Executive Summary

This request for investigation arises from research by the Center for Digital Democracy (CDD) and its ongoing investigation of data marketing and profiling companies that have joined to the U.S.-EU Safe Harbor framework, as developed by the U.S. Department of Commerce (DOC) and formally accepted by the European Commission (EC). These 30 companies (data marketing and profiling companies) are similar in that they collect, use and share EU consumers' personal information to create digital profiles about them, analyze their behavior, and use the data to make marketing and related decisions regarding each of them. While these companies are largely unknown to EU citizens, they pride themselves on knowing everything about individuals and how to comprehensively profile and target them. The commercial surveillance of EU consumers by U.S. companies, without consumer awareness or meaningful consent, contradicts the fundamental rights of EU citizens and European data protection laws, and also violates the intention of the Safe Harbor mechanism to adequately protect EU consumers' personal information.

This filing is intended to provide the Federal Trade Commission (FTC) with factual information and legal analysis on probable violations of Safe Harbor commitments that materially mislead EU consumers. FTC should investigate these companies' practices using its subpoena authority and other methods of investigation. When FTC holds these data marketing and profiling companies' practices up against their public statements to DOC and consumers, it seems likely (based on how these companies differently describe themselves to clients) that the agency will find numerous deceptive misstatements. If such violations are found, FTC should make sure these companies cannot continue in the Safe Harbor program without first addressing all violations, and submitting to active oversight.

Among the companies covered are data broker companies with reams of for-sale sensitive information on individual consumers, data management platforms that allow customers to rapidly analyze their own consumer information and combine it with outside data sources to produce marketing insights, and mobile marketers that track devices and tie them to user profiles so as to sell advertising customers the most profitable consumers' attention. The 30 companies cited in CDD's filing include Acxiom, Adara Media, Adobe, Adometry, Alterian, AOL, AppNexus, Bizo, BlueKai, Criteo, Datalogix, DataXu, EveryScreen Media, ExactTarget, Gigya, HasOffers, Jumptap, Lithium, Lotame, Marketo, MediaMath, Merkle, Neustar, PubMatic, Salesforce.com, SDL, SpredFast, Sprinklr, Turn, and Xaxis.

Privacy is at risk because these data marketing and profiling companies, through the use of unique identifiers and sophisticated tracking and analysis, create detailed digital dossiers of EU consumers—even in the absence of certain traditional types of personal information (such as a name or government identification number). They use such data sources as public records, census data, online tracking technologies, consumer trailing through mobile devices (following users both in the physical world and online), and many

other sources. These companies add to this information through a variety of data sources, which can include sensitive information such as addresses, past purchase history, income, demographics, and family structure. A common feature of the business practices of nearly all the companies cited in this complaint is the involvement of an array of third-party data brokers and other information providers, who supply rich data sets used for the profiling and targeting of EU consumers. All of the companies, we believe, fall far short of the commitments they have made under the Safe Harbor.

According to Safe Harbor certification commitments to DOC, these data marketing and profiling companies have pledged to follow higher standards of transparency, consumer choice, and data security than are normally required by American law. In order to do business in the EU these companies have committed to clearly inform EU consumers of the purposes for which their personal information is processed, where it goes in the data processing ecosystem, and how individuals can opt out before their information is shared or used in a way beyond their initial consent. These principles (called Notice, Choice, and Onward Transfer in the Safe Harbor and this request) are minimum standards the EC approved for these companies to avoid the absolute prohibition on data transfers laid out in the EU's Data Protection Directive of 1995. In order to rise to "adequacy" sufficient under that law, the companies commit to the Safe Harbor principles, and for the Safe Harbor to function properly there must be active enforcement of these promises by a public authority. That authority is FTC, and its legal authority to punish misrepresentations is established under Section 5 of the FTC Act.

In a May 2014 report, FTC found that a group of companies (data brokers) similar to those cited in this filing operate with limited transparency and hide their real activities from consumers because of leeway in their under-regulated industry. The issues with data brokers identified by that report apply to the companies outlined in this request, many of which operate (at least some of the time) as data brokers. In fact, FTC's broad findings seem to apply to most of the companies analyzed here, even if they are not formally "data brokers," because profiling consumers and providing their information to advertisers is at the center of these companies' business. FTC found that data brokers did not give consumers effective disclosures, opt-outs, or contractual protections of privacy when they sold their data on to other companies. These three problems FTC identified are likely to constitute violations of Safe Harbor commitments of Notice, Choice, and Onward Transfer.

This request for investigation encourages FTC to open inquiries on all of these companies under three related patterns of deception:

1. **Companies are misstating their actual purposes and practices of data collection and use.** As evidenced in the summaries of each company, many of the data marketing and profiling companies have made insufficient disclosures and omitted material information in, for example: listing types of data that might be collected while making no mention of the actual uses that the personal information is subject to. As FTC found in its data broker report, these companies

fail to give consumers transparency (i.e. Notice) because any disclosures they make are on websites that consumers cannot readily find, while data collection occurs on other websites and through offline sources like public records. As FTC also found in its data broker report, these companies provide ineffective opt-out features (i.e. Choice) because the companies often continue to sell and use consumers' data after they opt out, either using the data for non-marketing purposes or aggregating the individual's profile data into other products with more consumers—collection of personal information does not cease, however. As FTC additionally found in its data broker report, the companies it looked at were careful to control their own intellectual property (datasets on consumers) with contracts but were not similarly careful to check what commitments their data source companies had made that they, as recipient companies, had to abide by (all data brokers investigated contractually limited use of their own data downstream, but only one data broker made a cursory investigation of the websites of companies from which it received information to see what that company told consumers)—and as a result EU consumer data is leaking to third-party companies without any safeguards that these Safe Harbor companies should insist on before such transfers (i.e. Onward Transfer). The indicia of violations that CDD found in this respect require the FTC use its subpoena power to find out exactly how inaccurate the privacy disclosures and DOC Safe Harbor declarations these companies have made actually are, considering such information as their contracts with data sources and data customers, and confidential data processing practices.

2. **Companies are misrepresenting legal facts of importance to EU consumers.** Both in stating that information they are using has been anonymized, and disclaiming responsibility as data controllers, these companies mislead EU consumers who have specific understandings of "anonymous" and "data controller" in their data protection regime. This is material because consumers cannot protect their legal rights if they have been misled to believe that their rights do not apply to a particular company. These companies are redefining terms of significance from EU law and the Safe Harbor, and in contradicting the definitions of the Safe Harbor framework they are violating their promise to DOC and concurrently misleading consumers. Moreover, FTC's enforcement authority normally takes into consideration the perception of a targeted group of consumers—Safe Harbor declarations to EU consumers that misstate data marketing and profiling companies' duties under EU law are materially deceptive to the EU consumers to which they are directed.
3. **Companies have merged with and acquired other companies, expanded their data collection and profiling capabilities, changed their entire corporate structure and business plan, but not updated their Safe Harbor disclosures or made clear to consumers their ongoing duties to protect personal information.** In spite of the clear order of the Safe Harbor's FAQ 6,

many of the data marketing and profiling companies have merged with others and increased their use of EU consumer personal information without making this change clear to DOC and the impacted consumers. FAQ 6 states that *before* a merger these companies must seek clearance from DOC, and provide a plan for keeping personal information secure in the new entity—companies with outdated documentation who have already merged are failing in a Notice duty to EU consumers whose information was collected pre-merger, as well as those whose information will be collected in the future.

In the interest of effectively administering the Safe Harbor, as it is concurrently under review and possible suspension by the EC, FTC has a clear duty to enforce the framework against companies that demonstrate a pattern of violation despite self-certification and claims to abide by the principles. FTC should open investigations on these data marketing and profiling companies and stand by its enforcement commitments made when the Safe Harbor was first approved, as well as FTC commissioners' ongoing assurances of the validity and importance of such enforcement.