug. 2014).

[2] U.S. Department of Commerce, "FAQ - Self-Certification," export.gov, http://export.gov/safeharbor/eu/eg_main_018388.asp (viewed 21 May 2014).

AOL

Complaint number	6
Company profile	AOL is a mass media company that distributes content, products, and services to consumers, publishers, and advertisers. Of relevance to this request, AOL provides advertising services that include behavioral and household-level tracking and targeting as well as detailed profiling of individuals.
Main website	www.aol.com/
Safe Harbor/privacy statements	According to its Safe Harbor statement, "AOL's offerings include portal services (such as AOL.com and The Huffington Post) and advertising services (such as those offered by AOL Advertising). In connection with these offerings, AOL may collect personal information to operate and improve the Web sites and services; to personalize content and advertisements; to serve advertisements; to fulfill requests for products, programs, and services; to communicate with customers and respond to inquiries; to conduct research about use of AOL offerings; to help offer other products, programs, or services that may be of interest to users … ."[1] Beyond this acknowledgement of "personalized advertising"—which is really individual profiling—AOL fails to explain adequately *how* such data are collected from consumers, how they are processed and used for profiling, and to what extent consumers can opt out of the profiling process. Additionally, the main AOL privacy page—AOL Privacy Highlights—to which users are directed when they click on the lone privacy link at the bottom of the AOL.com home page, has *no mention* of Safe Harbor whatsoever. (It does include a section on opting out, however, which directs users to an "Opt Out form Online Behavioral Advertising (Beta)" page from the Self-Regulatory Program for Online Behavioral Advertising.)[2] Only when one clicks on the single in-line reference to the "full privacy policy" on the Privacy Highlights page does one find a reference to Safe Harbor: a one-sentence assurance that "AOL adheres to the EU-US Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement, and is registered with the U.S. Department of Commerce's Safe Harbor Program," which includes an embedded link to *yet another* page that includes one additional sentence—"AOL Inc. collects and

	processes personal information from users within the European Union in connection with its various product and service offerings, which include portal services (such as AOL.com); social networking services; and advertising services (such as those offered by Advertising.com)"—plus two addresses for questions or complaints.[3] (The AOL Advertising website, similarly, which may have even more reason to conduct a full discussion of the Safe Harbor Framework, is equally wanting in this regard, with the same trifurcated, cursory approach to Safe Harbor.)[4]
Non-compliance/ false claims	A closer examination of AOL's advertising practices—which include both behavioral and household-level targeting—underscores the inadequacy of its efforts to meet the Safe Harbor Notice and Choice requirements.[5] AOL has created a range of online profiling services that collect, analyse, and use detailed consumer data to track individuals across their online journeys and target them with personalized advertising. AOL's AdLearn technology, for example, processes up to 4 billion transactions a day, using over 400 servers to bid on 3.5 billion impressions daily to reach over 188 million users on over 6,000 websites each month.[6] "Since it first launched," the company boasts, "AdLearn has been the decisioning engine behind trillions of impressions and billions of user actions … ."[7] Although AOL claims that "[s]trict privacy regulations are in place to prohibit the linking of PII (personally-identifiable information) to campaign and/or advertiser data," its use of "3rd party data matching vendors and unique IDs in place of PII" enable it to target specific individuals with fine-grained precision.[8] As the company explains to its clients, "By combining the technology and scale of Advertising.com with the extensive AOL user database, you'll learn more about your customers than you ever thought possible! … Strategic Insights Platform (SIP) analyzes audience and behavioral data to create a profile of your customer."[9] AOL's data partners include BlueKai, LiveRamp, AddThis, Datalogix, Bizo, Experian, Neustar, eXelate, IRi, Nielsen Catalina, and IXI, none of which is mentioned in its Safe Harbor documentation.[10] Nor does AOL mention its recent $90 million acquisition of Gravity, whose "…proprietary Interest Graph … pulls out users' interests, habits, and preferences to allow for customized serving of ads and/or editorial content."[11]

	AOL's one-size-fits-all Safe Harbor statement and its segmented, difficult-to-follow privacy policy fall short of clearly and adequately describing the various ways in which the company collects consumer data for the purposes of targeted advertising. AOL may have made strides in unifying its several advertising properties under the ONE banner, which promises to "… leverage the teams and technologies behind Adap.tv, AdLearn Open Platform (AOP) and MARKETPLACE to drive powerful brand insight and action across all screens including TV, formats and inventory types." But, by fracturing its disclosures and failing to describe the purposes and methods of its data processing, it seems there are no disclosures or mechanisms to satisfy Notice and Choice concerning this new personalized advertising service, which AOL describes as "… the first platform that empowers brands with a holistic view of the consumer's journey through the marketing funnel, and makes that insight actionable, in real-time on the platform."[12]
FTC action on possible violations	AOL's Safe Harbor status should be investigated by FTC in light of the company's failure to provide an adequate explanation of the full range of its targeted advertising practices and personal information amalgamation as they relate to AOL's participation in the EU-US Safe Harbor Framework. At present, there is no mention of Safe Harbor on the AOL privacy page to which EU consumers are directed from either the AOL homepage or the link on the company's Safe Harbor page on the Export.gov website. This will likely mislead EU users and not properly inform them of their rights and AOL's commitments under the Safe Harbor. Furthermore, AOL's marketing materials reveal considerable admissions of consumer profiling, behavioral targeting, and identification of individuals to third parties that is not "anonymous" under EU legal standards. As a data controller and Safe Harbor participant AOL has made commitments that it seems to be shirking, directly injuring EU consumers and their expectations of privacy.

[1] AOL, Safe Harbor Organization Information, expires 9/23/14, http://safeharbor.export.gov/companyinfo.aspx?id=20249 (viewed 14 May 2014).

[2] Digital Advertising Alliance, "Opt Out form Online Behavoral Advertising (Beta)," http://www.aboutads.info/choices/ (viewed 11 June 2014).

[3] AOL, "AOL Privacy Policy," Last Updated 06-28-2013, http://privacy.aol.com/privacy-policy/; AOL, "European Union Safe Harbor," http://privacy.aol.com/eu-safe-harbor/ (both viewed 14 May 2014).

[4] AOL Advertising, "Privacy Policy," http://advertising.aol.com/privacy; AOL Advertising, "AOL Advertising Privacy Policy," http://advertising.aol.com/privacy/aol-advertising (both viewed 14 May 2014); AOL, "European Union Safe Harbor."

[5] See, for example, AOL Advertising.com, "Targeting," https://www.advertising.com/advertiser/targeting#null (viewed 29 May 2014).

[6] AOL Advertising.com, "AdLearn," https://www.advertising.com/advertiser/adlearn (viewed 2 July 2014)

[7] AOL Advertising.com, "Platform Features: Performance + Scale," http://www.adlearnop.com/platform-features/performance-scale (viewed 7 July 2014).

[8] AOL Advertising.com, "Platform Features: Data Access," http://www.adlearnop.com/platform-features/data-access (viewed 29 May 2014).

[9] AOL Advertising.com, "Platform Features: Campaign + Audience Insights," http://www.adlearnop.com/platform-features/campaign-audience-insights (viewed 29 May 2014).

[10] AOL Advertising.com, "Platform Features: Data Access."

[11] Liva Judic, "AOL Plays Catch-Up on Ad, Content Targeting with $90.7 Million Gravity Buy," ClickZ, 24 Jan. 2014, http://www.clickz.com/clickz/news/2325058/aol-plays-catch-up-on-ad-content-targeting-with-usd907-million-gravity-buy (viewed 29 May 2014).

[12] "AOL to Build First Cross-Screen Programmatic Advertising Platform - ONE By AOL," 26 Mar. 2014, http://corp.aol.com/2014/03/26/aol-to-build-first-cross-screen-programmatic-advertising-platfor/ (viewed 30 Apr. 2014).

AppNexus

Complaint number	7
Company profile	AppNexus provides a platform combining real-time bidding, third-party data acquisition, and audience analytics for companies wanting to engage in online data profiling and consumer targeting.
Main website	www.appnexus.com/
Safe Harbor/privacy statements	The AppNexus "… technology platform that our clients use to buy, sell, and deliver online advertising," according to the company's Safe Harbor declaration, "… is designed to enable these advertising purposes through the use of non-personally identifiable information, which includes such things as browser version, cookie id, page visited, date and time, and IP address."[1] Although AppNexus provides two privacy policies on its website, one for the AppNexus Platform ("For personal information we transfer from the European Union to the United States, we adhere to the principles of the U.S.-E.U. Safe Harbor Framework and U.S.-Swiss Safe Harbor Framework, as set forth by the U.S. Department of Commerce") and one for the company generally ("For sensitive information, as required by the Safe Harbor Principles, we will obtain authorization prior to sharing the information or using it for a purpose other than that for which it was collected"), neither sheds any light on its non-PII claims.[2] AppNexus does, however, provide a cookie-based mechanism that allows users "… to opt out of having the [AppNexus] Platform used to select ads for your browser based on your online web browsing behavior."
Non-compliance/ false claims	The company's non-PII claims mean little in the context of AppNexus's collaborative efforts to aggregate and analyze consumer data for the purposes of personal profiling and targeted marketing (which the company regularly trumpets in its own product and services literature). AppNexus works with a broad array of other data profiling partners to build detailed digital profiles that combine online, offline, and mobile data tied to individual consumers. AppNexus's App Marketplace, for example, includes a number of third-party user-data apps, including BlueKai's Audience Creator App, eXelate's Audience eXplorer App, Lotame's Crowd Control App, and Neustar's Audience Wizard App, all of which gather personal information for marketing purposes in ways that are

	contradictory to AppNexus's Safe Harbor declaration.[3] "With a single click," AppNexus tells its clients, "you can integrate new capabilities into your network … ," capabilities that based upon the collection and analysis of significant amounts of personal information.[4] Additionally, LiveRamp (whose CRM Retargeting App is part of the AppNexus App Marketplace) was recently acquired by Axciom, which represents a significant commingling of everyone's data across the board.[5] As an active participant in real-time bidding, moreover, AppNexus uses its Big Data technology to update its consumer profiles on the fly. "We see in our peak day I think 39.5 billion ads in one individual day," explains AppNexus co-founder and Chief Technology Officer Mike Nolet. "It's about 600,000-odd requests per second. … And the reality of that is, a lot of that buying is being driven by behavior, and so we must have cookie data server-side. … We have to be able to do 600,000 reader requests a second. Now we deliver about 150,000 – 170,0000 ads a second, so every time we win an auction we do write updates to our cookie store."[6] As the company explains, "The AppNexus platform uses advanced machine learning and probability modeling to match the right ads with the right users. … Our granular reporting tools provide you with up-to- the-hour information and are available in local time zones and multiple currencies. With impression level views, our reporting provides sophisticated ways to report on and manage your data, and helps you to drive actionable business insights."[7] In a recent report on the impact of such advertising in Europe, Graham Wylie, senior director of EMEA and APAC marketing for AppNexus, observed that whatever it's called—real-time bidding or real-time advertising, AdTech or programmatic marketing—"the goal has always been the same: to give advertisers the agility to tailor their message for an audience of one, anywhere on the web and in less than the 200 milliseconds it takes a page to load. It has massive implications for brands, advertising & media buying agencies and the website publishers that use advertising to fund their free content."[8] Such technology, unfortunately, also has massive implications for consumer privacy.
FTC action on possible violations	FTC should investigate AppNexus in light of the company's false claim of restricting its data collection and use to non-

	identifiable data, a significant legal point that affects EU consumers' rights, and its corresponding failure to provide an adequate Notice and Choice concerning the detailed personal data that it does collect (both individually and in partnership with other data-mining firms) from unsuspecting consumers. The company is collecting and sharing information identifying EU consumers and using it to build consumer profiles with other data companies without proper consumer consent, in violation of commitments it has made under the Safe Harbor.

[1] AppNexus, Safe Harbor Organization Information, expires 6/27/14, http://safeharbor.export.gov/companyinfo.aspx?id=19346 (viewed 8 Apr. 2014).

[2] AppNexus, "Platform Privacy Policy," http://www.appnexus.com/platform-policy; AppNexus, "Privacy Policy," http://www.appnexus.com/privacy-policy (both viewed 21 May 2014).

[3] AppNexus, "AppNexus Apps," http://www.appnexus.com/appnexus-apps (viewed 8 Apr. 2014).

[4] AppNexus, "Build a Differentiated Ad Network," http://www.appnexus.com/differentiated-ad-network (viewed 1 May 2014).

[5] Scott Howe, "And So It Begins," Acxiom, 1 July 2014, http://www.acxiom.com/begins/ (viewed 5 July 2014); Calvin Pappas, "LiveRamp is Now Live on the AppNexus Marketplace," LiveBlog, 22 Mar. 2013, http://blog.liveramp.com/2013/03/22/liveramp-is-now-live-on-the-appnexus-marketplace/ (viewed 15 July 2014).

[6] Quoted in "CTO Panel Discusses the Impact of Real-time Big Data," Aerospike, 14 Dec. 2012, http://www.aerospike.com/blog/impact-of-real-time-big-data-on-the-business-2/ (viewed 7 July 2014).

[7] AppNexus, "Build a Differentiated Ad Network," http://www.appnexus.com/differentiated-ad-network (viewed 15 July 2014).

[8] Quoted in Circle Research, "Why and How 'Programmatic' is Emerging as Key to Real-time Marketing Success," June 2014, http://www.iabeurope.eu/files/7214/0197/2316/The_Why_and_How_of_programmatic_-_European_report_-_FINAL.pdf (viewed 7 July 2014).

Bizo

Complaint number	8
Company profile	Bizo offers a targeted business-to-business advertising platform that is used by such major corporations as American Express, Mercedes Benz, Porsche, Microsoft, and UPS to reach more than 120 million business professionals around the world. Claims of anonymity and non-personally-identifiable information notwithstanding, Bizo's business model is based on its compilation of detailed personal profiles of individuals. (In July 2014, LinkedIn announced its plans to acquire Bizo.)
Main website	www.bizo.com/
Safe Harbor/privacy statements	Bizo claims in its Safe Harbor statement to be "… a B2B audience targeting platform that uses non-personally identifiable business demographic information … collected from a wide variety of sources in a manner that is anonymous and non-personally identifiable," while its privacy policy declares that "Bizo complies with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Information from European Union member countries and Switzerland. Bizo has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[1] Concerning the company's data collection and usage, that policy explains that > Bizo has developed a proprietary technology that converts and optimizes information about business people into non-personally identifiable business demographic segments called Bizographics. This information includes, but is not limited to, information such as industry, company size, functional area, seniority, location and gender. … Bizo may collect, host and manage the Personal Information that our Web site partners have collected from their sites. This data is the property of the particular Web site partner who is collecting such information and is subject to its privacy policy. Bizo will not use this data in any way that is not authorized by that partner.[2]
Non-compliance/ false claims	Doubts about "anonymized" data abound, and Bizo offers no proof that its proprietary "Bizographics" could not be "re-identified." Indeed, Bizo's product information reveals a

	company that is much more involved in precision ad targeting than its Safe Harbor statement and privacy policy would suggest, and raising doubts about its claims of anonymity. Bizo's technology and data partners, for example, include eXelate, Google, BlueKai, Genome, Audience Science, AOL, Lotame, AppNexus, LiveIntent, MediaMath, Microsoft, Tribal Fusion, Turn, Undertone, X+1, Monetate, Adobe, and BrightRoll.[3] Such partnerships, including one with Oracle's Eloqua platform, suggest that Bizo is focused on the collection of personal information on identifiable individuals. With the Oracle Eloqua AdFocus application, for example, "… [u]sers can target personalized placements through the Bizo ad network … ."[4] The company's marketing platform, Bizo Data Solutions, enables companies "… to better understand and more efficiently engage target audiences across their entire marketing funnel … to [i]dentify which audiences are visiting their websites and social channels … [e]ngage website audiences with personalized content … [and] [r]each and influence their target audiences anywhere online by combining Bizo's data management capabilities with precise ad targeting."[5] Bizo's real-time bidding (RTB) platform is equally inimical to user privacy and anonymity, combining personal data from multiple sources with cookie-based user targeting and retargeting of individuals who have previosusly visited a company's website. "Real-time bidding," Bizo explains to its clients, "can provide you with highly detailed analytics insights about your prospects … ."[6] Bizo's integration with other marketing products and services, moreover, including those of Salesforce, BlueKai, and Google, illustrates how such data profiling cannot be considered anonymous. These Bizo Data Solutions, the company explains, allows marketers to "… [e]ngage website audiences with personalized content" and to undertake precise ad targeting."[7]
FTC action on possible violations	Bizo should be investigated by FTC in light of the company's false claim of restricting its data collection and use to non-identifiable data, the effect on its disclosures of its combination of this data with personal information gathered by clients, and its corresponding failure to provide adequate Notice and Choice concerning the detailed personal data and other identifiable information that it collects and sells to others (both on its own and by

	incorporating other companies' data-mining products).

[1] Bizo, Safe Harbor Organization Information, expires 12/8/14, http://safeharbor.export.gov/companyinfo.aspx?id=20825(viewed 8 Apr. 2014); Bizo, "Bizo, Inc., Privacy Policy," http://www.bizo.com/privacy-policy/ (both viewed 21 May 2014).

[2] Bizo, "Bizo, Inc., Privacy Policy."

[3] Bizo, "Bizo Channel Partners," http://www.bizo.com/channel-programs/ (viewed 31 May 2014).

[4] Kelly Liyakasa, "Oracle Eloqua, Bizo To Fuel Each Other's Marketing Products," Ad Exchanger, 24 Oct. 2013, http://www.adexchanger.com/digital-marketing-2/oracle-eloqua-bizo-to-fuel-each-others-marketing-products/ (viewed 1 May 2014).

[5] Bizo, "Bizo Marketing Platform," http://media.bizo.com/www/marketing/Bizo-DataSheet_DataSolutions_v1.pdf (viewed 7 July 2014).

[6] Bizo, "The 5-Minute Real-Time Bidding (RTB) Primer," http://com-bizo-public.s3.amazonaws.com/www/marketing/Bizo-5_Min_RTB_Primer.pdf (viewed 1 May 2014).

[7] Bizo, "Business Data Solutions," http://www.bizo.com/data-solutions/; Bizo, "Bizo Marketing Platform: Data Solutions," http://media.bizo.com/www/marketing/Bizo-DataSheet_DataSolutions_v1.pdf (both viewed 1 May 2014).

BlueKai

Complaint number	9
Company profile	BlueKai (now owned by Oracle) is a data management platform that provides third-party data for use in personal profiling and consumer tracking for the purposes of delivering targeted advertising.
Main website	www.bluekai.com/
Safe Harbor/privacy statements	BlueKai's Safe Harbor statement to the Commerce Department, a mere two sentences, offers little insight into what the company does with consumer data and why, simply citing its "… work with website publishers and advertisers to collect non-personally identifying information over time and across the Internet to determine or predict user characteristics, behavior or preferences typically for use in ad delivery."[1] BlueKai's privacy policy (which begins with the statement "BlueKai has been acquired by Oracle and will soon transition to the Oracle Privacy Policy" and includes a link to that policy) states that "... BlueKai complies with the U.S.-EU Safe Harbor Framework and the U.S. Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personally identifiable information from European Union member countries and Switzerland. BlueKai has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[2] The privacy statement also offers the following details about the company's data-collection and usage practices: BlueKai's mission is to build the world's most comprehensive online data directory with utmost attention and diligence to ensuring your anonymity and privacy. Our business is based upon the collection and use of anonymous customer preferences via partner websites in order to allow advertisers, publishers, and other content providers to deliver content that is relevant and meaningful to their users. … We collect non-personally identifiable information regarding offline collected attributes and digital usage patterns of users of mobile devices and computers. In this policy, we refer to this non-personally identifiable information, together with other non-personally identifiable information that we obtain from third parties in order to influence which types of marketing

	messages and other content are displayed to you, as "Preference Data." We use Preference Data to prepare groups of users, referred to as "segments," based upon their behavior and preferences. … We use non-personally identifiable means, including "cookies", "pixel tags," and in some instances, statistical ID's, to collect and store Preference Data. … We also may collect demographic information such as a user's gender, age, and income range. In addition, we may collect information about a user's browsing behavior, such as the date and time they visit the Web pages on which we are collecting Preference Data, the content areas or pages of the Web sites that a user visits (e.g., "sports section" or "technology section"), and other click-stream data, none of which includes personal information about the user. … BlueKai enables clients to utilize Preference Data via mobile devices such as smart phones and tablets. In many respects, the process we use in mobile is similar to those we've used for our online Preference Data. However, as cookies are less reliable on mobile devices, BlueKai uses statistical ID's to help us process mobile Preference Data. The use of statistical ID's does not impact BlueKai current data retention rate.[3] BlueKai also includes cookie-based means for users to opt out of the company's collection of Preference Data.[4]
Non-compliance/ false claims	Despite the company's claims of ensuring users' anonymity and privacy, BlueKai's own product applications reveal a data profiling and targeted advertising enterprise of enormous proportions. Claiming to be "… the industry's leading cloud-based big data platform that enables companies to personalize online, offline and mobile marketing campaigns with richer and more actionable information about targeted audiences. BlueKai's Data Management Platform (DMP) centrally organizes a company's customer and audience data in the cloud to help implement personalized marketing campaigns across all channels … ."[5] BlueKai's Audience Data Marketplace is billed as "the world's largest collection of branded and unbranded 3rd party data available online," providing "… direct access to more than 200 data providers."[6] Offering detailed profiles of over 700 million consumers, BlueKai's technology allows its clients to "[s]lice and dice [their] own online and offline first-party data … . Marketers can pull in

	and analyze all audience data presenting a 360-degree view … .”[7] On its own and in collaboration with other data-driven marketers, BlueKai threatens the privacy of EU citizens and consumers. And now, as part of Oracle, the two companies “will enable Marketers to: Manage online and offline campaigns through a single hub across owned, earned, and paid media; Build more complete customer profiles, enriched with detailed 1st party data, easily accessible 3rd party data, and new 2nd party partner data; Deliver personalized content and offers based on more comprehensive customer behavior data.”[8]
FTC action on possible violations	BlueKai should be investigated by FTC in light of the company’s false claims of restricting its data collection and use to non-personally identifiable data, and its corresponding failure to provide adequate Notice and Choice concerning the detailed personal data that it does collect. It is questionable that its cookie-based opt out is sufficiently clear or effective, especially since BlueKai collects user data across devices that do not use cookies. Its disclosures to officials and consumers about predicting user behavior for advertising falls far short of its role processing, buying, selling, and trading vast amounts of personal information among hundreds of third parties—most of whom will receive EU consumer data with no Notice or opt out offered to individuals. The company’s promises to allow clients to incorporate and use first-party and third-party data further undercuts its claims of anonymity. BlueKai’s disclosure about the data it collects does not come close to describing the large amount of data collection, analysis, and consumer targeting it purports to do in its materials aimed at prospective clients.

[1] BlueKai, Safe Harbor Organization Information, expires 3/12/15, http://safeharbor.export.gov/companyinfo.aspx?id=22352 (viewed 8 Apr. 2014).

[2] BlueKai, "Privacy Policy," http://bluekai.com/privacypolicy.php (viewed 21 May 2014).

[3] BlueKai, “Privacy Policy.”

[4] BlueKai, “Consumers,” http://bluekai.com/consumers.php#optout (viewed 11 June 2014).

[5] BlueKai, “About Us,” http://bluekai.com/about-us.php (viewed 2 May 2014).

[6] BlueKai, “Data Providers,” http://bluekai.com/data-providers.php (viewed 31 May 2014).

[7] BlueKai, "Data Management Platform," http://bluekai.com/data-management-platform.php (viewed 2 May 2014).

[8] Oracle, "Oracle Buys BlueKai," http://www.oracle.com/us/corporate/acquisitions/bluekai/general-presentation-2150582.pdf (viewed 7 July 2014).

Criteo

Complaint number	10
Company profile	Criteo is a personalized marketing company that works with Internet retailers to serve targeted online display advertisements to consumers who have previously visited the advertiser's website. Such "re-targeting" tactics, based on the compilation of detailed personal profiles, tracks individuals from site to site without their knowledge and consent or other adequate privacy safeguards.
Main website	www.criteo.com/
Safe Harbor/privacy statements	Although Criteo's Safe Harbor statement claims that "… [i]t does not collect personally identifiable information of the visitor nor store the IP addresses of visitors for OBA [online behavioral advertising] purposes," it also admits that its "… browser cookie tracks the products viewed by the visitor and pages visited of the individual advertiser for whom Criteo is delivering ads."[1] Its corporate privacy policy assures visitors that "Criteo complies with the U.S. – E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. Criteo has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[2] That privacy policy also makes a number of other assertions concerning Criteo's data-collection and usage practices: Criteo specializes in creating personalized advertisements. We work with online partners to build advertisements for users who visit their website or mobile applications and with publishers to display personalized advertisements. Our aim is to deliver advertisements by displaying products and/or personalized banners that you might be interested in, based on your recent browsing behavior. … We collect only anonymous data through anonymous cookies or equivalent identifiers that record: • events related to your activity on the partner's website (such as the number of pages viewed, the products you viewed on that website, your searches made on the partner's website)

	• information provided by trusted partners that may include socio-demographic data such as age range, • information related to your device (device type, operating system, version) • and events related to the Criteo ad serving activity such as the number of ads displayed to you. We do know that the internet browser and/or mobile operating system you are using has visited one of our partner sites in the last thirty days. … We share information collected with our subsidiaries or affiliated companies. We share aggregated data with our partners, i.e. data that does not permit identification of a partner, or permit you to be identified. We share non-aggregated data only upon approval of our partners and in compliance with our commercial agreements. … Criteo "tags" visitors to its partners' websites with anonymous browser cookies. Users tagged by Criteo are given an anonymous identifier. At no point does Criteo collect personal data, such as your name or address. The browser cookies track the products viewed by the visitor and pages visited of the partner for whom Criteo is delivering ads. Pixel tags are used by Criteo to transfer anonymous data from our partner's websites to Criteo's servers.[3] Criteo also offers two opt-out mechanisms, one specifically for Criteo ("If you no longer want to be exposed to Criteo personalized banners, you can opt out simply by clicking on the opt-out button below"), and another designed specifically for EU consumers through IAB Europe's Opt-Out Platform.[4]
Non-compliance/ false claims	An examination of the company's overview of its tracking and targeting technology—"We are a global technology company that enables e-commerce companies to leverage large volumes of granular data to efficiently and effectively engage and convert their customers"—renders any claim of "anonymity" all but meaningless.[5] "We have access to two types of differentiating data," the company explains: "(1) valuable consumer purchase behavior data, including products that a consumer has recently looked at or purchased; and (2) our own operating data and insights, which we have accumulated through our experience in

	delivering over 500 billion internet display advertisements."[6] As the company explains in a Securities and Exchange Commission filing, "We partner with our clients to track activity on their websites and optimize our advertising placement decisions based on that activity and other data … . Every day we are presented with billions of opportunities to connect individuals that are browsing the internet … with relevant messaging from our clients. For each of these opportunities, our algorithms will have analyzed massive volumes of data to observe and predict user intent and deliver specific messaging and products … . Access to high quality data assets fuels the accuracy of our algorithms. These data assets include our clients' sensitive and proprietary data, such as transaction activity on their websites; … third-party data, such as customer demographic and behavioral data derived from third-party cookies; as well as internally developed data that includes vast and proprietary knowledge we have extracted from having delivered and measured responses to over 500 billion advertising impressions."[7] Criteo's special brand of targeting, moreover, focusing on those consumers who have already visited a website, is particularly invasive, based as it is on stalking those users as they traverse the Internet: "Ninety-five percent of the visitors who come to a website do not complete a transaction. Instead, they wander away without buying. Criteo's personalized retargeting service brings them back to the fold."[8] With its retargeting technology integrated with a number of major ad exchanges (including AppNexus, Casale, Google, Microsoft, OpenX, PubMatic, and Rubicon), Criteo's reach is extensive.[9] And the company has been especially active in the EU, working with Google's DoubleClick Ad Exchange. "Early on, Criteo recognized the scale that the DoubleClick Ad Exchange (ADX) could deliver," a Google case study reports. "As a result, Criteo was the first buyer to go live with RTB on the ADX in Europe. Today, Criteo is a high volume, global buyer using real-time bidding with ADX. They're seeing great results in more than 19 countries."[10] Curiously, Criteo seems aware that its particular form of digital profiling raises privacy concerns. As the company acknowledges in its "Smart CMO's Survival Handbook for Data-driven Advertising," "Data-driven advertising puts your company in contact with sensitive consumer information that could be subject to regulations. And those

	regulations change faster than you can say, 'Of course we're compliant!'"[11] Safe Harbor standards have *not* changed, and yet for a variety of reasons (including its recent acquisition of AdQuantic, which is not mentioned in its Safe Harbor documentation), Criteo's certification must be investigated.[12]
FTC action on possible violations	Criteo's Safe Harbor certification should be investigated by FTC in light of the company's insufficient description of its complex retargeting and consumer profiling in consumer-facing disclosures, and its corresponding failure to provide adequate Notice concerning the detailed personal data that it does collect and create through tracking consumers and gathering identifiable information about their actions. Criteo's data commingling and sharing of personal information with "affiliated companies" also merits scrutiny under the Notice and Choice requirements. Moreover, telling EU consumers that no personal information is gathered or used in behavioral advertising should be investigated as an affirmatively misleading statement considering how such profiling works.

[1] Criteo, Safe Harbor Organization Information, expires 3/20/15, http://safeharbor.export.gov/companyinfo.aspx?id=22257 (viewed 3 May 2014).

[2] Criteo, "Criteo Website Privacy Policy," http://www.criteo.com/en/criteo-privacy-policy (viewed 21 May 2014).

[3] Criteo, "Privacy Policy," http://www.criteo.com/en/privacy-policy (viewed 11 June 2014).

[4] "Your Online Choices," http://www.youronlinechoices.com/uk/your-ad-choices (viewed 11 June 2014).

[5] Criteo, "Form F-1 Registration Statement Under the Securities Act of 1933," Securities and Exchange Commission, 18 Sept. 2013, p. 1, http://www.sec.gov/Archives/edgar/data/1576427/000119312513369592/d541385df1.htm (viewed 4 May 2014).

[6] Criteo, "Form F-1 Registration Statement Under the Securities Act of 1933," pp. 6, 8.

[7] Criteo, "Form 20-F filing with the U.S. Securities and Exchange Commission," annual report for the fiscal year ending 31 Dec. 2013, p. 60, http://ir.criteo.com/secfiling.cfm?filingID=1193125-14-85442&CIK=1576427 (viewed 15 July 2014).

[8] Google, "Criteo Gains Great Results and Scale by Retargeting Audiences through Real-time Bidding with DoubleClick Ad Exchange," 2011,

http://static.googleusercontent.com/media/www.google.com/en/us/intl/en/doubleclick/pdfs/Criteo-and-DoubleClick-Ad-Exchange-Case-Study-6-1-2011.pdf (viewed 2 June 2014).

[9] "Criteo Retargeting Company," FindTheBest, http://retargeting-companies.findthebest.com/q/14/11641/What-ad-exchanges-are-integrated-with-Criteo-Retargeting-Company (viewed 14 July 2014).

[10] Google, "Criteo Gains Great Results and Scale by Retargeting Audiences through Real-time Bidding with DoubleClick Ad Exchange."

[11] Criteo, "The Smart CMO's Survival Handbook for Data-driven Advertising," http://www.criteo.com/us/research/all-the-papers/download/1821 (viewed 2 June 2014).

[12] AdQuantic, the French ad-tech company, "has developed a bid management tool for search marketing based on game theory, quantum physics and related mathematical models."Ingrid Lunden, "Criteo Buys AdQuantic, A Startup That Applies Quantum Physics To Search Marketing," TechCrunch, 10 Apr. 2014, http://techcrunch.com/2014/04/10/criteo-buys-adquantic/ (viewed 2 June 2014).

Datalogix

Complaint number	11
Company profile	Datalogix provides digital profiling and consumer tracking services to companies engaged in online advertising by connecting that advertising to offline sales data from loyalty cards and other records.
Main website	www.datalogix.com/
Safe Harbor/privacy statements	Datalogix's eight-word declaration concerning the "Personal Information Received from the EU/EEA and/or Switzerland" reflects the disregard that it has for the U.S.-EU Safe Harbor Framework. Most companies manage to couch their statements in full sentences, but Datalogix's telegrammatical declaration—"Commercial purposes related to advertising and associated services"—underscores the contrast that exists between statements to DOC deemed sufficient for the Safe Harbor and marketing bravado elsewhere.[1] Its corporate privacy policy is more forthcoming, especially with regard to the collection and processing of personally identifiable information. Thus in addition to its Safe Harbor endorsement ("Datalogix follows the Safe Harbor Principles published by the U.S. Department of Commerce with respect to the transfer of personal information from the European Union to the U.S., and has certified to the U.S. Department of Commerce its adherence with the Safe Harbor Framework."), Datalogix's privacy policy includes the following information: Datalogix receives data from consumer marketing companies & data compilers. This data consists of Personally Identifiable Information ("PII") and Attributes. PII includes name, postal address, and email address. Attributes include demographic and behavioral information, such as past purchases. … Datalogix does not transfer data identified with residents of the EU to unrelated third parties, except in accordance with the Safe Harbor Privacy Framework. In the event that Datalogix ever needs to transfer data to an unrelated third party, Datalogix will ensure that such party is either subject to the Safe Harbor Agreement, subject to similar laws providing an adequate and equivalent level of privacy protection, or will enter into a written agreement with the third party requiring them to provide protections consistent with the Safe

	Harbor Privacy Framework and this policy. Datalogix may share data as described below: Agents and service providers. Datalogix may share data, including PII, with agents and service providers who work on behalf of or with us to provide some aspects of our services including, for analytical purposes, to measure current campaigns or to inform future campaigns. These agents and service providers do not have an independent right to use or share this information. Partners. Datalogix may share data, including PII, with partners to help provide more tailored advertising and for analytical purposes. Datalogix does not share PII with our Digital Ad Serving partners (an entity without consumer relationships that serves advertising on the websites of others). Corporate transfers. If Datalogix is purchased, or assets related to Datalogix are purchased, Datalogix and any data associated with our advertising and measurement products will be transferred. Affiliates. Although Datalogix currently does not have a parent company, any subsidiaries, joint ventures, or other companies under common control (collectively, "Affiliates"), we may in the future. Datalogix may share some or all of the information in our possession including PII and non-PII with these Affiliates.[2] Datalogix also offers users a cookie-based mechanism "to opt out of Datalogix cookie-based digital online advertising. If you elect to opt out, we will set an Ignore Flag that indicates that you have opted out."[3] In a separate privacy document concerning its use of cookies the company constrains its policy to one venue where EU consumers are least likely to encounter Datalogix cookies, explaining that "The Datalogix website uses Google Analytics and Webtrends cookies to collect information about how the website is used, including details of the site where the visitor has come from and the total number of times a visitor has been to this website. Datalogix uses this information to improve the website and enhance the visitor experience."[4]
Non-compliance/	In its product literature the company offers revealing

false claims	details about the power of its technology, which enables "… brands to reach their customers anywhere online across display, video, mobile and social … ," using applications that are "… integrated with virtually every major media company, including publishers, portals, exchanges, [and] ad networks."[5] Datalogix works with such data-driven partners as AppNexus, BlueKai, Criteo, DataXu, Facebook, and Google to compile fine-grained dossiers on individual consumers.[6] "With Datalogix's solution, offline transaction data is overlaid with demographic and other data types from various third-party sources to add value to the customer."[7] Datalogix also plies its profiling trade in various social media outlets, including Facebook and Twitter, giving its clients the ability "… to create Facebook digital audiences from their own offline customer files using DLX OnRamp."[8] The company, "a source for real-world data for online targeting," uses "tens of millions of … Affiniti Cookies to support online targeting."[9] "DataLogix' audience platform is powered by a database with over $1 trillion dollars in consumer spending behavior."[10] "Available data spans hundreds of product categories and a host of recency, frequency and monetary value data elements."[11] DataLogix promises it can "can apply almost any 'real-world' or offline data set to the tens of millions" of what it calls its own brand of "anonymous cookies."[12] In a variety of online contexts, then, and with offline data as part of its digital profiling arsenal, Datalogix tracks consumers with great precision.
FTC action on possible violations	Datalogix's brief disclosure about sharing unspecified PII with partners but not Digital Ad Serving Partners is not sufficient to inform EU consumers about the uses of their personal information and to thereby satisfy the Notice and Choice requirements of the Safe Harbor. Although the company claims to make some steps towards Onward Transfer compliance, without sufficient disclosures to satisfy Notice, EU consumers do not know what data is being collected or how it is being used or shared—Onward Transfer safeguards are necessary but not sufficient to satisfy Safe Harbor commitments. FTC should investigate this company's failure to give proper Notice to EU consumers concerning the extent of its data-mining and personalized profiling practices. Since Datalogix is clearly transferring personal information to third parties FTC should also investigate whether the company has violated

	its duty to provide sufficiently effective opt-in mechanisms for sensitive information and opt-out Choice for less sensitive information.

[1] Datalogix, Safe Harbor Organization Information, expires 1/14/15, http://safeharbor.export.gov/companyinfo.aspx?id=21548 (viewed 18 May 2014).

[2] Datalogix, "Privacy," https://www.datalogix.com/privacy/ (viewed 21 May 2014).

[3] Datalogix, "Privacy." A separate "Datalogix UK Privacy Policy" requires users to submit their name and address in order to "opt out of all DLX-enabled advertising." Datalogix, "Datalogix UK Privacy Policy," http://eu.datalogix.com/uk-privacy/ (viewed 11 June 2014).

[4] Datalogix, "Cookies," http://www.datalogix.com/privacy/cookie-policy/ (viewed 11 June 2014).

[5] Datalogix's "media partners" include 4info, AdapTV, AdMobius, AOL, AppNexus, Audience Science, BlueKai, Brand.net, BrightRoll, Cadreon, Conversant, Criteo, DataXu, Digilant, Drawbridge, eBay, eXelate, Facebook, Google, JumpStart, Legolas, Lotame, Millennial Media, MediaMath, NetMining, Pandora, PlaceIQ, Rocket Fuel, Specific Media, SpotXchange, Tapad, Tremor Video, Tribal Fusion, Twitter, Tube Mogul, Turn, Undertone, Videology, Vivaki, x+1, Xaxis, Yahoo, and YuMe. Datalogix, "Digital Media," http://www.datalogix.com/digital-media/ (viewed 4 May 2014).

[6] Datalogix, "Digital Media."

[7] IBM Software, "Datalogix: Using IBM Netezza Data Warehouse Appliances to Drive Online Sales with Offline Data," http://public.dhe.ibm.com/common/ssi/ecm/en/imc14697usen/IMC14697USEN.PDF (viewed 4 May 2014).

[8] "Datalogix Announces Facebook Partner Categories for CPG, Retail and Automotive Brands," 10 Apr. 2013, http://www.datalogix.com/2013/04/datalogix-announces-facebook-partner-categories-for-cpg-retail-and-automotive-brands/ (viewed 2 June 2014).

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

[10] Datalogix, "Datalogix 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).

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

[12] Datalogix, "DLX Platform," http://affiniti.datalogix.com/index.php?id=6 (viewed 1 Apr. 2010).

DataXu

Complaint number	12
Company profile	DataXu is a data analytics and digital profiling company that identifies and tracks individual consumers across multiple platforms and devices, online and off. The company developed "the only real-time multivariate decision system that learns how consumers engage across channels" and extended its "platform to optimize media investments in real time based on consumer sentiment."[1]
Main website	www.dataxu.com/
Safe Harbor/privacy statements	DataXu's Safe Harbor statement outlines the company's "Data Collection for our Platform: We may collect information such as your browser type (e.g., Firefox or Internet Explorer), operating system (e.g., Macintosh or Windows), Internet provider (e.g., Verizon or Comcast), IP address, and whether you respond to an ad. We do not collect your name, address, phone number, e-mail address, Social Security Number, credit card information, insurance plan numbers, financial account numbers, or health related information. We use two technologies to collect information, both of which are widely used on the Internet: cookies and pixel tags. The information that we collect via our technologies is used for the purpose of targeting ads, measuring the effectiveness of ads on behalf of DataXu's advertisers and to identify the audience most likely to respond to an advertisement. This information also helps DataXu ensure that you don't repeatedly see the same ad. We may also use non-PII data from third parties. We retain the information collected via our technology for up to 13 months. After that time, we aggregate the data and retain it for analytical purposes.[2] DataXu's corporate privacy policy simply explains that it "… complies with the U.S. – E.U. Safe Harbor framework and the U.S. – Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland," and "… adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[3] That statement also explains, however, that "Your personal information, including your name and e-mail address, may

	be shared with authorized companies that provide services to help us with our business activities, such as facilitating our marketing efforts … .”[4] The company has an additional privacy statement that describes … how DataXu collects and uses the information we obtain from third party websites via our technologies. It also describes the choices available to you regarding our use of your information and how you can opt-out of having your information collected. … We do not collect information generally considered Personally Identifiable Information (PII) such as your name, address, phone number, e-mail address, Social Security Number, credit card information, insurance plan numbers, financial account numbers, or health related information. We collect IP address to provide more relevant content based on your region, which may be classified as PII in some jurisdictions. … We use two technologies to collect information, both of which are widely used on the Internet: cookies and pixel tags. The information that we collect via our technologies is used for the purpose of targeting ads, measuring the effectiveness of ads on behalf of DataXu’s advertisers and to identify the audience most likely to respond to an advertisement. This information also helps DataXu ensure that you don’t repeatedly see the same ad. We may also use non-PII data from third parties. … There are two ways you can opt-out of DataXu ad optimization. • Block all cookies by disabling cookie use in your browser. This may cause some sites to work incorrectly. • Opt out by setting a cookie which tells the DataXu system to ignore you and not display targeted ads. Please note that you will continue to see generic advertising. … We may transmit or share our data with third-party service providers (e.g., data storage and processing facilities) in order for those service providers to perform business functions for us or on our behalf. We may share the information we collect to do business with related, authorized third parties, such as our

	advertising clients.[5] Both privacy statements include a link to a third-party site, Ghostery, that allows users to manage the tracking cookies that appear on their browsers, including DataXu's cookies.[6]
Non-compliance/ false claims	DataXu's product descriptions are rife with examples of data mining and personalized advertising practices that are not evident in its Safe Harbor-compliance disclosures. Combining extensive data collection with detailed analytics, DataXu captures "… vast amounts of real time digital signals as they move from site to site, device to device and location to location."[7] The company promises to "… deliver a consistent and effective brand message at every touchpoint as consumers move from digital to physical and across multiple devices. We designed DataXu from the ground up to track and optimize the full customer journey" leveraging display, video, mobile, Facebook Exchange and other platforms to reach specific consumers with individually tailored advertising.[8] DataXu's Customer Intelligence product draws on consumer behavioral data to create detailed profiles of individuals, while its Customer Engagement product exploits that data to create personalized marketing messages for specific consumers.[9] DataXu's technology, moreover, grows more precise with each ad campaign, using "… data from previous campaigns to inform each new decision, making the system smarter with each individual interaction. Offline and website data can be included in this continuous learning cycle, producing better decisions and improving ROI, automatically."[10] This re-use and amalgamation of personal information makes DataXu a controller within the Safe Harbor and EU law.
FTC action on possible violations	Because of its failure to provide adequate Notice concerning its data mining and personalized profiling practices, FTC should investigate DataXu's Safe Harbor compliance. The company's disclosures suggests that because it does not collect some personal information it is not violating the privacy rights of EU consumers, but it can be seen that DataXu knowingly collects offline data, IP addresses, and cookies/pixel tags that are identifiable according to EU law. It then uses these technologies for behavioral targeting that goes well beyond its disclosures on use of personal information. Also, the company's policies are self-contradictory: though it says it does not collect name and contact information, it reserves the right

	to share those details about a user with others. This would tend to mislead consumers and understates what the company does with its tracking technologies. FTC should also investigate the company's opt-out mechanisms to see if they are conspicuous and effective enough to satisfy Safe Harbor commitments.

[1] DataXu, "About Us: Vision," http://www.dataxu.com/about-us/vision/ (viewed 15 July 2014).

[2] DataXu, Safe Harbor Organization Information, expires 8/8/15, http://safeharbor.export.gov/companyinfo.aspx?id=24045 (viewed 26 May 2014).

[3] DataXu, "Privacy Policy for our Corporate Site," http://www.dataxu.com/about-us/privacy/privacy-policy-corporate-site/ (viewed 21 May 2014).

[4] DataXu, "Privacy Policy for our Corporate Site."

[5] DataXu, "Data Collection for our Platform," http://www.dataxu.com/about-us/privacy/data-collection-platform/ (viewed 21 May 2014).

[6] Evidon, "Ghostery Enterprise," http://info.evidon.com/more_info/ (viewed 13 June 2014).

[7] DataXu, "The DataXu Platform," http://www.dataxu.com/platform/what-is-dataxu/ (viewed 26 May 2014).

[8] DataXu, "The DataXu Difference," http://www.dataxu.com/platform/benefits/ (viewed 26 May 2014).

[9] DataXu, "The DataXu Platform."

[10] DataXu, "Technology: The Science and Technology Behind Programmatic Marketing," http://www.dataxu.com/platform/technology/ (viewed 26 May 2014).

EveryScreen Media

Complaint number	13
Company profile	EveryScreen Media provides real-time bidding and other advertising services to mobile marketing companies, including extensive data profiling and location-based consumer tracking.
Main website	www.everyscreenmedia.com/
Safe Harbor/privacy statements	EveryScreen Media's one-sentence Safe Harbor declaration—"Receipt of anonymous user activity on publisher sites as sent by mobile supply side platforms used within a mobile real time exchange bidding environment for advertisers, agencies and demand side platforms to reach advertising audience segments"—belies both the intricacy and the sheer range of the company's data-driven technology.[1] Nor does the company's privacy policy (under a new corporate name that it apparently hasn't registered with the Department of Commerce) disclose such details: "Dstillery complies with the US-EU Safe Harbor Framework and US-Swiss Safe Harbor Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. Dstillery has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[2] The company does not offer an opt-out mechanism for its various data-collection and usage practices, which it describes in the following manner: Dstillery data is sourced from leading supply-side platform partners, publishers, advertisers, and third party data providers. The data that we use are anonymous elements of information which allow us to provide reach and relevant audience to our clients. We do not collect or use Personally Identifiable Information (PII) such as your name, address, phone number, email address in connection with our Services. … We combine location data with other data signals, including third party and client-owned data, to create non-personally identifiable cohort audience segments. These audience cohort segments allow us to expand reach by finding similar users with the same likes and

	dislikes. … We also may collect personally identifying information (PII) that can be used to identify you. We only collect Personally Identifiable Information when you specifically provide it to us. For example, in connection with your use of certain features of the website you may be asked to create a user account and provide certain information including your name, email addresses, address, and telephone number. We may use PII to fulfil your requests and respond to your inquiries. We do not sell PII or other information you make available to the website, or share such information with any third parties.[3]
Non-compliance/ false claims	EveryScreen Media's product literature, in contrast, explains that the company "… provides real-time bidding and data science technology for leading mobile marketing companies."[4] Zeroing in on specific individuals and tracking them using "… location with other data signals, including third party and client-owned data …. ."[5] Additionally, EveryScreen Media works "… with third party data partners to bring in niche data … for additional audience identification. We have partnered with several companies that have unique local, social and mobile data."[6] EveryScreen Media's approach to mobile targeting should raise Safe Harbor-compliance concerns, combining as it does location and device data tied to a profile—which amounts to the collection and use of personal information identifiable to a single consumer by harnessing "… a combination of data sources—yours, ours and others. … We listen to billions of impressions, classifying each piece of associated data received from our supply partners. This data includes geo-location, timestamp, device and context"[7] The company's prowess in mining mobile data, finally, now includes " … the ability to track important post-click actions that occur after an ad is served."[8] Ranging from "… a purchase, a form completion, an app download, or some other event of significance to the advertiser," these "conversion events" captured by EveryScreen Media without the mobile user's knowledge or consent are further evidence of the company's failure to comply with Safe Harbor.
FTC action on	FTC should investigate EveryScreen Media's Safe Harbor status in light of the privacy threats posed by its targeted

possible violations	mobile advertising practices and data-mining partnerships. A privacy policy that says that the company never collects PII misleads EU consumers whose understanding of "personal information" includes the identifiable information (including and linked to the consumers' location at all times) this company routinely amasses on them. Offering no opt-in or opt-out mechanism to comply with Choice potentially flies in the face of compliance with Safe Harbor. This company is collecting, and likely sharing, highly sensitive location and device-use data that is identified or identifiable to individual EU consumers, which requires full Notice and consent. EveryScreen/Dstillery does not seem to take this personal information seriously or treat it as such.

[1] EveryScreen Media, Safe Harbor Organization Information, expires 6/19/14, http://safeharbor.export.gov/companyinfo.aspx?id=19109 (viewed 5 May 2014).

[2] Dstillery, "Privacy Policy [Effective: December 07, 2012]," http://www.everyscreenmedia.com/privacy/ (viewed 21 May 2014).

[3] Dstillery, "Privacy Policy."

[4] EveryScreen Media, "Company Overview," http://www.everyscreenmedia.com/company/overview/ (viewed 5 May 2014).

[5] EveryScreen Media, "Using Data Science to Find the Right Person at the Right Place," http://www.everyscreenmedia.com/data-science/overview/ (viewed 2 June 2014).

[6] EveryScreen Media, "Data Management Platform: Overview."

[7] EveryScreen Media, "Data Management Platform: Overview," http://www.everyscreenmedia.com/products/data-management-platform/overview/ (viewed 5 May 2014).

[8] EveryScreen Media, "Conversion Tracking," http://www.everyscreenmedia.com/products/houston-real-time-bidding-platform/conversion-tracking/ (viewed 5 May 2014)

ExactTarget

Complaint number	14
Company profile	ExactTarget is a provider of digital marketing automation and analytics software and services, including data profiling and online tracking of individual consumers.
Main website	www.exacttarget.com/
Safe Harbor/privacy statements	ExactTarget (which was acquired by Salesforce three months before its most recent certification in November 2013) claims in its Safe Harbor statement to provide an "opt-in" email targeting service:[1] "ExactTarget provides online software tools for our clients who communicate via email and other electronic means to customers and prospects that have opted in to receive their electronic communications."[2] And although the link that it provides to its privacy policy directs visitors to a page that is bereft of any mention of Safe Harbor, the "Salesforce.com ExactTarget Marketing Cloud Website Privacy Statement" does include a Safe Harbor section: "In connection with the Services branded as 'Buddy Media' and 'ExactTarget', salesforce.com complies with the U.S.- E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from the European Union member countries and Switzerland. Salesforce.com has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[3] While this privacy statement pertains mainly to Salesforce customers who visit its corporate site (i.e., representatives of companies that avail themselves of one or more Salesforce products or services), the company's "Indexed Content Privacy Statement" is much more pertinent to EU consumers: This Indexed Content Privacy Statement describes salesforce.com's privacy practices relating to content that has been made publicly available on the Internet and that is accessed, used and maintained in connection with the provision of the Services (the "Indexed Content"). … The Services provide platforms and online tools that allow Customers to: (i) monitor, access, and manage Indexed Content relating to their businesses, brands, activities and industries; (ii) engage in online

	conversations with individuals posting Indexed Content on the Internet; (iii) analyze trends in Indexed Content, such as sentiment and volume; and (iv) measure engagement with, and performance of, Indexed Content posted by Customers. The use of information collected through our online tools shall be limited to the purpose of providing the Services to our Customers. … To provide the Services to our Customers, the Company collects Indexed Content from a variety of publicly-available portions of Web sites, such as blogs, news Web sites, and social networking Web sites, which may include third party personally identifiable information. In general, anyone can find the Indexed Content via a standard Internet search engine or by visiting applicable Web sites themselves. The Company has no ownership rights in the Indexed Content or any direct relationship with individuals whose personally identifiable information may be processed as part of providing the Services. The Company obtains Indexed Content using proprietary Web crawler technology, via public APIs, or through agreements with Web site operators or other third party providers. The Company also may obtain Indexed Content directly from Customers' social networking Web sites upon their request and in accordance with the authentication process established by such social networking Web sites. … Examples of the types of Indexed Content the Company collects and maintains include: (i) publicly available content based on search queries from our Customers, including the source of any such information; (ii) public content available on Customers social networking Web sites and accounts; and (iii) publicly available metrics relating to the public content retrieved from the Internet such as number of comments, number of unique individuals commenting, number of Likes and number of followers. … Customers are responsible for their use of Indexed Content. Salesforce.com requires Customers to use Indexed Content in accordance with the Company's Terms of Service or other applicable agreement between the parties, the terms of service of the applicable Web site from which the Indexed Content is obtained or derived, and applicable law.

	… The Services allow Customers to monitor individuals who interact with the Indexed Content posted by Customers to their own Web sites or to third party social networking Web sites. This may include tracking a user who shares or clicks on a link to a Customer's Web site or advertisement in order to determine whether such action resulted in the individual purchasing a Customer's product or otherwise engaging with the Customer's Web site. Customers are responsible for complying with any legal requirements in using functionality that allows tracking of individuals. … If you wish to access, correct, amend or delete any personal information pertaining to you which is held by any of our Customers, or opt out of communications from any such Customers, you should direct your query directly to the applicable Customer. We will acknowledge Customer requests to update or remove any Indexed Content pertaining to you from our Services, where the Customer has no ability to do so via use of the Services, within thirty (30) days.[4]
Non-compliance/ false claims	The company fails to meet the Framework's Notice and Choice requirements, however, neither fully disclosing the extensive nature of its consumer-tracking and ad-targeting practices (both alone and in combination with Salesforce), nor providing a means for EU consumers (i.e., its clients' customers) to exclude themselves from these practices. ExactTarget's marketing materials on its corporate website provide ample evidence of the company's tracking and targeting activities that contrast sharply with its modest Safe Harbor disclosure. By its own admission, ExactTarget tracks individuals as they engage in a number of online activities, monitoring and analysing "… customer journeys across every touchpoint—email, mobile, social, web, and beyond—helping marketers put customers at the center of everything they do."[5] The personal data that it collects, moreover, is used "… to deliver customized content across all … marketing channels." By using "… customer behavior and preferences to create unique, personalized experiences," collecting "… real-time information about customer activities" and consolidating data from multiple sources for a deeper understanding of customer attributes and behaviors," ExactTarget builds a detailed "… 360° profile incorporating any type of interactions or behavior data—including point of sale, web analytics, real-time

	events, and more."[6] As ExactTarget points out, "Mobile web traffic now accounts for nearly 30% of all web viewing. And since mobile devices don't use cookies … ." The company's solution to this problem, combining "… ExactTarget Marketing Cloud customer and interaction data" with "… the incredible targeting data at your disposal in social media," may prove a profitable business strategy, but it represents yet another assault on EU consumer privacy.[7]
FTC action on possible violations	Until such time that ExactTarget can clear up the uncertainty surrounding the precise nature of its own ad-targeting practices—and the impact on those practices of its acquisition by Salesforce—the company's Safe Harbor status is questionable and should be investigated by FTC. Consumers would not likely know that limited email contact with a retailer would open them up to "360° profil[ing]" across all their web-enabled devices, creating large data sets of personal information that might be shared with third parties. Furthermore, disclaiming all responsibility for "Indexed Content" has no bearing on ExactTarget's liability as a controller for processing personal information of EU consumers. Its practices of "[c]onsolidat[ing] data from multiple sources for a deeper understanding of customer attributes and behaviors" are far beyond the minimum requirements for being deemed a controller, and ExactTarget's disclaimer has no effect on the disclosure, access, and opt-out duties that Safe Harbor requires. The depth of consumer tracking the company claims to perform, in short, goes well beyond the limited opt-in communications it purports to restrict itself to in its Safe Harbor disclosure.

[1] "Salesforce.com Completes Acquisition of ExactTarget," 12 July 2013, http://www.salesforce.com/company/news-press/press-releases/2013/07/130712.jsp (viewed 25 May 2014).

[2] ExactTarget, Safe Harbor Organization Information, expires 11/2/14, http://safeharbor.export.gov/companyinfo.aspx?id=20658 (viewed 6 May 2014).

[3] ExactTarget, "Privacy Policy," http://www.exacttarget.com/privacy-policy (viewed 14 May 2014); Salesforce, "Salesforce.com ExactTarget Marketing Cloud Website Privacy Statement," http://www.exacttarget.com/privacy-policy/website-privacy-statement (viewed 21 May 2014).

[4] ExactTarget, "Salesforce.com Marketing Cloud Indexed Content Privacy Statement," http://www.exacttarget.com/privacy-policy/indexed-content-privacy-statement (viewed 13 July 2014).

[5] ExactTarget, "Company," http://www.exacttarget.com/company (viewed 6 May 2014).

[6] Salesforce, "ExactTarget Marketing Cloud," http://www.exacttarget.com/marketing-cloud-product-showcase (registration required).

[7] ExactTarget, "Ads: Overview," http://www.exacttarget.com/products/ads (viewed 6 May 2014).

Gigya

Complaint number	15
Company profile	Gigya provides social media services to website operators, covering log-in and registration procedures, user-identity storage, gamification tools (i.e., advertisements appearing as games), and other technology to create detailed user profiles and consumer tracking systems on various social networks.
Main website	www.gigya.com/
Safe Harbor/privacy statements	Although Gigya admits in its Safe Harbor statement that it "…may access personal information about Gigya's customers' consumers in the EU and Switzerland," it also explains that "Gigya acts as a data processor on behalf of its customers with respect to such consumer data and accordingly only carries out the instructions of such customers with regard to the collection, processing, and protection of such consumer data."[1] In addition to the standard endorsement of Safe Harbor ("Gigya is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and (1) the European Union and (2) Switzerland, respectively. We have certified that we adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and (1) the E.U. and (2) Switzerland, respectively"), the company's privacy policy also includes the following two caveats for "International Users": A. On the Gigya Website The Gigya Website is hosted in the United States. If you use the Gigya Website from the European Union, or any other region with laws governing data collection and use that may differ from United States law, please note that you are transferring your personal data outside of those jurisdictions to the United States. The United States does not have the same data protection laws as the European Union and other regions. By providing Personal Information under this Privacy Policy, you consent to the use of Personal Information in accordance with this Privacy Policy and the transfer of your Personal Information to the United States. B. Through the Gigya Services The Gigya Platform is hosted in the United States. In addition, Gigya offers a European Union-based Data Center for EU-based customers subject to such

	restrictions as indicated above ("EU Data Center"). The EU Data Center will house the Identity Storage and Data Store for Client's that elect this option. The Gigya Platform will make calls to the EU Data Center. If you are an End User of a Client utilizing the Gigya technology, be sure to check that website's Privacy Policy in order to confirm whether the EU Data Center is being utilized.[2] Additionally, Gigya's privacy policy offers the following options, under its "Your Choices" section, for those encountering Gigya's services on a client's website: If you are an End User registered on a Client's website using Gigya's technology to power its Social Components and you want to edit or delete any information captured about you on that Client's website, you should contact the website owner directly. We have provided tools for our Clients using Gigya's Identity Storage to allow the Client to implement a profile screen on their website that gives End Users the option to edit, delete, and download their information. It is up to each individual Client to utilize these tools. Through our Social Compliance™ service, used in connection with Gigya's Identity Storage, Gigya will delete any non-public Facebook profile information if a user revokes permissions from the Client's application to which those permissions were previously granted. If you are an End User registered on a Client's website using the Gamification component specifically, you have additional privacy settings you may access directly, in the event you do not want your profile and ranking to be displayed to other users on the website via the Leaderboard plugin. These settings are available in the "User Status" Social Plugin.[3] If you would like to opt out of having your image or name displayed publicly to other users of a Client's website, you should contact that website's owner directly.
Non-compliance/ false claims	The above statements and disclaimers of liability fall short of providing adequate Notice and Choice to consumers, and those about U.S. law and the EU Data Center seem to be aimed at Gigya's corporate customers, not the End User consumers whose information is being used. The Safe Harbor requirements are not met in Gigya's Safe Harbor or

	privacy policy statements, both of which lack details about the company's consumer profiling and targeting practices, which the company willingly shares with its own corporate clients. Claiming to reach 1.5 billion unique users per month through its work with some 700 corporate customers. Gigya promises to "[h]arness identity and behavior data to power data-driven marketing" by collecting "… valuable identity and behavior data in one place with a next-generation database designed to store data streams from social network profiles and user activities across multiple devices." [4] Gigya's Rachel Serpa discusses her company's approach to social marketing on the Gigya blog: "As consumers interact and share information about themselves across social networks and other channels, huge quantities of structured data (email, gender, birthdays, etc.) and unstructured data (interests, web actions, etc.) are created. Successful brands pay close attention to these psychographic and demographic signals to reach consumers with highly relevant messages at prime points of influence."[5] The company also employs manipulative "gamification" strategies, in which marketing messages are disguised as games in order to "[d]rive valuable user actions" (such as spending additional time being exposed to advertising, and surrendering additional behavioral data in the process).[6] And whether they realize it or not, when users avail themselves of Gigya's Social Login service (which gives users the option of linking an existing site account with one or more social accounts), they are also giving marketers "… permission to access rich, first-party social data. Detailed profile information such as interests, demographics, education, social connections, work history, and more can easily be stored" in a company's database, "… or automatically stored via Identity Storage—Gigya's dynamic, cloud-hosted database."[7] Either way, the consumer's privacy is compromised.
FTC action on possible violations	FTC should investigate Gigya in light of the clear discrepancy between its Safe Harbor and privacy policy statements and the detailed, data-driven targeted advertising that it actively undertakes. It seems that this company exercises control over the means of processing personal information, making it a controller under the Safe Harbor. As a controller it cannot only provide opt-out Choice to EU consumers when its clients choose to use its

	opt-out tools. Its disclosures fall short of informing consumers that their social network information is repeatedly being scraped and their actions are being manipulated by gamification, all to the benefit of marketers who are collecting personal information about them.

[1] Gigya, Safe Harbor Organization Information, expires 12/1/14, http://safeharbor.export.gov/companyinfo.aspx?id=20991 (viewed 6 May 2014).

[2] Gigya, "Privacy Policy," http://www.gigya.com/privacy-policy/ (viewed 21 May 2014).

[3] Gigya, "Privacy Policy."

[4] Gigya, "Collect Overview," http://www.gigya.com/collect/; Gigya, "About Us," http://www.gigya.com/company/ (both viewed 6 May 2014).

[5] Rachel Serpa, "How to Harness Social Data to Establish Consumer Relationships," Gigya Blog, http://blog.gigya.com/how-to-harness-social-data-to-establish-consumer-relationships/ (viewed 15 July 2014).

[6] Gigya, "Convert Overview," http://www.gigya.com/convert/ (viewed 6 May 2014).

[7] Gigya, "Social Login," http://www.gigya.com/social-login/ (viewed 6 May 2014).

HasOffers

Complaint number	16
Company profile	HasOffers specializes in advertising attribution analytics for both desktop and mobile platforms. (On 17 July 2014, HasOffers announced that it had changed its name to Tune.)[1]
Main website	www.hasoffers.com/
Safe Harbor/privacy statements	HasOffers' statement on file with the Department of Commerce explains that the company "… provide[s] our customers with online advertising technology that tracks end-user impression, click, and conversion data and helps customers evaluate the effectiveness of their ad campaigns. For our customers located in EU/EEA and/or Switzerland we process and manage account data, including customer and employee names, information about advertising campaigns, publisher names, and advertiser records."[2] While purportedly demonstrating its compliance with the U.S.-EU Safe Harbor Framework, HasOffers' Safe Harbor declaration offers no indication whatsoever of the inner workings of the company's mobile app tracking system—which it describes elsewhere as "the industry standard platform for mobile app marketers which unbiasly [sic] attributes app installs, in-app engagement, and purchases back to marketing sources (such as social networks, publishers, and mobile ad networks)"—nor of the privacy threats inherent in that system.[3] HasOffers' privacy statement is equally uninformative in this regard: "HasOffers complies with the U.S. – E.U. Safe Harbor framework and the U.S. – Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. HasOffers has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[4] Concerning the personal information that it collects, HasOffers' privacy policy notes, "We collect personally identifiable information on the Site when you attempt to become a Subscriber or otherwise choose to provide personally identifiable information to us. Personally identifiable information is any information that can be used to identify or locate a particular person or entity. This may include, but is not limited to: name, business entity name

	and/or your title with the applicable business entity, as well as your personal and/or business entity related e-mail address, mailing address, daytime and/or cellular telephone numbers, fax number, credit card and/or any other information requested on the applicable Subscriber registration form."[5] This policy also explains the company's use of cookies ("You cannot use this site or the Services without agreeing to accept the cookies that we use with the Site"), as well as providing a means to opt out of both targeted advertising (via AdRoll) and company emails.[6]
Non-compliance/ false claims	HasOffers' questionable mobile tracking practices came to light earlier this year when Facebook abruptly removed the company from its Mobile Measurement Partner (MMP) program.[7] This incident in itself, in light of HasOffers' continued participation in the Safe Harbor framework, warrants scrutiny from the FTC. For although HasOffers CEO Peter Hamilton may claim otherwise ("I want to be clear that we did not violate any privacy regulations, and there was no data leakage or inappropriate data provided to advertisers," he stated on 13 February 2014), subsequent coverage in the trade press suggests a potentially major—if largely hidden—privacy breach.[8] "In an email to customers obtained by VentureBeat last fall," as Ad Exchanger's Zach Rogers explains, "HasOffers CEO Peter Hamilton described how the company "inappropriately" let its customers access device-level performance and attribution data. That violation—helping app owners obtain user-level, albeit anonymous, data—would be significantly more serious than the official reasons given for its expulsion."[9] Even in the absence of its Facebook violation, HasOffers' mobile tracking practices warrant scrutiny from the FTC, such as its "Advanced Mobile Targeting" product, which "… allows ad networks, agencies, and advertisers to create highly specific rules to target and optimize campaigns for preferred audiences and user experiences. … Advanced mobile targeting can be as simple as choosing which browsers or operating systems to target, or as fine-grained as only accepting clicks with specific sub-ids passed in."[10] HasOffers' highly granular approach to user profiling, down to the level of specifying individual consumers for tracking and targeting on both desktop and mobile platforms, raises concerns about the company's Safe Harbor certification.
FTC action on	While Facebook is to be commended for its decisive action

possible violations	to affirm its data-handling standards among its partners, this does not relieve FTC's obligation to examine HasOffers' Safe Harbor status in light of its MMP expulsion. Indeed, if industry's oft-touted self-regulatory privacy practices are to mean anything at all, HasOffers itself should have filed a full explanation of the Facebook incident with the Department of Commerce well in advance of its 14 May 2014 re-certification deadline. In the absence of such documentation, FTC should investigate this company for its targeting and profiling of individuals and sharing of their data with third parties without Notice or Choice. HasOffers' privacy policy seems to cover only data collection on its own site, providing EU consumers with no Notice of its data collection and use elsewhere.

[1] Peter Hamilton, "The Search for TUNE," Tune Blog, 17 July 2014, http://www.tune.com/blog/introducing-tune/ (viewed 12 Aug. 2014).

[2] HasOffers, Safe Harbor Organization Information, expires 5/14/15, http://safeharbor.export.gov/companyinfo.aspx?id=22730 (viewed 25 May 2014).

[3] HasOffers, "About HasOffers," http://www.hasoffers.com/about/ (viewed 25 May 2014).

[4] HasOffers, "Privacy Policy," http://www.hasoffers.com/privacy-policy/ (viewed 21 May 2014).

[5] HasOffers, "Privacy Policy."

[6] AdRoll, "AdRoll's Privacy Policy," https://www.adroll.com/about/privacy (viewed 16 June 2014).

[7] Kontagent was also removed from the Facebook's MMP program. The two companies, according to a report in Ad Exchanger, "violated their agreements with Facebook, including holding onto data longer than their contracts allowed and failing to require their advertisers—app developers—to notify users of data collection through updates to their privacy policies." Zach Rogers, "Facebook Drops Two Mobile Ad Partners For Keeping Data Too Long," Ad Exchanger, 12 Feb. 2014, http://www.adexchanger.com/data-exchanges/facebook-drops-two-mobile-ad-partners-for-keeping-data-too-long/ (viewed 7 May 2014).

[8] Peter Hamilton, "Facebook Attribution for MobileAppTracking," HasOffers Performance Marketing Blog, 13 Feb. 2014, http://www.hasoffers.com/blog/facebook-attribution-mat/ (viewed 7 May 2014).

[9] Zach Rogers, "How Facebook's Expulsion Of HasOffers Went Down," Ad Exchanger, 18 Feb. 2014, http://www.adexchanger.com/mobile/how-facebooks-expulsion-of-hasoffers-went-down/ (viewed 7 May 2014).

[10] HasOffers, "HasOffers Launches Advanced Mobile Targeting," 10 Sept. 2013, http://www.hasoffers.com/news/hasoffers-launches-advanced-mobile-targeting/ (viewed 3 June 2014).

Jumptap

Complaint number	17
Company profile	Jumptap is a mobile ad network specializing in targeted advertising applications and services, including detailed consumer profiling and personalized marketing practices.
Main website	www.jumptap.com
Safe Harbor/privacy statements	Jumptap admits in its Safe Harbor declaration that it uses a range of consumer information in its targeting efforts, including "information collected by our partners and shared with us to improve the relevance of ads," and "data from third party business partners."[1] It also claims that its "system does not store explicit personal data that would enable you to be identified in real life," while its privacy policy simply states that "Millennial Media's Jumptap subsidiary adheres to the Safe Harbor Privacy Principles developed by the U.S. Department of Commerce and the European Union (EU), as well as the U.S-Swiss Safe Harbor, and has Safe Harbor self-assessment procedures in place."[2] That privacy policy also includes the following statements concerning Jumptap's collection and use of consumer data: Millennial Media collects data from across our Platform. This data, which may include anonymous identifiers associated with your mobile device and the location of your device, does not identify you personally, and may come from such sources like your mobile web browser, or the apps that you use. We use a variety of technologies to collect this data, including "cookies" … . Millennial Media's affiliated entities covered by this policy may share data with each other or with other affiliated entities. We may also share any aggregate or de-identified information with our partners. … We may, on behalf of our clients and partners, collect information from end users. This may occur, for example, if someone submits information in response to an ad that we provide on behalf of an advertising client. Such information may consist of PII, non-PII, or both. In such situations, we collect the information and provide it to our client, and it will be subject to that client's privacy practices.[3] Both Millennial Media and its Jumptap subsidiary offer separate mechanism for consumers to opt out of the collection of data for "interest-based advertising."[4]

Non-compliance/ false claims	Jumptap, which promises "Consumer-Level Targeting" to its mobile-marketing clients, provides a revealing portrait of the company's data-mining and consumer profiling practices in its product literature. Drawing on the resources of over 20 offline data partners (including Acxiom, DataLogix, Polk, and TargusINFO), Jumptap claims to deliver "… the most targeted way to advertise on smartphones, tablets and other devices across all operating systems and carriers."[5] The offline data these partners share with Jumptap include highly detailed, personally identifiable information. With such vast amounts of consumer data at its disposal, Jumptap reaches 171 million consumers on over 51,000 sites and apps on smartphones and tablets, zeroing in on "… devices, locations, content and creative to reach the right consumers," who are them dispatched "… straight to calls, downloads, m-Commerce stores, landing pages and more."[6] More importantly, Jumptap was acquired by Millennial Media (which is *not* Safe Harbor-certified, and to which the jumptap.com domain is now re-directed) in November 2013, just 20 days after its last certification. In the process, Jumptap's technology was fundamentally altered: "With the completed acquisition, Millennial Media will integrate Jumptap's assets into the company's existing technology platform, including cross-screen targeting, comprehensive third-party data assets, and advanced real-time bidding technology. Millennial Media's enhanced position in the programmatic market now includes one of the most mature mobile DSP bidders (at over 1.5 billion bids per day), and one of the world's largest mobile exchanges, MMX."[7] Thus Jumptap, which posed a significant threat to consumer privacy even before its acquisition, now raises even greater Safe Harbor concerns.
FTC action on possible violations	In light of Jumptap's questionable data-mining and targeted advertising practices, and its possible failure to comply with Safe Harbor FAQ 6 regarding mergers and acquisitions, FTC should investigate and suspend Jumptap's Safe Harbor status until Millennial Media applies for and receives Safe Harbor certification. The company's disclosures that it uses unnamed third-party companies' data do not come close to informing consumers of the depth and specificity of data it is gathering on them from these partners, and FTC should investigate Jumptap for deceptively vague statements,

	regarding targeting and third parties, that could materially mislead consumers.

[1] Jumptap, "Monetizing Mobile 101: Gain More From Your Mobile Traffic," IAB presentation, 3 June 2013, p. 13, http://www.iab.net/media/file/Jumptap_MonetizingMobile_IAB_060313_Coppola.pdf; Jumptap, Safe Harbor Organization Information, expires 10/16/14, http://safeharbor.export.gov/companyinfo.aspx?id=20152 (both viewed 12 May 2014).

[2] Millennial Media, "Company Privacy Policy," http://www.millennialmedia.com/privacy-policy/ (viewed 21 May 2014).

[3] Millennial Media, "Company Privacy Policy."

[4] Millennial Media, "Opt Out," http://lp.mydas.mobi/rich/foundation/opt-out.php; Jumptap "Jumptap Opt Out," https://opt.jumptap.com/optout/opt?tlid=noid&__hstc=34171390.9a02601ccf8b2ca4e810ecf0e09ba079.1399918883988.1402951491370.1402981631069.7&__hssc=34171390.3.1402981631069&__hsfp=1693187529 (both viewed 16 June 2014).

[5] Jumptap, "The Leader in Targeted Mobile Advertising," fact sheet, 2012.

[6] Jumptap, "Generate Leads on Smartphones and Tablets," fact sheet, 2013.

[7] "Millennial Media Completes Acquisition of Jumptap," 6 Nov. 2013, http://www.millennialmedia.com/pressroom/press-releases/millennial-media-completes-acquisition-of-jumptap/ (viewed 12 May 2014).

Lithium Technologies

Complaint number	18
Company profile	Lithium Technologies provides social media customer management software for enterprise corporations seeking to implement data profiling and consumer tracking and targeting.
Main website	www.lithium.com/
Safe Harbor/privacy statements	Lithium Technologies (which "provides online communities for marketing, commerce, support and innovation purposes") claims in its Safe Harbor declaration that "[w]e never use community end user data for marketing purposes"[1] Its privacy policy simply states that "Lithium Technologies complies with the U.S. – E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. Lithium Technologies has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[2] The company's privacy policy also makes the following statements concerning its collection and use of consumer data: > As a matter of policy we do not sell your personally identifying information. We may disclose your personally identifying information … to companies that provide services to help us with business activities such as marketing or website analytics. These companies are authorized to use your personally identifying information only as necessary to provide these services to us. > … We partner with a third party ad network to either display advertising on our Web site or to manage our advertising on other sites. Our ad network partner uses cookies and Web beacons to collect non-personally identifiable information about your activities on this and other Web sites to provide you targeted advertising based upon your interests. …[3] This privacy statement also includes two mechanisms for consumers to opt out of Lithium's "behavioral targeteing," through both TRUSTe's Preference Manager and Google Ads Settings.[4]

Non-compliance/ false claims	Lithium's own marketing materials, on the other hand, reveal the extent to which it both targets and tracks individual consumers across the Internet. "Our social platform enables you to engage with customers not only on your domain," Lithium promises its clients, "but off domain as well—creating a unified and more satisfying customer experience."[5] Extensive data mining and analytics, moreover, "… enable Lithium Social Intelligence to mirror your community structure so you can intuitively understand and drill down into what users are doing on your community."[6] Additionally, although Lithium also claims in its Safe Harbor declaration that "We never rent or sell … information to third parties," this promise means little when the company is actively *acquiring* third parties (such as the "once-controversial social scoring startup" Klout).[7] This acquisition, Lithium explains, "brings together the 100 million consumers who engage across Lithium communities every month with the 500 million consumers touched by Klout to establish one of the biggest data footprints of consumer attitudes, preferences and activities."[8] Acquisitions such as these, which Lithium fails to mention in its Safe Harbor documentation, raise serious questions about the company's certification.
FTC action on possible violations	Lithium's Safe Harbor certification should be investigated for not updating both its Safe Harbor documentation and its own privacy policy to reflect its consumer-tracking practices, especially in light of its acquisition of Klout. Furthermore, the types of targeting it offers to clients for tracking and connecting with individual users seems to demonstrate that its Safe Harbor declaration is misleading, as that statement would preclude marketing that targets consumers based on their individual characteristics. Lithium does not inform EU consumers of the actual uses of their data the company manages as a part of its daily business.

[1] Lithium, Safe Harbor Organization Information, expires 12/12/14, http://safeharbor.export.gov/companyinfo.aspx?id=21124 (viewed 12 May 2014).

[2] Lithium, "Lithium Privacy Policy," http://www.lithium.com/privacy (viewed 21 May 2014).

[3] Lithium, "Lithium Privacy Policy."

[4] TRUSTe, "Your Advertising Choices," http://preferences-mgr.truste.com/; Google, "Privacy & Terms: Advertising," http://www.google.com/policies/technologies/ads/ (both viewed 16 June 2014).

[5] Lithium, "Social Marketing: Drive Social Marketing Success," http://www.lithium.com/products-solutions/social-marketing (viewed 12 May 2014).

[6] Lithium, "Social Web Analytics," http://www.lithium.com/products-solutions/social-media-analytics (viewed 12 May 2014).

[7] JP Mangalindan, "Klout Acquired for $200 Million by Lithium Technologies," CNN Money, 26 Mar. 2014, http://tech.fortune.cnn.com/2014/03/26/klout-acquired-for-200-million-by-lithium-technologies/ (viewed 12 May 2014).

[8] Rob Tarkoff, "Lithium Acquires Klout," Lithium's View Blog, 27 Mar. 2014, http://community.lithium.com/t5/Lithium-s-View-blog/Lithium-acquires-Klout/ba-p/139508 (viewed 12 May 2014).

Lotame

Complaint number	19
Company profile	Lotame is a data management platform that collects and organizes detailed consumer profiles, combining first- and third-party data to target specific individuals.
Main website	www.lotame.com/
Safe Harbor/privacy statements	Although Lotame has applied for and received Safe Harbor certification since 2011, according to its most recent Safe Harbor declaration it "does not currently receive personal information (understood in U.S. terms as 'Personally Identifiable Information' or 'PII') from the EU in connection with marketing, but may at a future time."[1] As a disclosure to EU consumers, this statement is inherently misleading, since those consumers cannot be expected to understand the reference to the definition of PII in the U.S. (where cookies and other tracking numbers are handled differently than in the EU). The Safe Harbor itself applies to all identifiable personal information,[2] not PII "understood in U.S. terms." The company's privacy policy, meanwhile, simply states that "Lotame complies with the US-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. Lotame has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[3] Additionally, concerning its data collection and use, Lotame's privacy policy includes the following statements: To deliver our services, we and our clients collect, organize, and use non-personal information reflecting your interactions with a variety of websites. This information includes items such as the date and time you visited a Website, your browser information, your IP address, your browsing behavior, your age and gender, and interests you express or imply at social networking sites or other websites you visit. Lotame's DMP recognizes your computer over time by setting a unique browser cookie, which your browser relays to our servers when you visit websites that are affiliated with our partners or clients. We and our clients may also supplement the information we collect with additional non-personal information we obtain from

	other companies. In certain of these cases, information we or our clients obtain from third parties is derived from personal information and de-identified prior to its use. We analyze the non-personal information we collect or obtain from third parties and organize it into anonymous user profiles, groups, and audiences, based on factors such as age, gender, geography, interests and online actions. We and our clients and partners then use these anonymous user profiles, groups and audiences to design and deliver customized advertising campaigns or other relevant content. We and our clients also use this data for other related purposes (for example, to do research regarding the results of our online advertising campaigns or to better understand the interests or activities of Website visitors.) The behavioral categories we use to customize the ads you may see or for related purposes do not use personal information such as your name, address, e-mail address, phone number, birth date or social security number. Our technology and services are designed to limit our use of consumer data to anonymous, non-personal information. Note that we license our DMP to third parties, such as website publishers and marketers. A third party licensee using Lotame's DMP may elect to collect, manage and use other types of data through Lotame's DMP, which may include personal information (where permissible). Please consult the privacy policies of the Websites you visit to become familiar with their privacy practices.[4] Additionally, Lotame provides users "with the ability to opt-out of our use of information about your previous browsing to tailor the ads you see."[5] The opt-out mechanisms include the National Advertising Institute's "Consumer Opt-out" service, the Digital Advertising Alliance's (DAA) Self-Regulatory Program for Online Behavioral Advertising, and, for EU consumers, the IAB Europe's "Your Online Choices" page.[6]
Non-compliance/ false claims	Coming as it does from a company that bills itself as "the global leader in delivering truly unified audience relationship management anywhere anytime," Lotame's Safe Harbor and privacy statements invite scrutiny (as does the presence on its staff since April 2013 of a "Director of European Business Development").[7] In any case, Lotame's own website offers plenty of other statements that raise

	concerns regarding the privacy of EU citizens and consumers. The company, for example, promises that its clients will be able "… to reach even the most granular audience with ease."[8] Lotame describes its data management platform as "… the backbone of data-driven marketing, and serves as a unifying platform to collect, organize and activate your first- and third-party audience data from any source," including online, offline, mobile, and point-of-sale data. "… Lotame collects audience data based on specific behaviors (such as click, download, comment), interests (such as sports, football, parenting, museums, travel) or demographic information."[9] (Demographic information, such as race, is sensitive information even "understood in U.S. terms," despite the company's Safe Harbor declaration.) Lotame Audience Data, the company explains, include "Demographics (Age, Gender, Geography, … Level of Education), Interests (Profile-based, Contextual, Demonstrated, Undeclared), Actions, … Media, … Interaction (How people interact with content and ads: clicks, time spent, interactions, videos completed), [and] Sentiment and Exposure (What people say, what they read, and when and how they say and read it)."[10] Lotame's partnerships with various third-party data providers raise additional privacy concerns. Its partnership with PubMatic, for example, "… represents the first fully-integrated offering of its kind to provide users with a comprehensive view of audience data from any source," and allowing them to "… [p]ersonalize content on an individual impression basis."[11] Other Lotame partners include AdMobius, Alliant, Bizo, BlueKai, Dataline, Datalogix, eXelate, Medicx, Mastercard, and V1.[12] All of these repositories of detailed consumer information combine to form, in Lotame's own words, "… a premier source of precise, intelligent and up-to-the-minute audience data—a key asset for successful campaigns. … Lotame collects more than 2 billion individual demographic, interest, action, search and purchase intent data points daily … . In addition, we partner with on and offline data partners who provide declared or demonstrated—not panel-based—data to maximize scale."[13] Lotame's mobile data management platform offers data collection that is both covert and automatic, gathering "… data from various browsers and devices without hindering the consumer experience in an automated fashion,"

	aggregating and activating first-party data, and accessing "… unique behavioral and demographic audience data from multiple mobile sources through Lotame's partnership with AdMobius, the industry's leading mobile 3rd party data provider."[14] Over time, Lotame promises its clients, "As the Lotame DMP evolves, enterprises are able to use audience data to supercharge their customer interactions."[15] Such marketing power and precision, unfortunately, comes at the expense of consumer privacy.
FTC action on possible violations	Lotame's Safe Harbor certification should be examined closely by FTC, in light of the company's questionable current declaration that reads out EU legal definitions of personal information, as well as ad-targeting practices for which Notice and Choice must be clearly given if the Safe Harbor standard is to be met. Its control over the means of processing and its practice of combining information from partners to create consumer profiles make Lotame a controller. This company apparently collects EU consumer personal information and uses it for targeting of individuals, and shares individuals' detailed profiles with third parties without any privacy protections—and its disclosure implies it does not comply with Safe Harbor due to a self-serving understanding of PII.

[1] Lotame, Safe Harbor Organization Information, expires 11/22/14, http://safeharbor.export.gov/companyinfo.aspx?id=20874 (viewed 12 May 2014).

[2] *See* definition of "personal data" and "personal information" in Safe Harbor Annex I.

[3] Lotame, "Lotame Privacy Policy," http://lotame.com/legal (viewed 21 May 2014).

[4] Lotame, "Lotame Privacy Policy."

[5] Lotame, "Lotame Privacy Policy"; Lotame, "Opt-out and Preferences Manager," http://www.lotame.com/opt-out-preference-manager (both viewed 16 June 2014).

[6] National Advertising Initiative, https://www.networkadvertising.org/; Digital Advertising Alliance, " Self-Regulatory Program for Online Behavioral Advertising," http://www.aboutads.info/; "Your Online Choices," http://www.youronlinechoices.eu/ (all viewed 16 June 2014).

[7] "Lotame Appoints Director of European Business Development," 3 April 2013, http://lotame.com/news/lotame-appoints-director-european-business-development (viewed 12 May 2014).

[8] Lotame, "Audience Data," http://lotame.com/data (viewed 12 May 2014).

[9] Lotame, "The Power of a Unifying DMP," http://lotame.com/audience-management-platform/power-unifying-dmp (viewed 12 May 2014).

[10] Lotame, "Data Solutions," data sheet.

[11] "PubMatic Partners With Data Management Platform Lotame To Help Publishers Boost Engagement," 9 Apr. 2013, http://www.pubmatic.com/press/2013/PubMatic-Partners-With-Data-Management-Platform-Lotame-To-Help-Publishers-Boost-Engagement.php (viewed 12 May 2014).

[12] Lotame, "Smart Data," http://lotame.com/data-management-platform/target-audience-segments (viewed 3 June 2014).

[13] Lotame, "Smart Data."

[14] Lotame, "Mobile Data Management Platform," http://lotame.com/mobile-data-management-platform (viewed 3 June 2014).

[15] Lotame, "Audience relationship Management," http://lotame.com/audience-management-platform/audience-relationship-management (viewed 3 June 2014).

Marketo

Complaint number	20
Company profile	Marketo makes marketing automation software for companies interested in lead-generation and personalized advertising applications, including detailed consumer profiling, tracking, and targeting.
Main website	www.marketo.com/
Safe Harbor/privacy statements	Marketo is typical of those U.S. marketing companies that assert compliance with the Safe Harbor Framework as a *processor* rather than a *controller* of personal information from EU countries: "Since EEA Data covered by this Notice is by definition sent to us by another company in the EEA (e.g., a customer of Marketo), the categories of data sent and the purposes of processing often depend on such other company … . We collect and use EEA Data for purposes of providing products and services to our customers, communicating with corporate business partners about business matters, processing EEA Data on behalf of corporate customers, providing information on our services, and conducting related tasks for legitimate business purposes."[1] In addition to a privacy policy stating that Marketo "… adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement," this policy also explains its use of cookies (required cookies, performance cookies, functionality cookies, and analytics and retargeting cookies), as well as various third-party means of opting out of these cookies (Network Advertising Initiative, Digital Advertising Alliance, About Cookies.org, and Macromedia). Marketo's website also maintains a separate "Safe Harbor Notice" that includes the following explanations concerning Marketo's Safe Harbor participation: **Categories of EEA Data** We sell integrated web-based business application software largely to small and midsize businesses. We receive mostly business-related information from the EEA, including contact information of individual representatives of the businesses with whom we are dealing, including, without limitation, names, addresses, work phone numbers, work email addresses, etc. of EEA Persons ("EEA Data"). In connection with some services, e.g., Marketo's Lead Management services, our customers use our hosted technology platform to store and

	process EEA Data at their own discretion. Since EEA Data covered by this Notice is by definition sent to us by another company in the EEA (e.g., a customer of Marketo), the categories of data sent and the purposes of processing often depend on such other company, with whom the EEA Persons typically have a closer employment or business relationship (and which, therefore, can provide additional information on categories of data shared with us). **Purposes** We collect and use EEA Data for purposes of providing products and services to our customers, communicating with corporate business partners about business matters, processing EEA Data on behalf of corporate customers, providing information on our services, and conducting related tasks for legitimate business purposes. **Disclosure** We share EEA Data with our affiliates and contractors, who process EEA Data on behalf of Marketo. We also share EEA Data with other third parties for the purposes for which we receive the EEA Data (e.g., performance of contractual obligations and rights), and we may also disclose EEA Data where we are legally required to disclose (e.g., under statutes, contracts or otherwise) or the disclosure is permitted by law or the Safe Harbor Principles and we have a legitimate business interest in such disclosure.[2]
Non-compliance/ false claims	The above definition for "EEA Data" is confusingly written, partly due to its numerous clauses with two consecutive uses of "including." This definition would lead reasonable consumers to think this data was comprised of "contact information of individual representatives of the businesses with whom we are dealing," which is then qualified by the remaining portions of the definition. Assuming that the company collects consumer data, as its business model requires, this is misleading because it does not disclose the collection or use of any consumer personal information. Further, Marketo's Safe Harbor and privacy statements give consumers little information about the nature of the data collected or how they are processed, nor do they say what "products or services" are implicated. As Marketo's own marketing makes clear, however, its extensive suite of data collection, storage, and analysis technologies raises questions about its Safe Harbor disclosure in light of the

	detailed consumer profiling and tracking involved. Marketo's Consumer Engagement Marketing service, for example, includes a "marketing database of record that constantly learns about your customers. … That data spans contact information, demographic data and transactional data, but also automatically stores digital behaviors about each individual person that interacts with your marketing."[3] Operating across multiple platforms, moreover, Marketo empowers its clients to "[t]rack consumer behaviors, affinity, and context across every digital, social, and mobile channel in a single data repository. … For each Marketo customer organization, our platform stores and maintains an individual, secure and trusted database with information about each prospect and customer, including context and online and offline behaviors. … Our platform uses big data techniques to scale to support databases with tens of millions of customer and prospect records, and a billion or more individual data points about their behaviors."[4] Promising "… deep, durable 1:1 customer relationships," Marketo also allows companies to combine first- and third-party data: "Our platform is designed to be extensible to create a digital marketing hub, bringing together our applications with a growing number of third-party application providers in our LaunchPoint partner network, the largest and most complete ecosystem of marketing solutions. Further, our platform includes interfaces for data exchange with other enterprise systems and applications."[5] On its own and in partnership with other data providers, Marketo represents a significant threat to E.U. consumer privacy.
FTC action on possible violations	Marketo's Safe Harbor certification should be investigated and sanctioned in light of the company's failure to disclose the full range of its data-mining and ad-targeting technologies, which are never properly described in its Safe Harbor disclosure. It instead suggests that it is only collecting contact information for its corporate partners' employees, which is contradicted by the company's marketing about its data capabilities and services.

[1] Marketo, Safe Harbor Organization Information, expires 4/26/15, http://safeharbor.export.gov/companyinfo.aspx?id=22762 (viewed 13 May 2014).

[2] Marketo, "Privacy Policy," http://www.marketo.com/trust/legal/privacy; Marketo, "Marketo Safe Harbor Notice," http://www.marketo.com/trust/safe-harbor (both viewed 21 May 2014).

[3] Marketo, "Marketing Database of Record," http://www.marketo.com/software/consumer/marketing-database/ (viewed 13 May 2014).

[4] Marketo, "The Most Advanced Platform for Customer Engagement," http://www.marketo.com/platform/ (viewed 13 May 2014).

[5] Marketo, "The Industry's Most Powerful and Complete Platform for Digital Marketing," http://www.marketo.com/digital-marketing-platform/ (viewed 3 May 2014).

MediaMath

Complaint number	21
Company profile	MediaMath is a digital marketing technology whose marketing "operating system" (TerminalOne) combines digital media and consumer data in a single platform that permits consumer profiling, tracking, and targeting.
Main website	www.mediamath.com/
Safe Harbor/privacy statements	MediaMath claims in its Safe Harbor certification statement, with regard to personal information received from the EU/EEA and/or Switzerland, that "[a]ll data collected is anonymous and no personally identifiable information is collected through our buying platform, Terminal One." Upon its re-certification in May 2014, the company added the following acknowledgement that some of the data it collects might, in fact, be classified as "personally identifiable" in the EU: "We recognize, however, that in some contexts, both IP Address and cookie ID may be considered personal data under the EU's 1995 Data Protection Directive. As a precaution, we have signed onto the US-EU and US-Swiss Safe Harbor Frameworks due to the possibility that an European Data Protection Authority might deem some of the information we collect to be personal data." [1] The company's privacy policy simply states that "MediaMath complies with the US-EU Safe Harbor Framework and the US Swiss Safe Harbor Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personally identifiable information from European Union member countries and Switzerland. MediaMath has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[2] Concerning its data collection and usage, MediaMath's privacy policy explains that In the course of delivering an ad to you, MediaMath does not collect personally identifiable information about you. Personally identifiable information includes data such as your name, address, phone number, social security number, or email address. MediaMath does collect non-personally identifiable information about you, for the use of targeting ads and measuring the effectiveness of ads on behalf of MediaMath's

	advertisers. … MediaMath may use this non-personally identifiable data to create data segments, and these data segments are generally based upon the websites that you visit. MediaMath also receives information from 3rd party data providers who collect and make available information such as behavioral, contextual, and demographic data, for our clients to use in targeting ads through our platform. For example, our clients may use health-related segments such as an inferred interest in health and wellness or cough medicine and allergy medications. … MediaMath does not collect data or create data segments that are based upon what we consider to be sensitive information (for example, we don't use any data segments to determine credit worthiness, for insurance underwriting or similar purposes). At MediaMath, we think it's important to provide transparency to help you have a better idea of which segments might be collected by us, so you can make informed decisions.[3] The privacy policy also discusses the company's use of cookies ("A MediaMath cookie is a unique number that is assigned to your browser the first time MediaMath serves your browser an ad or identifies your browser on a client's website"), and offers a variety of third-party opt-out mechanisms (Network Advertising Initiative, Digital Advertising Alliance, Digital Advertising Alliance Canada, and Digital Advertising Alliance EU).
Non-compliance/ false claims	The company's advertising platform, as MediaMath proclaims elsewhere, is designed to track and target individual consumers with extreme precision, in contrast to the seemingly innocuous audience segmenting described above. Through MediaMath's TerminalOne, for example, "… marketers can speak to their customers as individuals, utilizing the latest technology and audience data to deliver finely targeted ad messages across channels … ."[4] MediaMath works with "… over 150 technology, media, and data partners across the digital ecosystem" to target individual consumers with great precision.[5] "Through seamless integration with all leading data providers," the company explains, "MediaMath's data management platform enables advertisers to build custom data cooperatives and effectively synchronize first- and third-

	party data across multiple campaigns."[6] MediaMath gained considerable consumer-targeting power in 2013 when it acquired Akamai, whose Advertising Decision Solutions (ADS) system gives MediaMath and its clients new access to behavioral data.[7] Among the company's partners is LiveRamp (recently acquired by Acxiom), which allows MediaMath "… to build a seamless programmatic buying experience using offline data. LiveRamp has onboarded data for over 65 brands to TerminalOne, MediaMath's proprietary digital media, data management, and analytics platform. … 'Offline' customers can be found online, thus widening the marketer's audience pool."[8] Additionally, "MediaMath customers … have access to more than 60 billion monthly video impressions thanks to key agreements with several ad exchanges … . MediaMath's programmatic video ad options … include inventory from ad exchange partners LiveRail, BrightRoll, Adap.tv and DoubleClick Ad Exchange."[9] MediaMath's data profiling and consumer targeting will become even more powerful with its recent acquisition of Tactads, the France-based provider of cookie-less and cross-device targeting technologies. "Integrated into TerminalOne," MediaMath explains, "these technologies will provide advertisers the ability to communicate with consumers and unify marketing efforts across smartphone, tablet, laptop, desktop, and other devices."[10]
FTC action on possible violations	MediaMath should be investigated in light of the company's failure to provide adequate Notice of the full range of its data-mining and ad-targeting technologies, and of its partnerships with LiveRamp, Akamai, and others.[11] In its certification with DOC it acknowledges that IP addresses and cookies can be personal data in EU law, but in policies meant for consumers it deceptively describes these same tracking identifiers as "non-personally identifiable." Any assertion that it is not a controller is rebutted by its control over, and commingling of, large amounts of EU consumer personal information. Its assertion that all data it collects and uses are anonymous and non-personal is contradicted by its actual practice of integrating its data with many other companies' data sets of first- and third-party information, as well as its emphasis on individual tracking and targeting. Furthermore, targeting consumers using "health-related segments" is inherently using highly personal information about a person's health that requires

	advance affirmative opt-in Choice under the Safe Harbor.

[1] MediaMath, Safe Harbor Organization Information, expires 5/15/15, http://safeharbor.export.gov/companyinfo.aspx?id=23428 (viewed 11 Aug. 2014).

[2] MediaMath, "Privacy Policy," http://www.mediamath.com/privacy/ (viewed 21 May 2014).

[3] MediaMath, "Privacy Policy."

[4] "MediaMath," Ad Age Audience Buying Guide 2013, http://brandedcontent.adage.com/audiencebuyingguide2013/network.php?id=9 (viewed 13 May 2014).

[5] "MediaMath," advertising brochure, emphasis in the original, pp. 4-5.

[6] "MediaMath," Ad Age Audience Buying Guide 2013.

[7] Jason Del Rey, "Mediamath Acquires Akamai's Ad Business to Beef Up Data-Management Capabilities," *Ad Age*, 24 Jan. 2013, http://adage.com/article/digital/mediamath-acquires-akamai-s-ad-business-beef-data-management-capabilities/239365/ (viewed 17 July 2014).

[8] MediaMath, "MediaMath Partners With LiveRamp to Incorporate CRM Data into Programmatic Media Buying," LiveBog, 30 Apr. 2013, https://blog.liveramp.com/2013/04/30/mediamath-partners-with-liveramp-to-incorporate-crm-data-into-programmatic-media-buying/ (viewed 13 May 2014).

[9] Michelle Castillo, "MediaMath Adds Several Ad Exchanges: Clients Can Now Choose from DoubleClick Ad Exchange, BrightRoll," *Adweek*, 22 Apr. 2014, http://www.adweek.com/videowatch/mediamath-adds-several-ad-exchanges-157170 (viewed 3 June 2014).

[10] "MediaMath Acquires Tactads to Enable Cookieless, Cross-Device Targeting and Measurement," CNW, 24 Apr. 2014, http://www.newswire.ca/en/story/1343707/mediamath-acquires-tactads-to-enable-cookieless-cross-device-targeting-and-measurement (viewed 7 July 2014).

[11] For full list of MediaMath's many partners, see MediaMath, "Partner Marketplace," https://open.mediamath.com/partners (viewed 13 May 2014).

Merkle

Complaint number	22
Company profile	Merkle is a customer relationship-marketing (CRM) agency that specializes in data-based marketing applications, including consumer profiling and targeted advertising.
Main website	www.merkleinc.com/
Safe Harbor/privacy statements	With regard to personal information received from the EU/EEA and/or Switzerland, Merkle takes a decidedly hands-off approach in its Safe Harbor certification, denying all responsibility for such data. The company, it declares, "… acts as a processor on behalf of its clients, … processes marketing information of its clients and on behalf of its clients … [and] acts on the instructions of its clients and does not control or share such data without direction from the client. …"[1] The company's EU Safe Harbor privacy policy repeats this processor-on-behalf disclaimer and promises that "Merkle will not disclose to third parties personal data processed in this capacity, except as permitted or required by the processing agreement, EU Safe Harbor, applicable Member State data protection law or as otherwise required by law."[2] Its corporate privacy policy, meanwhile, offers the following details about the company's data-collection and usage practices: Information is at the core of Merkle's business. Merkle obtains marketing information (including information about consumers and businesses) from and through our clients. Merkle also acquires marketing information from third parties to be used by our clients. Many of our client solutions involve various uses of information, including the storage, exchange, transfer, management, analysis and/or reporting of such information. Merkle does not collect data directly from consumers except for information collected as part of our clients' marketing programs, … Merkle provides information management and marketing services designed to help companies improve their marketing strategies and programs. These services may involve third parties and may utilize cookies, web beacons, or other tracking or retargeting mechanisms. When we provide these services to our clients, we process information according to the terms and conditions of the contract with our clients. Accordingly, Merkle relies upon the instructions of its clients with

	respect to the use of marketing information and ultimately our clients advise us as to a consumer's preferences or opt-in/opt-out choices.[3] Merkle's opt-out mechanisms are rudimentary, providing third-party mailing address for opting out of direct mail advertising and telemarketing calls, and relying "upon the instructions of its clients" for online opt-out procedures.
Non-compliance/ false claims	Merkle's privacy statements do not explain, however, what it does with user information, nor what information it collects, regardless of whom it is working for. In other contexts, however, Merkle is much more forthcoming about the power of its data practices, and the role it plays in identifying and targeting individual consumers. "Our dedication to a data-driven, information-based approach is a key reason for our clients' success," the company explains, and the key to Merkle's success is the precision with which it profiles individual consumers.[4] "Merkle's Connected Recognition solution supports a connected party-level event stream where all engagement with the customer is tied back to the master identifier."[5] So important is this unique ID that Merkle does not even bother with the pretense of anonymity: "This event stream is created for all known parties, whether they are repeat customers or anonymous parties that visited the website. All interactions that occurred with the consumer can be tied to the event stream to support integrated, cross media and channel marketing decisions."[6] Merkle's Connected Recognition process works across all channels and media, online and off, to create detailed personal dossiers—"a complete identity map across all party or user identifiers to ultimately be tied to an individual."[7] And "[b]ecause it links to a persistent offline ID and not just cookies, Merkle customers are safe from scale shrinkage due to data breakage when syndicating audiences to online channels."[8] Regardless of platform or location, Merkle remains committed to "… gaining a deeper understanding of 'the customer' as a unique individual by tracking that individual's related experiences and behaviors across different media (TV, direct mail, email, display) and channels (mobile, online, call center, support) … . Merkle is able to make that crucial connection between the customer identity and experience."[9] Merkle's data-profiling operation has grown considerably more powerful, moreover, as a result of a number of

	corporate acquisitions. "RKG and New Control are only the two most recent in a long string of Merkle acquisitions that began in 2011 and now include data exchange Brilig, responsive design company 5th Finger, social commerce platform Social Amp and search marketing and media agency IMPAQT."[10] Of particular interest to EU consumers, Merkle is active internationally, especially in the area of consumer profiling: "At Merkle, we support some of the world's biggest brands to optimize their global sourcing efforts—a process rooted in a deep understanding of local nuances, data-agnostic objectivity and empirical derivation of value—ultimately ensuring that our clients have an advisor to help them navigate the confusing and complex task of sourcing global marketing data.[11] Consumers, too, need help navigating these waters, but they are not likely to receive that assistance from companies like Merkle, which are actively involved in data mining and profiling.
FTC action on possible violations	Merkle should be investigated in light of the company's failure (1) to describe the active role it actually plays in structuring and deploying its clients' ad campaigns, and the control it exercises over EU consumers' personal information, and (2) to provide adequate Notice to consumers concerning the full range of its data-mining and ad-targeting technologies. The company incorrectly claims to be a processor, when it exercises control over the means of processing personal information, which it gathers from numerous third-party sources and combines for clients. Its current disclosure merely disclaims liability for actions that it never describes to EU consumers, thus failing to provide them Notice or give them a chance to consent. Merkle also might be failing to provide an effective mechanism for consumers to exercise Choice.

[1] Merkle, Safe Harbor Organization Information, expires 8/13/14, http://safeharbor.export.gov/companyinfo.aspx?id=19770 (viewed 13 May 2014).

[2] Merkle, "EU Safe Harbor Privacy Policy," http://www.merkleinc.com/eu-safe-harbor-privacy-policy (viewed 21 May 2014).

[3] Merkle, Privacy," http://www.merkleinc.com/privacy#.U6B3eY1dXfY (viewed 16 June 2014).

[4] Merkle, "Analytics," http://www.merkleinc.com/what-we-do/database-marketing-services/analytics (viewed 13 May 2014).

[5] Merkle, "Connected Recognition," http://www.merkleinc.com/what-we-do/database-marketing-services/connected-recognition (viewed 13 May 2014).

[6] Merkle, "Connected Recognition."

[7] Merkle, "Connected Recognition."

[8] "Merkle Extends CRM Strength Across Channels and Screens Via [x+1] Origin Data Management Platform," 30 Apr. 2014, http://www.xplusone.net/merkle_partners_with_x1/ (viewed 3 June 2014).

[9] Cloudera, "Merkle Delivers Connected Consumer Recognition with Its Enterprise Data Hub," http://www.cloudera.com/content/cloudera/en/our-customers/merkle.html (viewed 3 June 2014).

[10] Allison Schiff, "Merkle's Acquisition Spree Now Includes RKG," Ad Exchanger, 2 July 2014, http://www.adexchanger.com/agencies/merkles-acquisition-spree-now-includes-rkg/; "Merkle Acquires Brilig, a Leading Data Exchange for Online Advertising," 10 Sept. 2012, http://www.merkleinc.com/news-and-events/press-releases/2012/merkle-acquires-brilig-leading-data-exchange-online-advertising#.U8VoMY1dXfZ; Brilig, "Coop Members," http://www.brilig.com/coop-members.php (all viewed 17 July 2014).

[11] MediaMath, "MediaMath Partners With LiveRamp to Incorporate CRM Data into Programmatic Media Buying," LiveBog, 30 Apr. 2013, https://blog.liveramp.com/2013/04/30/mediamath-partners-with-liveramp-to-incorporate-crm-data-into-programmatic-media-buying/ (viewed 13 May 2014).

Neustar

Complaint number	23
Company profile	With its 2013 acquisition of Aggregate Knowledge, Neustar is now a leading provider of consumer profiling and targeted advertising for the Internet, telecommunications, entertainment, and marketing industries.
Main website	www.neustar.biz/
Safe Harbor/privacy statements	Neustar's Safe Harbor declaration concerning the personal information it receives from the EU/EEA and/or Switzerland is disarmingly simple: "Personal information about residents of the European Union and Switzerland received in the course of providing DNS services (including Registry and Site Protect services) and telephone call routing services."[1] This highlights information irrelevant to consumers: *where* information might be gathered from, but not *what* information it is nor *how* it will be used and shared. Its privacy statement is equally direct but unhelpful, repeating the DNS and call-routing stipulations and declaring its "… adherence to the Safe Harbor principles of notice, choice, onward transfer, security, data integrity, access, and enforcement."[2] While the more accessible "Neustar Privacy Center" offers highlights of the company's privacy principles, only the full Neustar Privacy Policy provides information on its data-collection and usage practices, including the following: **Personal Information Collection, Use, and Disclosure** **Information You Provide on our Web Sites**. On our web sites, we collect Personal Information only if you choose to give it to us, for example by subscribing to RSS feeds or blog posts or electing to "follow" Neustar on social media sites. Like all web sites, we automatically collect Log Data about your visits. This information does not identify you to us unless you have given us your name, contact information, or other Personal Information. We use Personal Information and Log Data to respond to your requests, process transactions you initiate, improve our web site, and deliver personalized content to you. We may disclose that information to third parties to help us in these activities, but we do not allow them to use the Personal Information for other purposes.

	Name, Address, Phone and Contact Data. Information collected from communication services providers for Numbering Services is strictly segregated and used to provide those services only. Separately, we collect name, address, telephone number, and other contact information from a wide variety of public and private sources. Our business customers use this information to identify or verify the identity of customers and prospective customers who contact them, to provide better customer service, and to communicate more effectively with consumers. **Market Segmentation Data**. We collect consumer survey data and household/neighborhood-level demographic data from third party providers, which we aggregate and use in our ElementOne platform to make predictions about the preferences and interests of large groups of similar consumers. **We do not track consumers on or off line, and we do not build consumer profiles based on a specific person's online behavior**.[3] To complicate matters further, Neustar maintains a separate privacy policy and opt-out mechanism for its AdAdvisor product (which "provides rich demographics-based data to online marketers and websites," and which is the only opt out that the company offers).[4]
Non-compliance/ false claims	Neustar's several privacy statements hide material information that is important to EU consumers, failing to reflect as these statements do Neustar's acquisition of Aggregate Knowledge (AK) just a month after Neustar's first Safe Harbor certification in September 2013. Both companies are Safe Harbor participants but their combined business structure is not covered by out-of-date Notice and Choice disclosures and mechanisms. Judging from Neustar's own comments on the impact of its AK acquisition—"The combination of Neustar's real-time, offline and online marketing solutions and Aggregate Knowledge's media intelligence platform provides agencies and marketers the ability to plan, target, engage and measure cross-channel campaigns more effectively in a single view,"—it seems clear that Neustar has undergone a fundamental change—one that needs to be reflected in its Safe Harbor and privacy policy documentation.[5] Such changes also are likely to require additional notifications to consumers so they can exercise Choice and opt out of new

	data sharing and uses. Both the parent and subsidiary have troubling practices under the Safe Harbor in addition to the aforementioned merger concerns. Neustar's "Buying Power" applications, for example, enable its customers to "gain instant intelligence on households likely to have the financial capacity to buy specific products or services. Ultimately, businesses can leverage these financial insights to tailor offers and promotions to match consumers with the most appropriate product or service and improve conversion rates and return on marketing investments, and improve customer experiences."[6] Neustar also claims that its scoring application can "match the right consumer with the right offer at the right price," explaining that "proprietary financial insight is delivered to help differentiate between groups of households that may appear to be identical using traditional segmentation platforms, but in fact are likely to have considerably different purchasing power. Buying Power Insight was designed to deliver insights about a household's expected financial resources by combining aggregated credit information and household-level demographics to build predictive segments based on the likelihood of household groupings to respond to offers and make purchases. With this insight, marketers can match prospects with the relevant product or service and the right promotion or offer."[7] For its part, Aggregate Knowledge claims that "AK's patented Media Intelligence Platform (MIP) is the industry's only data management solution of its kind providing "[a]udience and media data on a single platform. … Cross-channel insights in a single view, including Facebook. Track performance of all digital channels and mediums. [and] [c]omplete customer touch-point tracking."[8] Together, the merged companies are a marketing force to be reckoned with—and, therefore, a Safe Harbor participant of note. Clearly, the new Neustar has moved far beyond the modest DNS and call-routing service provider that first applied for Safe Harbor certification in September 2013. As the company announced upon the introduction of its new PlatformOne marketing product in March 2014, "There are three main components combined and integrated into this platform that make it a unique powerhouse for marketers:

	• Customer Intelligence—PlatformOne leverages Neustar's proprietary data … . Marketers can identify and verify their customers in real-time … . • Media Intelligence—PlatformOne provides marketers with real-time media intelligence by connecting online and offline data … . • Activation—By combining customer and media intelligence, PlatformOne ensures a personalized dialogue across every customer or prospect interaction.[9] Neustar, in other words, is not the same company that received Safe Harbor certification nine months ago, and Aggregate Knowledge—at least as an independent corporation that was certified a month earlier—no longer exists at all.
FTC action on possible violations	In light of both Neustar's and Aggregate Knowledge's failure to update their respective Safe Harbor certificates upon the consummation of their merger, both companies' compliance should be investigated and the current entity sanctioned by FTC. Contrary to affirmative disclosures that it does not track users online and profile them using that information, the company now "connect[s] online and offline data" and has access to Aggregate Knowledge's online tracking and profiling, including tracking through Facebook. Neustar's attempts at re-certification in September, moreover, should be contingent upon a full disclosure of the consumer tracking and targeting practices of the new company, along with adequate Notice and Choice covering these practices. The company's disclosures imply that it uses personal information, such as address and census data, but does not make clear to EU consumers that it is serving them to advertisers based on their buying power and susceptibility to an offer. Such silence on the actual data and targeting the company uses is materially misleading.

[1] Neustar, Safe Harbor Organization Information, expires 9/29/14, http://safeharbor.export.gov/companyinfo.aspx?id=20265 (viewed 13 May 2014).

[2] Neustar, "Privacy Policy," http://www.neustar.biz/privacy#.U31tmlhdXfY (viewed 21 May 2014).

[3] Neustar, "Privacy Policy."

[4] Neustar, “Neustar AdAdvisor,” http://www.adadvisor.net/; Neustar, “AdAdvisor Privacy Policy,” http://www.adadvisor.net/privacy.html; Neustar, “Opt-Out Here,” http://www.adadvisor.net/optout.html (all viewed 16 June 2014).

[5] “Neustar Acquires Aggregate Knowledge,” 30 Oct. 2013, http://www.neustar.biz/about-us/news-room/press-releases/2013/neustar-acquires-aggregate-knowledge#.U3_AolhdXfa (viewed 21 May 2014).

[6] Neustar, “Neustar® ElementOne Buying Power & Customer Insights,” http://www.neustar.biz/resources/product-literature/buying-power-insights-solution-sheet#.Uxys0vSwIxI (viewed 9 Mar. 2014).

[7] “Neustar® ElementOne Buying Power & Customer Insights.”

[8] Aggregate Knowledge, “How We’re Different,” http://www.aggregateknowledge.com/platform/media-intelligence-platform/how-were-different/ (link expired).

[9] Neustar, “PlatformOne™ Simplifies Complex Marketing Ecosystem; Its Unified Approach Maximizes Customer Reach, and Enhances Inbound/Outbound Marketing,” 24 Mar. 2014, http://seekingalpha.com/pr/9345183-neustar-launches-platform-to-centralize-marketing-solutions-and-optimize-campaigns (viewed 21 May 2014).

PubMatic

Complaint number	24
Company profile	PubMatic provides technology to help online publishers automate the process of data collection, consumer profiling, and personalized advertising.
Main website	www.pubmatic.com/
Safe Harbor/privacy statements	PubMatic's Safe Harbor statement is more forthright than most, in that the company acknowledges the collection of "… IP address and in some cases geo location and device ID from our publishers" as well as the collection of "… data through analysis of HTTP communications, including ad calls, and also through the use of cookies, which we distribute directly, and which our clients also distribute."[1] The company's privacy policy, with a separate, detailed page devoted to Safe Harbor, is also commendable. In addition to the standard Safe Harbor endorsement ("PubMatic has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement"), PubMatic also explains, "We collect and use EEA Data for purposes of marketing, providing and improving our products and services, communicating with corporate business partners about business matters, and conducting related tasks for legitimate business purposes. … We share EEA Data with our affiliates and contractors who process EEA Data on behalf of PubMatic."[2] While these statements pertain to the company's handling of its own customers' data, a closer examination of PubMatic's privacy policy reveals much more about how *consumer* data are handled. First, such data are collected from a variety of sources: … through the software applications made available by us for use on or through computers and mobile devices (the "Apps"), through our social media pages and apps (collectively, our "Social Media Pages") as well as through HTML-formatted email messages that we send to you that link to this Privacy Policy and our technologies used by our publishers, demand partners and third parties that we use to gather and process information on their behalf (collectively, including the Websites, the Apps and our Social Media Pages, the "Services"). By providing Personal Information to us, you agree to the terms and conditions of this Privacy Policy.[3]

	Such data, moreover, include highly detailed personal information: • Name • Postal address • Telephone number • Email address • Profile picture[4] PubMatic's privacy policy also discusses the company's other means of data collection (e.g., through one's browser or mobile device identifier; through the PubMatic app; through pixel tags; and through cookies), as well as how such information may be disclosed (e.g. among affiliates and third-party service providers). Pubmatic also provides a number of ways for consumers to opt out of cookies, through such third parties as the Network Advertising Initiative and Digital Advertising Alliance as well as on PubMatic's own site.[5] As PubMatic explains on its website, "Real-Time Bidding, pioneered for publishers by PubMatic in 2009, is the acquisition of media on an impression by impression basis. It allows both sellers and buyers to evaluate the attributes of each impression to determine its precise value. PubMatic allows publishers to truly unlock the value of their inventory by adding additional audience attributes to each impression. In fact, Publishers moving onto the PubMatic platform for Real-Time Bidding see a revenue increase between 30% and 70% for comparable inventory. Real-Time Bidding is a vital part of any digital monetization strategy. PubMatic's platform provides superior control for pricing rules and deep insights on buyer inventory preferences, packaging performance as well as bidding behavior. Our Unified Auction offers real-time evaluation of all demand sources regardless of their real-time buying capabilities. For buyers who do not have real-time bidding, PubMatic can offer a bid on their behalf based on historical buying insights—all while still managing business rules for brand control, pricing, and advertiser block lists.[6]

Non-compliance/ false claims	PubMatic's Safe Harbor and privacy documentation fall short, however, in the company's failure to disclose the nature and impact of strategic partnerships that PubMatic has developed, and how these alliances affect its own digital targeting practices by incorporating new sources of consumer data—data that is covered by the Safe Harbor definition of personal information regardless of its source. Nothing in the above disclosures expresses the vast scope of data collection and use overseen by PubMatic. The company's marketing literature is much more revealing in this regard. Concerning its partnership with Lotame, for example, PubMatic explains that this alliance "… represents the first fully-integrated offering of its kind to provide users with a comprehensive view of audience data from any source," allowing its clients to "… [p]ersonalize content on an individual impression basis. … By integrating Lotame's Crowd Control DMP, publishers will be better equipped to organize and leverage comprehensive data acquired from user interactions across multiple platforms … ."[7] In announcing an upgrade of its data management platform in June 2013, similarly, PubMatic noted that it now "… identifies devices and layers on more than 30 third-party parameters and up to 20 first-party parameters … adding the ability to combine first-party, geo, carrier, and device data into the PubMatic platform … ."[8] PubMatic has also enhanced its data mining and consumer profiling technology through the acquisition of Mocean Mobile (formerly Mojiva), allowing PubMatic to profile and target mobile users."[9] Such partnerships and alliances as these, which bring detailed consumer data onto automated ad-serving platforms, must be disclosed by those companies hoping to meet the Safe Harbor Framework's standards. In the absence of such details consumers cannot understand how their personal information is being used and disseminated, and Notice and Choice requirements cannot be met.
FTC action on possible violations	PubMatic should be investigated by FTC and sanctioned for insufficient Notice in light of the company's failure to provide adequate information concerning the detailed personal data that it incorporates in user profiling under partnerships with various third-party sources. FTC should also investigate whether the company gave consumers Notice of the true underlying purposes and uses of their

	information, or if the disclosures fell short by describing what information was collected but not making it clear to EU consumers how it was used.

[1] PubMatic, Safe Harbor Organization Information, expires 7/13/14, http://safeharbor.export.gov/companyinfo.aspx?id=19503(viewed 8 Apr. 2014).

[2] PubMatic, "Safe Harbor Notice," http://www.pubmatic.com/safe-harbor.php (viewed 21 May 2014).

[3] PubMatic, "Privacy Policy," http://www.pubmatic.com/privacy-policy.php (viewed 16 June 2014).

[4] PubMatic, "Privacy Policy."

[5] PubMatic, "Opt Out," http://www.pubmatic.com/opt-out.php (viewed 16 June 2014).

[6] PubMatic, "RTB and Yield Optimization," http://www.pubmatic.com/rtb-yield-optimization.php (viewed 3 June 2014).

[7] "PubMatic Partners with Data Management Platform Lotame to Help Publishers Boost Engagement," 9 Apr. 2013, http://www.pubmatic.com/press/2013/PubMatic-Partners-With-Data-Management-Platform-Lotame-To-Help-Publishers-Boost-Engagement.php (viewed 30 Apr. 2014).

[8] "PubMatic Sets A New Standard In Mobile Data Enrichment," 11 June 2013, http://www.pubmatic.com/press/2013/PubMatic-Sets-A-New-Standard-In-Mobile-Data-Enrichment.php (viewed 30 Apr. 2014).

[9] "PubMatic Acquires Ad Serving Company Mocean Mobile," 19 May 2014, http://pubmatic.com/press/2014/PubMatic-Acquires-Ad-Serving-Company-Mocean-Mobile.php (viewed 3 June 2014).

Salesforce

Complaint number	25
Company profile	Salesforce is a global cloud computing company that, through mergers and acquisitions, has become a leader in data mining, consumer profiling, and targeted advertising.
Main website	www.salesforce.com/
Safe Harbor/privacy statements	Salesforce, which has been a Safe Harbor participant since 2002, says in its certification statement that it "acts as a data processor and does not determine how its customers' data is utilized in salesforce.com's servers"; nor does it "… choose or determine the types of data that are submitted to salesforce.com's servers, and any access to or use of such data by salesforce.com is incidental to completing the contractual obligations of salesforce.com, as data processor, to its customers." [1] The company also explains that "[a]s part of salesforce.com's internal operations, salesforce.com transfers personal data of its current and prospective customers and current and prospective business partners to salesforce.com's U.S. data centers for processing and storage,"—although it does not disclose what those "internal operations" might actually entail.[2] Nor does the company's privacy policy shed any more light on its Safe Harbor status, declaring simply that "Salesforce.com is also a certified licensee of the TRUSTe EU Safe Harbor Seal and abides by the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce and the European Union. Salesforce.com has certified that it adheres to the Safe Harbor Principles."[3] While Salesforce's privacy policy describes the information it collects from its own customers (for example, when they "… request additional information or register on salesforce.com's Web site …" or when they "… purchase salesforce.com's applications or services …"), it is silent on the data collected from consumers who might encounter Salesforce's products and services on third-party sites. Nor is any mention made of the "Indexed Content Privacy Statement," available on Salesforce's ExactTarget subsidiary (see complaint no. 14, above), which does disclose the kinds of data collected from consumers.[4] Opt-out from those services, moreover, is limited to third-party, cookie-based services that are limited to cookies on Salesforce's corporate website.[5]

Non-compliance/ false claims	Salesforce fails to explain (or even to acknowledge) the impact of its many corporate acquisitions (no less than 30 over the past 8 years), including such major recent purchases as Radian6 in 2011, Buddy Media in 2012, and ExactTarget in 2013 for a combined expenditure of nearly $3.5 billion.[6] Each of these companies was a significant force in online marketing before being acquired, and brought data-driven advertising practices to Salesforce that without question have had a major impact on its operations. ExactTarget is the subject of a Safe Harbor complaint detailed elsewhere in this filing (see no. 14, above), while Salesforce combined Radian6 with Buddy Media in its Social Studio product as part of the Salesforce ExactTarget Marketing Cloud. Radian6 had earlier earned notoriety with its social media surveillance tools for "listening" to consumers, measuring their "sentiment," seeing "who is doing the talking," and allowing companies to "monitor and respond to social conversations in near-real-time."[7] Buddy Media, similarly, enabled brands to embed their content within the social experiences of users, with a suite of products that included ProfileBuddy ("Easily create and deploy interactive content that is tailored to your global brand"), ConversationBuddy ("Track and guide your interaction with customers from first click to the shopping cart"), ReachBuddy ("Use social hooks to create and deploy content across the open web"), and a service that enabled marketers to create "50 social applications—'sapplets'—including sweepstakes, contests, quizzes, polls and commerce to create content tied to users' social and interest graphs on Facebook and Twitter."[8] The combination of these companies—now known as Radian6 Buddy Media Social Studio—"is a single platform for social content marketing, engagement, publishing and analytics, built for both enterprise scale and consumer ease of use, that allows marketers to collaborate like never before. … No other solution enables you to manage the entire customer journey. … With Radian6 Buddy Media Social Studio, we help marketers build 1:1 relationships that grow value for both the brand and the consumer."[9] In the process of acquiring and incorporating these various marketing resources, Salesforce has transformed itself, as the company reveals in describing its ExactTarget Marketing Cloud, "… the customer platform for 1:1 marketing—making it possible for marketers to create a single view of every customer, manage the customer

	journey, and deliver optimized content on every channel and every device. It empowers brands to connect with customers in entirely new ways through email, mobile, social, web, and even connected products."[10] "The world is changing," Salesforce proclaims, referring to the "… 50 billion connected devices on the Internet of Things" that will enable companies "… to connect to customers in entirely new ways through the next generation of devices, apps, and products."—and to mine all of the new data to be found in these connections.[11] Salesforce's has failed to update either its privacy policy or its Safe Harbor documentation to reflect this transformation and the expansion of data sets and capabilities that are so relevant to the privacy of EU consumers.
FTC action on possible violations	In light of all the changes that Saleforce has undergone in recent years, as its own technology has matured and as it has incorporated technology from other marketing companies, the FTC should investigate and sanction the company for deceptive omissions. It is not possible for a Safe Harbor participant to avoid compliance by claiming ignorance of the content of information it holds, and in any case Salesforce appears to be cognizant of the personal information it is wielding to create its products and target specific individuals. It has combined EU consumer data and determined the means of processing in ways sufficient to have responsibility under the Safe Harbor as a controller.

[1] Inconsistently with these disclosures, there is no Safe Harbor exception for parties that attempt to remain ignorant of whether their data are personal information or not.

[2] Salesforce, Safe Harbor Organization Information, expires 7/31/15, http://safeharbor.export.gov/companyinfo.aspx?id=24034 (viewed 11 Aug. 2014).

[3] Salesforce, "Privacy Statement, effective as of March 12, 2014," http://www.salesforce.com/company/privacy/full_privacy.jsp (viewed 21 May 2014).

[4] ExactTarget, "Salesforce.com Marketing Cloud Indexed Content Privacy Statement," http://www.exacttarget.com/privacy-policy/indexed-content-privacy-statement (viewed 13 July 2014).

[5] Salesforce, "Privacy Statement, effective as of March 12, 2014."

[6] Alex Williams, "With ExactTarget Acquisition, Salesforce.com Has Spent Close To $3.5 Billion To Get Into The Chief Marketing Officer's Suite," TechCrunch, http://techcrunch.com/2013/06/04/with-exacttarget-acquisition-salesforce-com-has-

spent-close-to-3-5-billion-to-get-into-the-chief-marketing-officers-suite/ (viewed 30 Apr. 2014).

[7] "Bigger Financial Institutions Need Better Social Media Tools," The Financial Brand.com, 20 Feb. 2012, http://thefinancialbrand.com/22377/monitor-social-mentions-crm-radian6/ (viewed 17 May 2014).

[8] Buddy Media, "Solutions," http://www.buddymedia.com/solutions; Patrick Stokes, "Buddy Media Launches ReachBuddy to Power Your Connections Across Social Networks and the Open Web," 18 Apr. 2011, http://www.buddymedia.com/newsroom/2011/10/buddy-media-launches-reachbuddy-to-power-your-connections-across-social-networks-and-the-open-web/ (both viewed 28 Oct. 2011).

[9] Marcel LeBrun, "Introducing Radian6 Buddy Media Social Studio," ExactTarget Blog, 6 May 2014, http://www.exacttarget.com/blog/radian6-buddymedia-socialstudio-launch/ (viewed 30 Apr. 2014).

[10] LeBrun, "Introducing Radian6 Buddy Media Social Studio."

[11] LeBrun, "Introducing Radian6 Buddy Media Social Studio."

SDL

Complaint number	26
Company profile	SDL provides software and service solutions for language translation purposes Through recent acquisitions, it has also become a supplier of marketing automation applications and services, including data profiling and personalized advertising.
Main website	www.sdl.com/
Safe Harbor/privacy statements	On the surface, at least, SDL's Safe Harbor certification would appear to be beyond reproach, in that the company explains that it is the recipient only of "Data … transfered [sic] to US based office for the purposes of language translation services."[1] The company's privacy policy is equally direct: "SDL complies with the US - EU Safe Harbor Framework and the US - Swiss Safe Harbor Framework as set by the U.S Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland and SDL has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement."[2] That privacy policy acknowledges the use of cookies to collect "Client Information" (e.g., IP address and GeoIP information), "Essential Technical Information" (e.g., type of browser and operating system used, page or service requested), "Nonessential Technical Information" (e.g., the URL of the page from which the user entered SDL's site), and "Optional Information" (e.g., registration information, including name and email address, as well as user responses to blog comment forms).[3] A separate "Cookie Policy" discusses SDL's use of session and profile cookies, as well as third-party cookies such as Google Analytics and DoubleClick Cookies."[4] Also, the company explains, "In addition to our use of technologies as described herein, we may permit certain third party companies to help us tailor advertising that we think may be of interest to you based on your use of SDL Sites and/or Services and to otherwise collect and use data about your use of SDL Sites and/or Services. For more information about this practice, please see the 'Third Party Advertising Technologies' section below,'" (although this section or document does not appear on this page or anywhere else on SDL's website).[5]
Non-compliance/	Also missing from SDL's Safe Harbor and privacy

false claims	statements is any mention of Alterian, the marketing analytics and social media monitoring company that SDL acquired in early 2012 (see complaint no. 5, above).[6] In light of its acquisition of Alterian—over a *month before* SDL's original Safe Harbor certification in March 2012—SDL's Safe Harbor statement concerning its receipt of data solely for "language translation services"—was *never* accurate. Compare it with Alterian's Safe Harbor statement: "Data can be uploaded to our servers for the purposes of sending targeted digital communications to the data subject via our e-mail distribution software. … Generally, Alterian will simply be maintaining the system that performs the delivery and will not have any direct interaction with the data."[7] The combination of these two systems makes both outdated Safe Harbor disclosures materially misleading. As SDL's website makes clear, the SDL Intelligent Marketing Suite now powered by Alterian technology goes far beyond "email distribution software" and consumer data with which the company purports to have no "direct interaction." SDL's redesigned Intelligent Marketing Suite now integrates three distinct products, including a data-mining and –analysis application (SDL Customer Analytics}; personalized advertising campaign management (SDL Campaign Manager), and email profiling (SDL Email Manager).[8] SDL has also added Alterian's social media monitoring tool (SM2) to its arsenal, enabling its clients to track conversations and profile individual consumers.[9] "By tracking purchases, marketing responses, surveys and social media conversations," SDL explains, "our customer analytics software enables marketers to understand individual customers and better meet their needs, creating relevant customer experiences and building brand loyalty."[10] None of this would have been possible without its acquisition of Alterian, which fundamentally changed the nature of SDL's business. Such partnerships as these, moreover, which bring detailed consumer data to bear on what might otherwise be relatively privacy-neutral automated ad-serving platforms, must be disclosed by self-certified Safe Harbor companies.
FTC action on possible violations	SDL should be investigated and sanctioned in light of its failure to present an accurate description of the company's global operations, and for making affirmative statements to

	consumers that are deceptive. By misleading consumers on the important aspects of data collection and analysis performed by the technology it acquired from Alterian and incorporated with its existing business, including Alterian's social media monitoring, SDL likely violates the Notice and Choice requirements of the Safe Harbor framework. The company's disclosures in its privacy policy that it may place cookies and collect "optional" data that is covered personal information do not meaningfully inform EU consumers about the uses of their data.

[1] SDL, Safe Harbor Organization Information, expires 3/4/15, http://safeharbor.export.gov/companyinfo.aspx?id=22139 (viewed 17 May 2014).

[2] SDL, "Privacy Policy," http://www.sdl.com/aboutus/privacypolicy.html (viewed 21 May 2014).

[3] SDL, "Privacy Policy."

[4] SDL, "Cookie Policy," http://www.sdl.com/aboutus/cookiespolicy.html (viewed 18 June 2014).

[5] SDL, "Cookie Policy."

[6] "SDL's Acquisition of Alterian Further Demonstrates SDL's Commitment to Drive the Global Customer Experience," 30 Jan. 2012, http://www.sdl.com/aboutus/news/pressreleases/2012/sdl-acquires-alterian.html (viewed 17 May 2014).

[7] Alterian, Safe Harbor Organization Information, expires 8/13/14, http://safeharbor.export.gov/companyinfo.aspx?id=19791 (viewed 17 May 2014).

[8] "Alterian is Now SDL, Continuing to Drive the Global Customer Experience," 30 Jan. 2012, http://www.sdl.com/campaign/alteriannews.html#tabs (viewed 17 May 2014).

[9] "Alterian is Now SDL, Continuing to Drive the Global Customer Experience," 30 Jan. 2012, http://www.sdl.com/campaign/alteriannews.html#tabs (viewed 17 May 2014).

[10] SDL, "Customer Analytics," http://www.sdl.com/products/customer-analytics/ (viewed 17 May 2014).

Spredfast

Complaint number	27
Company profile	Spredfast provides social marketing software that allows companies to manage, track, and analyze their social media programs, and to undertake data mining and consumer profiling operations on Facebook, Twitter, and other major social networks.
Main website	www.spredfast.com/
Safe Harbor/privacy statements	With regard to "Personal Information Received from the EU/EEA and/or Switzerland," Spredfast explains that it is "… an enterprise-class social media management system that allows an organization to manage, monitor, and measure its voice across multiple social media channels." What Spredfast fails to explain fully, however, is that by allowing a company to "monitor" its voice, it is enabling that client to follow consumers' social media conversations (via "Social Streams monitoring") and collect and assess personal information (e.g., interests, preferences, needs, and tastes) in the process (through "Analytic Metrics and Reporting"). "Certain visitors to Spredfast's websites," the company adds, "choose to interact with Spredfast in ways that require Spredfast to gather personally-identifying information," but again it is being disingenuous. No consumer is "choos[ing] to interact" with Spredfast to facilitate considerable information gathering, and it is not clear from this disclosure what such an interaction might entail or how one can avoid it. Not only is it unlikely that many consumers are fully aware of how much personal information Spredfast collects and how those data are stored and processed, the company also is not "required" to collect personally identifiable information (or to aggregate and analyze such data once they are collected).[1] As a result, the above disclosure is not helpful or meaningful for EU consumers. On its own website, the company simply notes that "Spredfast's Privacy Policy Statement conforms to the U.S.-EU and U.S.-Swiss Safe Harbor Privacy Principles developed by the U.S. Department of Commerce in coordination with European Commission and the Federal Data Protection and Information Commissioner of Switzerland: Notice, Choice, Security, Data Integrity, Access, and Enforcement. Spredfast complies fully with the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks to provide

	adequate protection for personal data from Europe as required by the European Union's Directive on Data Protection and by Switzerland's Federal Act on Data Protection."[2] Concerning its data-collection and usage practices, Spredfast's privacy policy also explains that > The amount and type of information that Spredfast gathers depends on the nature of the interaction. Those who engage in transactions with Spredfast are asked to provide additional information, including as necessary the personal and financial information required to process those transactions. In each case, Spredfast collects such information only insofar as is necessary or appropriate to fulfill the purpose of the visitor's interaction with Spredfast. > … Spredfast discloses potentially personally-identifying and personally-identifying information only to those of its employees, contractors and affiliated organizations that (i) need to know that information in order to process it on Spredfast's behalf or to provide services available at Spredfast's websites, and (ii) that have agreed not to disclose it to others. Some of those employees, contractors and affiliated organizations may be located outside of your home country; by using Spredfast's websites, you consent to the transfer of such information to them. Spredfast will not rent or sell potentially personally-identifying and personally-identifying information to anyone.[3] Spredfast does not offer any opt-out mechanisms on its site.
Non-compliance/ false claims	While Spredfast's Safe Harbor statement and its privacy policy are comparatively reticent on the topic of its social media marketing practices, the company's website and product literature are full of information on the range and power of its technology (which is compatible with Facebook, Twitter, LinkedIn, Google+, YouTube, and other social networks). Spredfast's social relationship platform (SRP) product, for example, extends beyond mere conversation monitoring to include "… planning, listening, engaging, content discovery, coordinating, measuring, archiving, security, and integrating with other business applications."[4] The company's data mining and consumer profiling services allow its clients to "[t]arget specific and

	customized audiences on Facebook, LinkedIn, and Google+ by selecting attributes like gender, education, age, location, job function, and seniority. … Import all social networks posts automatically to ensure a complete and measurable aggregation of social activity … [and] Identify influencers."[5] Spredfast's "… preferred partner status with Facebook, Twitter, LinkedIn and Google+," moreover, connects it "to the heart of the social networks and allows us to optimize the most robust capabilities in our platform."[6] It also represents, unfortunately, a significant threat to consumer privacy. Spredfast should also be required to disclose and discuss its recent merger with Mass Relevance, a social media marketer that has never participated in the Safe Harbor program.[7]
FTC action on possible violations	Because Spredfast's disclosures are vague to the point of being misleading, it fails to offer adequate Notice and Choice concerning the various ways in which it collects and analyzes consumer data from social networks. The company purports to monitor consumers and report back to its clients on their social media actions, while it tells consumers that it never sells their personal information and doesn't explain how it uses such data. FTC should investigate this company's data practices and disclosures to EU consumers in light of Safe Harbor duties.

[1] Spredfast, Safe Harbor Organization Information, expires 7/25/15, http://safeharbor.export.gov/companyinfo.aspx?id=23614 (viewed 11 Aug. 2014).

[2] Spredfast, "Privacy Policy," http://www.spredfast.com/privacy-policy/ (viewed 21 May 2014).

[3] Spredfast, "Privacy Policy."

[4] Spredfast, "Social Relationship Platform Checklist," http://info.spredfast.com/SRPChecklist.html (registration required).

[5] Spredfast, "Social Relationship Platform Checklist."

[6] Spredfast, "Who We Work Together," http://www.spredfast.com/who-we-work-with/ (viewed 18 May 2014).

[7] Cotton Delo, "Social-Marketing Startups Spredfast and Mass Relevance Merge," *Ad Age*, 2 Apr. 2014, http://adage.com/article/digital/social-marketing-startups-spredfast-mass-relevance-merge/292443/ (viewed 18 May 2014).

Sprinklr

Complaint number	28
Company profile	Sprinklr provides software and services that allow companies to undertake social media surveillance, by covertly monitoring social networks, collecting and analysing the data therein, and using those insights for personalized marketing.
Main website	www.sprinklr.com/
Safe Harbor/privacy statements	According to its Safe Harbor declaration, "Sprinklr is a social media management system … . The Sprinklr system is a tool that enables companies and organizations to process and manage publicly available information about their brand on the Internet. The system aggregates and saves a record of public information that is available about user interactions with a company or organization on the Internet."[1] Its privacy policy, meanwhile, offers what it calls "Sprinklr's promises to each Customer," based on the seven Safe Harbor Principles, including the following three items: 1) Notice. When Sprinklr collects your personal information, we give you timely and appropriate notice describing what personal information we are collecting, how we will use it and the types of third parties with whom we may share it. This notice is located in this policy. Sprinklr has advised its Customers to provide similar notice to their unique customers and partners of their use of the Sprinklr system. 2) Choice. Sprinklr will give you choices about the ways we use and share your personal information, and we will respect the choices you make. Please recognize that Sprinklr is a system used by Customers and, as such, we advise and encourage our Customers to take appropriate action with respect to their own privacy standards as it relates to social media management. 3) Relevance. Sprinklr will collect only as much personal information as is required to meet the specific, identified purposes of Customer contracts, and we will not use it for other purposes without obtaining your consent.[2]
Non-compliance/ false claims	However straightforward these statements might seem, it appears that Sprinklr, in practice, fails to provide sufficient Notice and Choice by obscuring the extent to which the

	company, for the purposes of targeted advertising, aggregates and analyzes massive quantities of social network communications (including non-publicly available information) and then links its findings to specific consumers. Neither its Safe Harbor documentation nor its corporate privacy policy makes these processes clear, although they are described in detail in Sprinklr's own product literature. Among the company's social media surveillance systems, for example, is a product called Social Engagement, which Sprinklr describes as "… a centralized communication hub for monitoring and responding to vast amounts of conversations across numerous social channels. We support Twitter, Facebook, LinkedIn, Google+, YouTube, Instagram, Foursquare, Flickr … ."[3] Sprinklr's Social CRM product allows companies to link their own first-party consumer records to data mined from "… hundreds of social channels" for a "… unified 360 profile views of your customers over time."[4] Sprinklr also links its clients to various third-party data sources for even more detailed consumer profiling. According to the company, "Sprinklr can integrate and communicate two-way with virtually any 3rd party or proprietary enterprise platform on the market while providing a consistent and seamless user experience."[5] Sprinklr's Social Listening Insights product, finally, "acts like a social 'central nervous system' tracking, listening to, and reacting to millions of social signals related to markets, customers, products, and competitors."[6] Such covert surveillance, while no doubt useful to marketers, is clearly inimical to consumer privacy. Moreover, Sprinklr should be required to disclose and discuss its recent acquisition of Dachis Group, whose "… big data social analytics platform monitors over 50 million social signals and 1 million brand advocates in real-time. Dachis Group delivers powerful insights by tracking, monitoring and helping manage conversations and content across 30,000 brands, 100 million social accounts, and an aggregate audience of 5.2 billion followers, fans, subscribers and contributors across dozens of the largest social platforms."[7] This acquisition likely adds to Sprinklr's disclosure duties under the Safe Harbor.
FTC action on possible violations	Because Sprinklr fails to offer adequate disclosures and opt-out mechanisms concerning the various ways in which it aggregates and analyzes consumer data from social

	networks, it should be investigated and sanctioned by FTC. The "vast amounts of social data" this company is processing and preparing for customers is not purely public information and it requires adequate protections as personal information, including meaningful Notice and Choice. Stating that you process personal information for "identified purposes of Customer contracts" is insufficient to comply with the Safe Harbor's command that purposes be spelled out clearly for consumers.

[1] Sprinklr, Safe Harbor Organization Information, expires 6/26/15, http://safeharbor.export.gov/companyinfo.aspx?id=23640 (viewed 11 Aug. 2014).

[2] Sprinklr, "Sprinklr Social Media Management System Privacy Policy," http://www.sprinklr.com/privacy/ (viewed 21 May 2014).

[3] Sprinklr, "Social Engagement," http://www.sprinklr.com/social-media-management-system/engagement/ (viewed 18 May 2014).

[4] Sprinklr, "Social CRM," http://www.sprinklr.com/social-media-management-system/social-crm/ (viewed 18 May 2014).

[5] Sprinklr, "Social Enterprise Integration," http://www.sprinklr.com/social-media-management-system/enterprise-integration/ (viewed 18 May 2014).

[6] Sprinklr, "Social Listening Insights," http://www.sprinklr.com/social-media-management-system/enterprise-social-media-listening/ (viewed 18 May 2014).

[7] Sprinklr, "Sprinklr Acquires Dachis Group," Experience Management Blog, 19 Feb. 2014, http://www.sprinklr.com/social-scale-blog/sprinklr-acquires-dachis-group/ (viewed 18 May 2014).

Turn

Complaint number	29
Company profile	Turn provides data and media management technologies that combine offline and online marketing data for the purposes of consumer profiling, tracking, and targeted advertising.
Main website	www.turn.com/
Safe Harbor/privacy statements	With regard to "Personal Information Received from the EU/EEA and/or Switzerland," Turn simply notes that it "… operates a technology platform that collects information that helps our clients deliver advertising to websites. The information that is collected and used on our platform is considered non-personally identifiable information in most jurisdictions."[1] Its Privacy Guidelines are equally straightforward in this regard—"Turn has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement"—although the company also includes the following statement concerning the collection of PII on its *own* site: "We collect Personally Identifiable Information ('PII' or 'Personal Information') from the Site ONLY when you choose to provide it to us."[2] It is not clear, however, that consumers can exercise such choice when they encounter Turn technology when it is deployed to collect personal information on other sites: Our technology collects information about the website(s) that a browser visits and the advertisements that a browser displays while online. You may encounter our technology when Turn or a Business Partner purchases online advertisements on a website that you visit, an app that you use, etc.; and/or when one of our Business Partners places one of our web beacons on a property that you visit or use. We use the information collected by our technology in order to help make the Turn Ads you see more relevant to you, and for ad delivery and reporting purposes. … Our technology also offers data management services to Business Partners (our 'Data Management Platform' or 'DMP'). The Turn DMP enables Business

	Partners to collect, store, and analyze information about a browser or a user which may include PII. We provide Business Partners with a self-serve website tagging technology ('Flextag') that enables them to place data into the DMP. We require Business Partners using the DMP to adhere to the NAI Code and DAA Code or other applicable industry standards. We also contractually require that Business Partners don't bring PII or sensitive Non-PII audience segments into the DMP. However, Business Partners' use of the DMP is subject to their own privacy policies, not this one. … Turn does not collect PII via our technology. If we discover that PII has been inadvertently collected by our technology (e.g., where a Business Partner has used Flextag to bring PII into the DMP), we will take reasonable steps to attempt to remove the PII and to address the situation with the party responsible for such inadvertent collection. … Turn uses this information to analyze trends, identify the audience most likely to respond to an advertisement, and to tailor ads using only Non-PII.[3] Turn also maintains an opt-out page (laden with such caveats as "Opting out may hurt the sites and apps you love!" and "[I]f you opt out, you may be making it harder for your favorite websites or apps to survive"), based on its own as well as third-party opt-out mechanisms (Network Advertising Initiative, Digital Advertising Alliance, and Digital Advertising Alliance EU).[4]
Non-compliance/ false claims	Regardless of how reassuring its Safe Harbor and privacy statements may be to those in the EU and Switzerland, an examination of Turn's own product literature raises doubts about the adequacy of the Notice and Choice that it provides European consumers. Simply put, the extent of Turn's data-collection practices, and the range of partners it has enlisted in those efforts, call into question the company's purported compliance with the U.S.-EU and U.S-Swiss Safe Harbor Frameworks. Turn's data-driven consumer profiling operation "… makes nearly 100+ billion advertising decisions, analyzes over 1.5 trillion customer attributes, and provides instant access to billions of marketing data points" every day.[5] But Turn's Cloud Marketing Platform also integrates vast amounts of third-party consumer data, enabling its

	clients to overlay "… third-party data, offline data, and data from multi- channel media campaigns, then feed it back into your audience targeting plans for immediate action. … Turn has an extensive open marketplace of more than 50 third-party data providers. Take advantage of these partner relationships to explore more audience data, blend it with your own, and generate rich composite views of your audiences."[6] Having "… pre-integrated more than 100 of the best data, inventory, and technology providers throughout the marketing ecosystem," the "Turn Cloud Marketing Platform brings all your marketing data into one place—your single source of truth—and converts it into valuable insights, actions, and results. … The Turn platform responds within ten milliseconds to audience events online, so your segments adjust instantaneously as customers make a purchase, visit a web page, or interact in any way with digital channels. And because the Turn platform reaches more than 50 percent of Internet users, you can be sure you're pulling in plenty of data every moment of every day."[7] "The foundation of Turn software is our Cloud Marketing Platform,"the company explains. "Built with massive processing power and tremendous reach and scale, it's what digital advertising requires. Our lightning-fast database crunches mountains of data in milliseconds to give you the kind of real-time insights that lead to unreal advertising results. Every month, highly specialized proprietary algorithms, developed by our applied scientists, evaluate more than 1,000,000,000,000 ad impressions from global inventory partners—representing between 75% and 80% of the programmatic mobile, social, and display impressions available in the world. Data centers on three continents provide service stability and reliability."[8] On several fronts, then, Turn's capabilities threaten EU citizen and consumer privacy.

FTC action on possible violations	Because Turn fails to offer adequate information concerning the various ways in which it collects and analyzes consumer data, FTC should investigate and sanction the company. The information it is working with is personal information within the meaning of the Safe Harbor, and suggesting the opposite (i.e., that no PII is collected and used) to EU consumers is deceptive. Moreover, a company that is processing data from over half the world's internet users and serving that to customers in something described "your single source of truth" is not engaged in mere processing. Turn is exercising controller authority over huge amounts of EU consumer personal information, and so the failures of Notice and Choice referred to above are both material to EU consumers and affect a huge proportion of them.

[1] Turn, Safe Harbor Organization Information, expires 1/20/15, http://safeharbor.export.gov/companyinfo.aspx?id=21561 (viewed 20 May 2014). As discussed in attached legal analysis, neither the Safe Harbor nor EU law are jurisdictions that fall under such a permissive standard.

[2] Turn, "Privacy Guidelines," updated 26 Feb. 2014, http://www.turn.com/privacy (viewed 20 May 2014).

[3] Turn, "Privacy Guidelines."

[4] Turn, "Consumer Opt-Out," http://www.turn.com/privacy/customer-opt-out (viewed 18 June 2014).

[5] Turn, "Technology: Ingenuity That Delivers," http://www.turn.com/whyturn#technology (viewed 20 May 2014).

[6] Turn, "Audience Suite," http://www.turn.com/our-products (viewed 20 May 2014).

[7] Turn, "Ecosystem: Point and Click Access to 100+ Marketing Technology Solutions," http://www.turn.com/whyturn#ecosystem; Turn, "Platform: Your Single Source for All Marketing Data," http://www.turn.com/whyturn#platform (both viewed 20 May 2014).

[8] Turn, "Amplify," June 2013, http://www.turn.com/sites/default/files/TURN_brochure_print_LR_1.pdf (viewed 20 May 2014).

Xaxis

Complaint number	30
Company profile	Xaxis (which is owned by global ad giant WPP) is a media company focused on targeted advertising across a variety of digital platforms, through data mining, analytics, and detailed consumer profiling.
Main website	www.xaxis.com/
Safe Harbor/privacy statements	According to its Safe Harbor statement, Xaxis "… provide[s] technology and services that enable us and our clients use [sic] to buy, sell, and deliver online advertising. through [sic] the collection, analysis and use of non-personally identifiable information, including such information as browser version, cookie id, page visited, date and time, and IP address. We serve clients and buy, sell and deliver advertising globally, including in the US and the EU."[1] The privacy statement that it offers on its corporate website includes two specific references to EU privacy standards: • "Please note that in some countries an IP address is considered personal data by applicable law. If we conduct business in such countries and we know that you are located in such a country, we will treat your IP address as personal data. In such countries we interpose a 'black box' that is operated by an independent third party and that separates the user's IP address from other data we collect."[2] • "Xaxis for Publishers LT (formerly known as 24/7 Open AdStream LT), a service we primarily provide in Europe, places a cookie on your computer for the purpose of interest-based advertising as described above. This service was certified with the TÜV Trusted IT Data Privacy Certification Seal on January 24, 2013. You may opt out of interest-based advertising through the Xaxis for Publishers LT service by following the instructions in the section titled 'User Choice.'"[3] The Xaxis privacy policy also discusses its data-collection and usage practices, as follows: When you view and interact with websites and advertisements operated by our clients (and, in some cases, by our clients' clients), we may collect through our Services information regarding your browsing, usage and interactions. We may also collect information that allows us to identify browsers we have interacted

	with previously. Such information collected by our Services may include the type of Internet browser and computer operating system you use, your computer's Internet protocol ("IP" address), the URLs of the websites you visited before and after viewing an advertisement, and information related to websites and web pages you are viewing. We do not collect users' names, mailing addresses, phone numbers, email addresses or similar personally identifiable information. Whenever we refer to "you" or "your", we are referring to a browser or device and not an identifiable person. … We use the information collected through our Services to provide you with the most useful and relevant online advertising and to better customize the sort of advertisements you see on those sites. For example, if we think that a user is interested in apparel options, then our Services may help our clients deliver interest-based online advertisements to you about a particular type of apparel. We also may use such information to limit the number of times you see a particular ad, and for other purposes such as research, reporting and analysis. We may also receive from other companies information collected outside the Services for use in connection with the Services on behalf of our clients. We also do this in order to get a clearer picture of the types of advertisements that might be most relevant and useful to you. We do not associate such information with your name, mailing address, email address or similar personally identifiable information. We require our clients to comply with applicable laws governing online privacy. We encourage you to read the privacy policies of the websites you visit to better understand issues relating to your online privacy.[4] Xaxis also provides its website visitors a one-step process to "opt out of receiving our customized third-party advertisements," and requires its "… Xaxis Publisher Network (formerly 24/7 Access) clients to inform users about their privacy and information collection practices via their privacy policies and to include in their privacy policies information regarding the use of third-party advertising technology and services on their sites, the types of data collected through such services, the use and

	distribution of such data, and a link to an industry opt-out from interest-based advertising."[5]
Non-compliance/ false claims	Despite these measures, it is doubtful that EU consumers, who are most likely to encounter Xaxis technology as it is deployed on third-party sites, will be apprised of the full power and scope of Xaxis's consumer profiling and ad-targeting practices.[6] Xaxis's corporate slogan—"We Believe In Building A Better Experience By Knowing a Little Bit About Our Users"—barely touches on the true nature of those practices, which generate quite a lot of knowledge about users. Xaxis' data profiling has grown even more extensive with the company's integration into Facebook Exchange in September 2012, and its December 2013 merger with 24/7 Media:[7] Concerning the former, Xaxis explains that its "… Social Analytics Suite provides its advertisers with the opportunity to buy Facebook display inventory, enabling seamless coordination between their Facebook ad buys and the rest of their digital media spend. … FBX allows advertisers to utilize outside data resources in directing their Facebook ad buys and, through Xaxis, clients will be able to leverage both first- and third-party data to make more informed choices."[8] Xaxis' data management platform (DMP), similarly, "[a]llows advertisers to have one seamless conversation with their audience members across 6 channels," while its new Turbine DMP "… represents an evolution in the data management platform (DMP), an area that we invented for this industry seven years ago. As a data creation engine, Turbine provides advanced real-time audience segmentation capabilities to fuel the Xaxis product offerings. … [It] [i]nstantly responds to changes from more than 2 trillion anonymous data points."[9] Its merger with 24/7 Media, meanwhile, "… forming what will be the world's largest programmatic media and technology platform," poses enormous threats to consumer privacy: "The combined company, which will be known as Xaxis, brings together over 800 data and technology experts to help advertisers and publishers engage with audiences across all digital devices and channels. The new Xaxis will use its proprietary audience platform to programmatically manage over $750MM of audience-targeted media for more than 2,700 clients around the globe. … Combined the two companies will manage 2 trillion impressions annually across the world."[10]

	As with so many data-driven marketing companies, Xaxis' Data Management Platform (DMP) is very much a collaborative effort, gathering "… information across multiple online and offline channels" allowing "… advertisers to have one seamless conversation with their audience members across 6 channels," and connecting "… all online and offline data sources."[11] The company has also moved aggressively into the mobile arena, enabling its clients to "… integrate with consumers as they engage with their favorite sites and apps, and hone in on your ad's viewers via our hyper-local and interest targeting."[12]
FTC action on possible violations	Because Xaxis claims to use non-personal information that is personal information within the Safe Harbor definition, and despite small measures to separate IP addresses from other user information, the company's disclosures fall short of providing adequate Notice. Its disclosures suggest that it can't identify individuals, but then also hint at the fact that it is building advertising profiles on individuals using third-party data—which is not a clear statement of the company's purposes or data uses that EU consumers can understand. It is also questionable if its Choice opt out is effective, clearly explained, or if consumers can find it when they are interacting with Xaxis through clients (or "our clients' clients") like Facebook. The company's uses of Facebook, hyper-local tracking, and offline data to profile consumers are highly questionable, and FTC should investigate Xaxis for Safe Harbor violations and sanction it accordingly.

[1] Xaxis, Safe Harbor Organization Information, expires 1/11/15, http://safeharbor.export.gov/companyinfo.aspx?id=21481 (viewed 18 May 2014).

[2] Xaxis, "Xaxis Privacy Policy," http://www.xaxis.com/static/view/privacy-policy (viewed 21 May 2014).

[3] Xaxis' privacy policy also includes the industry-standard Safe Harbor endorsement: "We comply with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework, as set forth by the U.S. Department of Commerce, regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. We have certified that we adhere to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement. To learn more about the Safe Harbor program, and to view our certification, please visit http://www.export.gov/safeharbor/." Xaxis, "Xaxis Privacy Policy."

[4] Xaxis, "Xaxis Privacy Policy."

[5] Xaxis, "Xaxis Privacy Policy."

[6] Alexa, "xaxis.com," http://www.alexa.com/siteinfo/xaxis.com (viewed 21 May 2014).

[7] Xaxis, http://www.xaxis.com/#sthash.s3yWYeWa.dpuf (viewed 21 May 2014).

[8] "Xaxis Debuts Comprehensive Ad Buying and Analytics Solution With Support for Facebook® Exchange, Facebook's New Real-Time-Bidding System," Reuters, 13 Sept. 2012, http://www.reuters.com/article/2012/09/13/idUS119328+13-Sep-2012+BW20120913 (viewed 21 May 2014).

[9] Xaxis, "Xaxis Data Management Platform (DMP)," http://www.xaxis.com/products/view/xaxis-data-management-platform-dmp; Xaxis, "Turbine: The Next Generation in the Data Management Platform," http://www.xaxis.com/products/view/turbine (both viewed 17 July 2014).

[10] "Xaxis and 24/7 Media to Merge, Creating the World's Largest Programmatic Media and Technology Platform," 3 Dec. 2013, http://www.wpp.com/wpp/press/2013/dec/03/xaxis-and-247-media-to-merge/ (viewed 21 May 2014).

[11] Xaxis, "Xaxis Data Management Platform," http://www.xaxis.com/products/view/xaxis-data-management-platform-dmp (viewed 21 May 2014).

[12] Xaxis, "Xaxis Mobile," http://www.xaxis.com/products/view/xaxis-mobile (viewed 21 May 2014).