Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	**)**
Request for Investigation of 30 Companies'	**)**
Violation of the U.S.-EU Safe Harbor	**)**
Program	**)**

REQUEST FOR INVESTIGATION

Submitted by
Center for Digital Democracy

The Center for Digital Democracy (CDD) respectfully submits this request for investigation to the Federal Trade Commission (FTC) based its oversight of the U.S.-EU Safe Harbor framework (the Safe Harbor) under its FTC Act Section 5 authority.[1] CDD is a national nonprofit, nonpartisan organization dedicated to promoting responsible use of new digital communications technologies, especially on behalf of children and their families. The Safe Harbor requires participating companies to provide sufficient disclosures under the program to give EU consumers sufficient notice of company privacy practices, and choice to opt-out of new data use and transfer, as defined by standards set by the Department of Commerce (DOC) and approved by EU authorities. When companies fail to abide by the Safe Harbor transparency principles they are in violation of these commitments and subject to FTC Act enforcement. CDD has a strong interest in ensuring that FTC enforce meaningful Safe Harbor standards, which are currently being treated as a paper exercise by the American data-driven marketing industry. In order to protect EU consumers and bring the enforcement of the Safe Harbor in line with its intended purposes, FTC must open investigations into companies that make insufficient and misleading statements to consumers and DOC.

Chairwoman Ramirez recently stated that FTC: "welcome[s] any substantive leads provided to us, such as the complaints we received . . . alleging a large number of Safe Harbor-related violations. . . . You can expect to see more enforcement actions on this front in the coming months."[2] FTC is the primary and central enforcer of the Safe Harbor, the Chairwoman made clear

[1] Due to a 2006 amendment to FTC's Section 5 authority, Congress has made clear that the agency is fully empowered to enforce cases that threaten U.S. exports regarding "foreign victims" in cases which "involve material conduct occurring within the United States." *See* 15 U.S.C. § 45(a)(3)(A)(ii), (a)(4)(A)(ii), & (a)(4)(B). Hence, "[i]n the cross-border context, the FTC has jurisdiction to protect consumers worldwide from practices taking place in the United States." FTC, Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework 2 (Nov. 12, 2013), http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf.

[2] FTC Chairwoman Edith Ramirez, Keynote Address Trans Atlantic Consumer Dialogue Multi-Stakeholder Dialogue on the Transatlantic Trade and Investment Partnership 8 (Oct. 29, 2013), *available at*

"in the FTC's hands, Safe Harbor is an effective and functioning tool for the protection of the privacy of EU citizens' data transferred to the United States."[3] This submission is in line with FTC's public commitment to increase investigations and enforcement to preserve such effectiveness.

After investigating 30 companies (data marketing and profiling companies) that 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, CDD's research has revealed that these companies are potentially misleading EU consumers in violation of Safe Harbor commitments. In mandatory disclosures to consumers, these companies omit important information about the data practices under which personal information is processed. Moreover, the companies mislead EU consumers by misstating their legal status and the legal status of data they process. Finally, a subset of these companies have merged with others without making clear to consumers how their already-collected data will be protected or deleted going forward. These 30 data marketing and profiling companies merit being investigated for possible violations of commitments they made under the Safe Harbor.

I. CONTEXT OF THE SAFE HARBOR, AN EXCEPTION TO EU LAW

Data protection regarding personal information is central to EU consumer protection. Indeed, it is a fundamental right for EU citizens, established by EU treaties and meant to be guaranteed in every Member State's law.[4] In 1995 the EU passed Directive 95/46/EC of the European Parliament and of the Council, "on the protection of individuals with regard to the processing of personal data and on the free movement of such data,"[5] (Directive 95/46/EC or the Directive) which is meant to protect natural persons' right to privacy.[6] Data controllers who collect the information of EU consumers must comply with EU Member States' data protection laws, enacted pursuant to the Directive.[7] The Directive has been interpreted in the years since it was

http://www.ftc.gov/sites/default/files/documents/public_statements/protecting-consumers-competition-new-era-transatlantic-trade/131029tacdremarks.pdf.

[3] *Id.* She also reiterated these points directly to the EU's authority on fundamental rights, Justice Commissioner Viviane Reding. *See* Letter to Viviane Reding, European Commission Vice President in charge of Justice, Fundamental Rights and Citizenship (Nov. 12, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/letter-chairwoman-edith-ramirez-expressing-federal-trade-commissions-commitment-protecting-consumer/131112europeanvivianeredingletter.pdf.

[4] *See* EU Treaty on the Functioning of the European Union, Official Journal of the European Union C 326/47, art. 16, (Oct. 26, 2012), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN (requiring the EU bodies to lay down standard rules for data protection applicable across the Member States); EU Charter of Fundamental Rights, Official Journal of the European Union C 83/389, arts. 7 & 8, (Mar. 30, 2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF (describing the right to privacy and right to have personal information protected).

[5] Directive 95/46/EC, of the European Parliament and of the Council, 1995 O.J. (L 281, 23.11.1995, p. 31), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01995L0046-20031120&from=EN (as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003).

[6] Case C‑131/12, Google Spain SL v. Agencia Española de Protección de Datos, para. 3, 13 May 2014, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=255042.

[7] *Id.*

passed and there is a body of relevant data protection law, including opinions by an expert body created by Article 29 of the Directive.[8]

Recently, the European Court of Justice (ECJ) ruled that under the Directive, profiling individuals by compiling information about them online is highly dangerous to fundamental rights, especially privacy rights.[9] Speaking about Google, the ECJ continued: "In the light of the potential seriousness of that interference [with fundamental rights], it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing."[10]

1. Transfers prohibited without adequate protections, oversight

Within the Safe Harbor U.S. companies can gather and use EU consumer information. The Directive, in Article 25(6), allows the European Commission (EC) to determine that a country has "adequate" privacy protections, and under Article 25(1) EU Member States are forbidden from allowing the transfer of personal information to countries that do not have such adequate protections in place.[11] Without finding the full U.S. legal system adequate, in July of 2000 the EC approved the DOC's resubmission[12] of Safe Harbor principles, the standards under which certain U.S. companies can voluntarily self-certify and thereby be deemed in compliance with Directive 95/46/EC.[13]

Approval was not unconditional. The EC decided to approve DOC's Safe Harbor principles and FAQs as adequate taken as a whole,[14] including enforcement assurances by DOC, FTC, and the Department of Transportation.[15] The EC's approval only allows transfers to companies who say they will comply with the Safe Harbor framework, and only those who are subject to oversight by agencies "empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality."[16] As a result, FTC enforcement on behalf of EU consumers is a necessary precondition[17] to which all Safe Harbor data marketing and profiling companies must submit.

The agreement between the EC and DOC is only in force as long as the EC supports it. Even at the beginning criticism and dissent in the EU was unmuted when the EC approved the

---

[8] *See* Directive 95/46/EC, *supra* note 5, arts. 29–30.

[9] Case C‑131/12, Google Spain SL v. Agencia Española de Protección de Datos, *supra* note 6, para. 80.

[10] *Id.* para. 81.

[11] Directive 95/46/EC, *supra* note 5, art. 25. The definition of adequacy is laid out in Article 25(2).

[12] An earlier draft was sent over for comment and was criticized by EU authorities, including the Article 29 Working Party. See *infra* note 18 for discussion of some of this pushback by EU data protection experts.

[13] *See* Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance) (2000/520/EC) (OJ L 215, 25.8.2000, p. 7) Corrigendum, OJ L 115, 25.4.2001, p. 14 (2000/520/EC) *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02000D0520-20000825&from=EN.

[14] *Id.* para. 5.

[15] *Id.* art. 1(1).

[16] *Id.* art. 2.

[17] *See also id.* Annex I ("its failure to comply with such self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts . . .").

Safe Harbor.[18] Initial approval was understood to be reviewable as technology developed and EU leaders gained experience with the system and its privacy protections.[19] The EC has reserved the right to change its approval "at any time" based on experience with the framework, changes in U.S. law, and the level of protectiveness of the Safe Harbor.[20]

Unlike other "Safe Harbor" self-regulation systems that might shield participants from government scrutiny, this one is merely a necessary certification for doing business and not a stand-alone self-regulatory regime. Companies join it voluntarily, and thereby bind themselves to abide by Safe Harbor standards that gain the force of law through FTC enforcement actions. Such actions by public authorities are a necessary part of the Safe Harbor, satisfying one of the EC's conditions in approving this program.

2. Safe Harbor now under EC review

Threat of revocation or amendment of the Safe Harbor was made definite and imminent in November 2013 when the EC highlighted strengthening the Safe Harbor as a necessary step in reestablishing trust in EU-US data flows.[21] "Making Safe Harbour safe" was one of six actions the EC asked of US leaders.[22] Although presented as suggestions, the EC announcement shows the EU will not accept business as usual in the future. In the case of systemic failure the EC will adapt or suspend the Safe Harbor, "for example if a body responsible for ensuring compliance with the Safe Harbour Privacy Principles in the United States is not effectively fulfilling its role."[23] Among the thirteen recommendations the EC provided for improving the Safe Harbor were: for all participating companies to have transparent privacy policies; to make privacy agreements with third-party recipients of data transparent; as well as active "ex officio" investigations of a portion of the participating companies, to check for noncompliance.[24] FTC stands in the best position to demonstrate industry compliance through investigation and enforcement.[25]

---

[18] The EC's approval of the Safe Harbor took into account the Article 29 Working Party's criticisms, seven reports in total, of the initial submission by the Department of Commerce. *Id.* para. 10 and accompanying footnote. Significantly, the Article 29 Working Party's criticism of an earlier DOC proposal emphasized that a Safe Harbor would only be acceptable if there was vigorous oversight and enforcement by a public body, such as FTC, and that consumer choice had to be construed strictly as the entire US system hinged on effective consumer choice. *See* Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Opinion 7/99: On the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce*, 5146/99/EN/final, 14 (Dec. 3, 1999), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp27en.pdf. Additionally, the EC approved the proposal despite the fact that the European Parliament thought that improvements still needed to be made in the proposed Safe Harbor framework. Commission Decision of 26 July 2000, *supra* note 13, para 12. These concerns continue into the present day, and the Safe Harbor is facing headwinds due to insufficient regard for enforcement and consumer choice.

[19] *See* Commission Decision of 26 July 2000, *supra* note 13, para. 9.

[20] *Id.* art. 4.

[21] Press Release, European Commission, Restoring Trust in EU-US data flows - Frequently Asked Questions 1 (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.pdf.

[22] *Id.*

[23] *Id.* at 3.

[24] *Id.* at 4 (see recommendations 1, 3, and 8).

[25] Since the recommendations regard both DOC and FTC, it is not for one agency alone to implement them. Nevertheless, it is a bad sign for the future of the Safe Harbor that a DOC representative is on record saying that

Indeed, FTC Commissioner Julie Brill has told EU leaders that active FTC enforcement is the basis on which Safe Harbor should not be revoked.[26] Also, in remarks to the European Institute she has described enforcing the Safe Harbor as a "critical role" and a "top enforcement priority" of the agency.[27]

Such assurances must be backed up by action, even after DOC and the EC's review of Safe Harbor is completed, since the EU still looks upon data transfers to U.S. companies with suspicion. EU experts have condemned the surveillance of EU citizens by American companies and the government,[28] and the political fallout of recent spying revelations have caused the EU Parliament to pass a resolution requesting "immediate suspension" of the Safe Harbor.[29]

II. FTC'S COMMITMENT AND ROLE AS ENFORCER

Without enforcement Safe Harbor cannot protect consumers as intended and it will fail. The EC explicitly reserved the right of Member States to cut off Safe Harbor company data flows in justifiable circumstances.[30] After that, the EC can contact DOC and suspend or limit the Safe Harbor.[31] Real consequences for American industry can therefore flow from a lack of enforcement. FTC recognized this issue and committed to solving it at the outset. The Safe Harbor framework

---

though DOC plans to implement many of the EC suggestions it will not result in significant regulatory change for Safe Harbor participants. Reuters, *U.S.-EU data privacy rules won't cause regulatory headache: official*, YAHOO NEWS, May 12, 2014, http://news.yahoo.com/u-eu-data-privacy-rules-wont-cause-regulatory-223540226--finance.html. Ted Dean, Deputy Assistant Secretary for Services, indicated that companies would be allowed to continue with much the same practices under DOC's envisioned changes. *Id.* This seemingly would not "make Safe Harbor safe" under the EC's substantive demands for reform, and the burden of reinforcing Safe Harbor before it is revoked falls to FTC enforcement.

[26] Stephen Gardner, *U.S. Officials Respond to EU Concerns Over Safe Harbor Data Transfer Program*, BLOOMBERG BNA, Dec. 16, 2013, http://www.bna.com/us-officials-respond-n17179880742/ ("Commissioner of the Federal Trade Commission Julie Brill said that the Safe Harbor program is 'a very effective tool for protecting the privacy of EU consumers,' and it shouldn't be suspended or renegotiated. . . . Brill defended the enforcement of Safe Harbor by the U.S. authorities. She said there had been 'numerous investigations into Safe Harbor compliance in recent months,' and 10 enforcement actions since 2009, leading to the sanctioning of companies including Facebook Inc.").

[27] FTC Commissioner Julie Brill's Opening Panel Remarks to the European Institute, Data Protection, Privacy and Security: Re-Establishing Trust Between Europe and the United States 5 (Oct. 29, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/data-protection-privacy-security-re-establishing-trust-between-europe-united-states/131029europeaninstituteremarks.pdf.

[28] EU Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, A7-0139/2014, (Feb. 21, 2014), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2014-0139&language=EN.

[29] Press Release, US NSA: stop mass surveillance now or face consequences, MEPs say (Mar. 3, 2014), http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203/.

[30] Commission Decision of 26 July 2000, *supra* note 13, para. 8. When a Member State finds probable "imminent risk of grave harm" to its citizen's privacy and determines that FTC is not taking adequate and timely steps, national authorities can suspend data flows. *Id.* art. 3(1)(b). If FTC fails to secure a violator's compliance with the Safe Harbor principles, the EC and EU Member States inform one another, *id.* art. 3(3), potentially causing all twenty-eight countries to ban data transfers to the relevant company.

[31] *Id.* art. 3(4).

contains an Annex where FTC's chair emphasized the agency's role in enforcing the Safe Harbor principles.[32]

1. FTC Act legal standard

The Safe Harbor approval by the EC included a letter from then FTC Chairman, Robert Pitofsky, asserting FTC's authority and ongoing role in enforcement actions[33] that would underpin the Safe Harbor principles. He explained:

> The Federal Trade Commission's legal authority in this area is found in Section 5 of the Federal Trade Commission Act ('FTC Act'), which prohibits 'unfair or deceptive acts or practices' in or affecting commerce. A deceptive practice is defined as a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion. A practice is unfair if it causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition.[34]

He specified that FTC Act Section 5 enforcement was called for "if a website falsely claims to comply with a stated privacy policy or a set of self-regulatory guidelines," as this is deceptive.[35] Pitofsky said that FTC would respond to patterns of conduct rather than vindicating individual consumer complaints.[36] He assured, "[t]he FTC will continue to assert its authority, in appropriate cases, to provide redress to citizens of other countries who have been injured by deceptive practices under its jurisdiction."[37]

Deception is a major focus of FTC Act enforcement. FTC's official policy is to look at a misleading statement or practice from the viewpoint of the group at which it is aimed,[38] in this instance reasonable EU consumers. In addition, the misrepresentation has to be material,[39] in this case showing a true statement would affect information-disclosing decisions by EU consumers.[40] Similar to materiality, the issue of injury is important to FTC review and the agency will proceed with an investigation when a misrepresentation causes consumers to act differently than they would with truthful information.[41] In making a case, FTC looks at the entire transaction or course of dealing between a company and a consumer.[42]

---

[32] *Id.* Annex III.
[33] Moreover, he touted FTC's "active monitoring and investigative efforts" as well as the Commission's responsiveness to referrals. *Id.* Annex V.
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] FTC, FTC Policy Statement on Deception 1 (Oct. 14 1983) (letter addressed to John Dingell, Chairman of House Committee on Energy and Commerce), *available at* http://www.fda.gov/ohrms/dockets/dockets/05p0224/05p-0224-cp00001-Exhibit-12-FTC-Policy-Statement-vol1.pdf.
[39] *Id.* at 1, 6 ("Where the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false, materiality will be presumed because the manufacturer intended the information or omission to have an effect.").
[40] *Id.* at 1–2 (i.e. "consumers are likely to have chosen differently but for the deception").
[41] *Id.* at 2, 6.
[42] *Id.* at 2.

Companies can run afoul of Section 5 with several types of material falsifications. Deception can both come in the form of affirmative misrepresentations and significant omissions.[43] Ambiguity is also actionable: "When a seller's representation conveys more than one meaning to reasonable consumers, one of which is false, the seller is liable for the misleading interpretation."[44] Moreover, pro forma disclaimers and statements made after deception are often not sufficient to clean a transaction of the original misrepresentation.[45] FTC "will . . . ask questions such as: how clear is the representation? how conspicuous is any qualifying information? how important is the omitted information? do other sources for the omitted information exist? how familiar is the public with the product or service?"[46] As will be discussed below, the secrecy and lack of transparency around data brokers and other data marketing and profiling companies requires FTC investigation and enforcement under this standard.

As the Safe Harbor FAQs specify, when FTC "determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible" the organization is not entitled to be a part of the Safe Harbor.[47] FTC's recent findings about the data broker industry and CDD's submission in this request for investigation show that many data marketing and profiling companies should not be entitled to remain in the Safe Harbor.

2. Companies' commitments to Safe Harbor Notice, Choice, and Onward Transfer Requirements

Unlike many companies operating under FTC's purview—who nevertheless are subject to sanction for unfair and deceptive practices—those at issue in this request for investigation have committed to specific standards requiring them to provide EU consumers with notice of privacy practices as well as the choice to opt out of information uses that consumers deem to violate their privacy. The companies also have duties to vet third parties that receive the personal information and stop them from using that information in ways that violate consumer understanding and choice. Therefore, these data marketing and profiling companies have an affirmative duty to truthfully and fully represent their relevant practices in their privacy policy—omissions and ambiguities in these disclosures are deceptive.

A data marketing and profiling company that has self-certified in the Safe Harbor:[48]

---

[43] *Id.*
[44] *Id.* at 3.
[45] *Id.* at 5.
[46] *Id.*
[47] Commission Decision of 26 July 2000, *supra* note 13, Annex II (FAQ 11).
[48] There are two narrow exceptions to full Notice and Choice requirements in the Safe Harbor framework, which do not apply to the companies at issue here. Although the Safe Harbor principles contains a narrow exception for third parties who are agents of Safe Harbor member companies, *see id.* Annex I n.1, this should not be applicable to most of the companies here because they are not performing tasks under a fiduciary duty. They generally contract with other companies at arm's length to provide them with services that are both protected trade secrets and based on proprietary data sets that contain more data than any one source has provided. Looking to the standard in Directive 95/46/EC that is similar to this exception, the requirement is for the company to be under the "direct authority" of data controllers or processors, which is not the relationship that these companies have with their clients. *See* Directive 95/46/EC, *supra* note 5, art. 2(f) (defining "third party"). Additionally, the Safe Harbor principles contain a second exception from Notice, Choice, and Onward Transfer for companies that are processing purely public information.

> must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. . . . in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.[49]

This is the **Notice** requirement (Notice) of the Safe Harbor. Participating companies mostly have privacy policies on their websites,[50] which they provide to the Department of Commerce in the process of self-certification.[51] It follows that these policies should therefore fully satisfy Notice, and properly inform EU consumers about the purposes for which their data is collected and used.

In order to make the disclosure meaningful, the companies are also under a **Choice** requirement (Choice) that shields consumers from data sharing they do not agree with, as well as new uses of already-collected information:

> An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual.[52]

Choice must be: "clear and conspicuous, readily available, and [provide] affordable mechanisms to exercise choice."[53] When companies are collecting and using sensitive information, such as racial demographic information, religious or political leanings, or medical information, companies

---

Commission Decision of 26 July 2000, *supra* note 13, Annex II (FAQ 15). However, it can be seen from a cursory inspection of these companies' businesses that they obtain public records and combine them with proprietary information such as commercial and derived data points. *See* FTC, Data Brokers: A Call for Transparency and Accountability ii (2014) (describing the public and nonpublic information sources that data brokers routinely use to create user profiles), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; *see also* company summaries accompanying this filing. As a result of neither exception applying, these companies all remain bound to comply with Notice, Choice, and Onward Transfer duties.

[49] Commission Decision of 26 July 2000, *supra* note 13, Annex I.

[50] As discussed in the attached company summaries, a few of the companies CDD researched have merged and now redirect to different privacy policies, though on the DOC Safe Harbor certification page there is no indication that the certified company no longer has a relevant policy.

[51] This does not apply to companies whose website privacy policies apparently only cover data collection on their own website, but not data they get through their clients or other third-party sources. It is possible that companies provide Notice and Choice through different forms of disclosure to EU consumers (i.e. pop-up disclosures on third-party sites) but this request for investigation was limited to public-facing privacy policies that were available to CDD through web searches. FTC's abilities to investigate further and request confidential business information from the companies will no doubt be of use in digging deeper into all of the statements EU consumers do and do not see when their information is being collected across many other internet properties.

[52] Commission Decision of 26 July 2000, *supra* note 13, Annex I.

[53] *Id.*

must provide a different Choice mechanism that asks individuals to *opt in* before the information is disclosed to third parties or used for a new purpose.[54]

Choice applies in full force to all of the marketing companies at issue in this request for investigation because, as the Safe Harbor FAQ states: "an individual should be able to exercise 'opt out' (or choice) of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective."[55] This is important because data marketing and profiling companies collect information from numerous sources so the most obvious form of opting out—deleting an account and ceasing to do business with a company—is not available to EU consumers, who never chose to deal with such companies in the first place.

In another requirement the Safe Harbor principles explicitly apply Notice and Choice within **Onward Transfer** requirements (Onward Transfer) for information given to third party agents, and this further requires Safe Harbor participants to ensure that the third parties are either companies subject to the Directive (i.e. EU companies), members of the Safe Harbor, or contractually bound to give similar privacy protections.[56] As a result, companies receiving personal information on EU consumers from other companies, such as those at issue here, need to give consumers the same "clear and conspicuous" accounts of information use and choices to opt out (or to opt in when dealing with more sensitive information) before any further transfer of information gleaned from EU consumers. In order to abide by this Onward Transfer duty, Safe Harbor companies would logically have to determine the Notice and Choice disclosures under which the companies that gave them information on EU consumers first collected this data.

The self-certification aspects of the Safe Harbor framework demonstrate further what should be included in proper Notice. The recent November 2013 EU statement on rebuilding trust around data flows gave companies' two Notice duties as: "(a) identify in its publicly available privacy policy that it adheres to the Principles and actually comply with the Principles, as well as (b) self-certify, meaning it has to declare to the U.S. Department of Commerce that it is in compliance with the Principles."[57] While the companies' statements to the DOC are relevant information to the full question of intent to comply, it is the first prong—public-facing privacy policies—that most directly regards possible deception of EU consumers under the FTC Act. Statements made only to DOC cannot satisfy the general transparency requirements at issue here. Companies within the Safe Harbor have a duty to, at the very least, self-assess to be sure that their "published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible."[58] Though the Safe Harbor FAQs present this as a part of self-certification, failure to abide by this requirement would be pertinent to FTC enforcement for a failure to abide by Notice and Consent requirements.

[54] *Id.*
[55] Commission Decision of 26 July 2000, *supra* note 13, Annex II (FAQ 12).
[56] *Id.*
[57] European Commission, Restoring Trust in EU-US data flows, *supra* note 21, at 3.
[58] Commission Decision of 26 July 2000, *supra* note 13, Annex II (FAQ 7).

III. ANALYSIS OF VIOLATION TYPES

It can be seen from the above discussion of Section 5 that, while the Safe Harbor principles are construed under U.S. legal standards, FTC must assess these companies' privacy disclosures from the perspective of an EU consumer. EU consumers' expectations and legal rights are determinative as to whether statements, omissions, or ambiguities are deceptive under the FTC Act. As such, EU legal standards and definitions are relevant—Notice requires frank and comprehensible explanations that EU consumers can understand and which enable them to exercise Choice and avoid unacceptable practices of data marketing and profiling companies. CDD has identified three broad types of violations that FTC should investigate in relation to the companies listed in the company profiles attached to this request for investigation.

1. Privacy policies that misrepresent companies' legal status and EU law

These companies' disclosures to the DOC and EU consumers make legal determinations that are incorrect under EU law[59] and would mislead consumers to believe that other parties are responsible for their information, or that all personal information is stored in a way that cannot affect their privacy. Both of these types of disclosures run contrary to EU legal standards, and therefore endanger EU consumers that rely on such misleading statements, risking their ability to seek remedies.

"FTC applies the same vigorous approach to protecting European consumers through enforcement of the U.S.-EU Safe Harbor Framework" as it applies to other consumer protection.[60] As a result, respecting anti-fraud legislation passed in 2006, FTC has filed complaints against U.S. companies that misrepresented legally-significant facts such as the validity of warranties abroad and whether the companies were subject to a foreign nation's law.[61] As can be seen from the complaints against a California company posing as a UK home electronics seller, normal Section 5 analysis allows FTC to consider foreign victims' understanding of their legal rights in determining if a representation is deceptive.[62]

[59] This analysis discusses EU standards to clarify what these laws should mean to a reasonable EU consumer, not to suggest that FTC apply foreign law. The two relevant definitions are also copied verbatim in the Safe Harbor, so they bear equally on these companies' intention to comply with Safe Harbor duties.

[60] FTC, Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework, *supra* note 1, at 3.

[61] Press Release, FTC Settlement Bans Online U.S. Electronics Retailer from Deceiving Consumers with Foreign Website Names (June 9, 2011), *available at* http://www.ftc.gov/news-events/press-releases/2011/06/ftc-settlement-bans-online-us-electronics-retailer-deceiving; Press Release, Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site (Aug. 6, 2009), *available at* http://www.ftc.gov/news-events/press-releases/2009/08/court-halts-us-internet-seller-deceptively-posing-uk-home.

[62] *See* FTC v. Jaivin Karnani, First Amended Complaint, CV 09-5276 DPP (N.D. Calif. May 16, 2011) (finding deception where UK consumers would believe their national law was applicable and product warranties were valid in the UK), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanicmpt.pdf; FTC v. Jaivin Karnani, Complaint for Permanent Injunction and Other Equitable Relief, CV09-5276 (N.D. Calif. July 20, 2009) (same), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/08/090806karnanicmpt.pdf.

a. These data marketing and profiling companies are "controllers" under EU law and the Safe Harbor definition

Many of these companies claim to be data "processors" and not data "controllers" under EU law. This is likely because the Safe Harbor FAQs seemingly creates a loophole for "processors"—allowing them to not apply certain Safe Harbor principles to information that is only intended for "mere processing."[63] Significantly, under Directive 95/46/EC the difference between data controllers and data processors is a central legal issue.[64] Consequently, these companies have a risk-based interest in avoiding compliance duties by portraying themselves as processors to EU consumers.

However, the definition of "controller" describes what most of the companies outlined in this request do as a matter of normal business. Controllers "determine[] the purposes and means of processing" according to both the Safe Harbor FAQ[65] and Directive 95/46/EC.[66] These data marketing and profiling companies are not receiving information merely for processing—indeed, they are creating products based on profiling consumers in new and innovative ways that client companies and EU consumers do not even understand.[67]

One can see why these companies are controllers, and the importance of this for EU consumer rights, from the application of the definition in a recent privacy decision by the European Court of Justice (ECJ) regarding an American search giant. Google is a data controller and subject to EU national law, under reasoning that seemingly applies to the larger[68] data marketing and

[63] Commission Decision of 26 July 2000, *supra* note 13, Annex II (FAQ 10). The logic is that if a controller in the EU has a contract for processing with a processor in the U.S., the controller remains responsible for the privacy of the information under the Directive. *Id.* Since foreign data processors are usually subject to a restrictive contract with a controller it is viewed as sufficient for another company, the controller, to be fully accountable in the EU for the actions of the processor. This logic fails if such contracts remain secret and possibly do not force third parties to uphold sufficient data protection standards.

[64] Most requirements in the Directive only apply to controllers. *See* Directive 95/46/EC, *supra* note 5, paras. 18, 19, 46, 51, 55, arts. 2(d) (defining "controller"), 2(e) (defining "processor"), 2(f) (defining "third party"), 4, 10–12, 16–18, & 23.

[65] Commission Decision of 26 July 2000, *supra* note 13, Annex II (FAQ 10). Both instruments have the same definition of "controller," presumably because DOC expected co-extensive coverage that would be deemed "adequate."

[66] Directive 95/46/EC, *supra* note 5, art. 2(d).

[67] FTC, Data Brokers, *supra* note 48, at 5 ("In recent years, the development of new technologies and business models, such as social media and mobile applications, has dramatically increased the availability, variety, and volume of consumer data. New forms of tracking and increasingly powerful analytics capabilities have emerged, such as mobile tracking and analytics services that enable tracking of users across devices so that companies can communicate a timely message tailored to a consumer based on the consumer's location. With these new sources and technologies, along with competitive demands from companies to seek more data about more consumers on an increasingly granular level, data brokers are finding new opportunities to collect, compile, package, and sell the consumer information they obtain.").

[68] The ECJ determined not only that Google was a controller, but also that it was covered by Spanish law because of Article 4(1)(c) of Directive 95/46/EC. Controllers that are not incorporated in an EU Member State are still subject to that nation's data protection law if they "make use of some equipment, automated or otherwise," in the Member State. Case C‑131/12, Google Spain SL v. Agencia Española de Protección de Datos, *supra* note 6, para. 6. Generally speaking, larger data companies build infrastructure close to their customers and data is stored near to consumers to shorten transmission time. While some of the smaller companies at issue here might not control hardware in every EU Member State, it seems likely that many of them are making use of technology abroad to process personal information to serve advertising products.

profiling companies at issue in this request. The Directive's definition states, in full: "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[69] The ECJ unequivocally read the definition to cover search engines that determine the purpose and means of categorizing data, including personal data,[70] and described it as "contrary not only to the clear wording of that provision but also to its objective" to accept that the company was not a controller simply because it was sorting data hosted by another company.[71] Companies that perform independent processing in addition to that of original data sources, and whose work makes personal data more easily disseminated, are therefore controllers.[72] While the ECJ was discussing a search engine and not a data marketing and profiling company, this opinion shows that controller status will arise from sorting internet users using personal information from many sources.

The profiles that data marketing and profiling companies make on consumers are especially suspect under this reasoning. The ECJ determined that a company that "establish[es] a more or less detailed profile" of an EU citizen "is therefore liable to affect significantly . . . the fundamental rights to privacy and to the protection of personal data" of that citizen.[73] So both the control that these data marketing and profiling companies wield as well as their ultimate goal of profiling consumers should implicate Directive 95/46/EC protections.[74] To the extent the data marketing and profiling companies share the decisions on purposes and means of processing EU consumers' personal information with client companies, the controller liability for proper data protection is shared among the companies.[75] Controllers cannot pass on responsibility lightly.

Importantly, the ECJ's interpretation is not a novel understanding of this legal definition. The expert Article 29 Working Party issued guidance in 2010 that addressed the "precise meaning" of "controller" and clearly set out criteria that inform companies when they are controllers.[76] The Working Party determined that the definition of controller throughout the EU[77] required a "functional" inquiry that allocated responsibility to the processing companies with "factual influence."[78] Such a factual analysis helps to define controllers even in complex technical online relationships, and this guidance put companies on notice that they are often responsible under the Safe Harbor or Directive 95/46/EC even if they regard themselves as "facilitators."[79] Under this analysis the companies at issue in this request are more than processors: companies that determine

[69] *Id.* para. 4.
[70] *Id.* para. 33.
[71] *Id.* para. 34.
[72] *Id.* paras. 35–36.
[73] *Id.* paras. 37–38.
[74] *See id.* para. 38.
[75] *Id.* para. 40.
[76] *See* Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN, 1–2, 7 (Feb. 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.
[77] *Id.* at 8 ("in the process of adoption of Directive 95/46 the determination of the controller becomes a Community concept, a concept which has its own independent meaning in Community law, not varying because of - possibly divergent - provisions of national law.")
[78] *Id.* at 1.
[79] *Id.* at 11; *id.* at 12 ("There is a growing number of actors who do not consider themselves as determining the processing activities, and thus responsible for them. A conclusion on the basis of factual influence is in those cases the only feasible option.").

the technical and organizational questions of which individuals to target and how to effectively do so are controllers, due to their authority over the "means" of data processing.[80] Intermediary companies are nonetheless controllers when they combine information from multiple sources.[81] Moreover, when these companies use others' data to create their own value-added services they similarly become controllers, either alone or jointly with their clients.[82]

This guidance shows that the companies at issue in this request for investigation are responsible for all the legal duties of a controller. The Working Party's examples show that companies using customer information from one source to advertise for other clients are controllers,[83] as are companies that select individuals for clients from proprietary databases,[84] and behavioral advertising companies.[85] Further, companies at issue here are interacting with their clients as experts in online advertising, and "professional expertise of the service provider [can] play a predominant role, which may entail its qualification as data controller."[86] The Working Party emphasized the importance of properly categorizing entities, as controllers are ultimately responsible for all data protection duties recognized and enforced under EU law.[87] Purposive interpretation of data protection law requires that controllers retain responsibility for collected personal information, and do not simply avoid this duty with formalistic legal evasions.[88] Hence, controllers cannot contract out of their data protection duties.[89]

EU consumers have an expectation of retaining some control over their data even when held by third parties who received it from another entity. Considering that data passes from company to company, and through the hands of parties outside of EU jurisdiction, "effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the" original data sources.[90] Therefore it is irrelevant to the question of responsibility where these data marketing and profiling companies obtain their information—as controllers they are responsible for the data they hold and use.

As noted above, as stated in the Working Party's guidance, the "controller" status of the companies at issue in this request is an important issue to the legal claims of consumers across the EU,[91] as well as under the Safe Harbor. If they are, as many of them claim, mere processors instead

[80] *Id.* at 14.
[81] *Id.* at 30.
[82] *Id.* at 14.
[83] *Id.*
[84] *Id.* at 19 (giving the example of a headhunter company with a large database of job seekers).
[85] *Id.* at 23. This example notes further: "In all cases, (joint) controllers shall ensure that the complexity and the technicalities of the behavioural advertising system do not prevent them from finding appropriate ways to comply with controllers' obligations and to ensure data subjects' rights." *Id.*
[86] *Id.* at 28.
[87] *Id.* at 4.
[88] *Id.* at 4, 8, 12 ("the definition of data controller should be considered as a mandatory legal provision, from which parties cannot simply derogate or deviate. [Otherwise the definition] would run counter to the effective application of data protection law and would nullify the responsibility that data processing entails.").
[89] *Id.* at 9, 11.
[90] Case C‑131/12, Google Spain SL v. Agencia Española de Protección de Datos, *supra* note 6, para. 84.
[91] For example, Article 11 of Directive 95/46/EC would give EU consumers rights as against all data controller companies highlighted in this request, since one commonality among data marketing and profiling companies is that they collect personal information from many sources other than the consumer and then share it with third parties without the data subjects' knowledge.

of data controllers then consumers have little recourse against them in their own countries and have fewer explicit rights under the Safe Harbor principles. However, it seems likely that many, if not all, of these data marketing profiling companies determine the means of using and manipulating personal information—therefore they are data controllers. Consumers that are misled to think they do not have valid claims in foreign jurisdictions are materially deceived—it is the difference between individuals contacting an attorney and attempting to bring a case, or summarily losing their fundamental right to privacy though inaction. If the companies are allowed to continue to make these misrepresentations EU consumers will continue to have their ability to enforce their rights undercut, to the detriment of their privacy as well as the future feasibility of the Safe Harbor.

b. The tracking technologies these data brokers use are not anonymous under EU law and the Safe Harbor definition

The Safe Harbor has a high standard of information anonymization, adopted from the text of the Directive. "'Personal data' and 'personal information' are data about an identified *or identifiable* individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form."[92] (emphasis added). The range of information that data marketing and profiling companies deal with is often about an identified individual, and even after customary American industry anonymization practices it remains identifiable and hence covered by EU law and the Safe Harbor.

"Identifiable" information is a broad swathe of information these companies use as a matter of course.[93] Directive 95/46/EC explains that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person . . ."[94] Research on the issue shows that most types of anonymization (i.e. removing the most personal information that identifies an individual) do not prevent re-identification by controllers or third parties. Latanya Sweeney's definitive study on the issue[95] proved that Americans could be re-identified to health records to a high degree of accuracy using only birth date, zip code, and sex.[96] This type of proof has lead U.S. privacy scholars to determine that anonymization is largely impossible.[97] EU experts agree. Recognizing the danger

[92] Commission Decision of 26 July 2000, *supra* note 13, Annex I.

[93] For further clarity on this issue see Article 29 Data Protection Working Party, *Opinion 08/2012 providing further input on the data protection reform discussions*, 1574/12/EN 5–6 (Oct. 5, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf (explaining that "One of the main conclusions of this analysis is that a natural person can be considered identifiable when, within a group of persons, he or she can be distinguished from other members of the group and consequently be treated differently." and explaining the threshold that makes online and geolocation tracking "identifiable").

[94] Directive 95/46/EC, *supra* note 5, para. 26.

[95] Latanya Sweeney, k-*anonymity: A Model for Protecting Privacy*, 10 International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 557 (2002), *available at* http://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.pdf.

[96] Nate Anderson, *"Anonymized" data really isn't—and here's why not*, Ars Technica, Sep. 8, 2009, http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/.

[97] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006; Arvind Narayan, Edward Felten, *No Silver Bullet: De-Identification Still Doesn't Work* (July 9, 2014), *available at* http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf ("there is no evidence that de-

of re-identification of search terms (often not treated as personal information by internet companies), the Article 29 Working Party has specified that anonymization must be "completely irreversible," companies should guard against re-identification "even by combining anonymized information" held by other entities, and that companies that replace IP addresses and cookie identifiers in their own records with different unique identifiers should also destroy parts of their profiles on consumers to further anonymize the data.[98] These measures are not presented as best practices, they are the minimum legal standards for anonymization.

Since the EU law in question is a directive[99] and does not define "anonymous," as it does "controller," that word—as used by data marketing and profiling companies in privacy policies—is subject to Member State definition, and as a result the legal scope of anonymous data varies across the EU. In one study of four national data protection regimes[100] researchers found differences in the definition and application of "anonymous" as well as whether information that qualified as anonymous was nonetheless covered by data protection law.[101] These high, and varied, standards for what "anonymous" means in the EU should inform FTC's analysis in assessing whether Safe Harbor data marketing and profiling companies have acted deceptively under the FTC Act. EU consumers' expectations of "anonymity" includes more than removing a name or government ID number from a profile, anonymity in this case demands numerous failsafe measures to prevent identification and re-identification by first party and third party companies.

As one example, similar to the stated position of FTC staff in 2009,[102] in the EU the tracking technologies that data marketing and profiling companies use to track individuals on the

---

identification works either in theory or in practice and . . . attempts to quantify its efficacy are unscientific and promote a false sense of security by assuming unrealistic, artificially constrained models of what an adversary might do").

[98] Article 29 Data Protection Working Party, *Opinion 1/2008 on data protection issues related to search engines*, 00737/EN, 20 (April 4, 2008), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

[99] Regulations become directly effective law in all Member States when they enter into force, directives must be implemented by national lawmaking.

[100] *See* Joel R. Reidenberg & Paul M. Schwartz, Data Protection Law and On-Line Services: Regulatory Responses (2002), *available at* http://ec.europa.eu/justice/data-protection/document/studies/files/19981201_dp_law_online_regulatory_en.pdf.

[101] Some examples of nations' many divergences in implementation serve to show the complexity: the Belgian data protection law strictly construed "anonymous" yet also covered some fully anonymized data with certain consumer protections, *id.*at 27, 28; the French data authority views aggregated data as non-anonymous if it came from too small of a grouping and considers clickstream data to be non-anonymous personal information, *id.* at 32, 33; under German law encrypted data may be "anonymous" until the entity holding it is able to decode the encryption, and requires internet service providers to allow Germans the use of internet services and payment for them anonymously, *id.* at 37, 39; while British law views certain data as anonymous when personal identifiers are "unlikely to be capable of being attached." *Id.* at 42.

[102] *See* FTC, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising 21–22 (Feb. 2009), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf ("Staff believes that, in the context of online behavioral advertising, the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data. Indeed, in this context, the Commission and other stakeholders have long recognized that both PII and non-PII raise privacy issues . . ."). FTC staff noted "even where certain items of information are anonymous by themselves, they can become identifiable when combined and linked by a common identifier." *Id.* at 22. The identifiers at issue are the common tracking technologies that data marketing and profiling companies routinely use, such as cookies and IP addresses. *Id.* at 21.

internet are identifiable information, requiring extra consumer protections. In 2009 the EU enacted Directive 2009/136/EC of the European Parliament and of the Council,[103] also known as the "Cookie Directive" though it applies to many additional online trackers.[104] This directive recognized that third-party cookies are a significant issue of access and information storage on individuals' computers "of paramount importance" requiring "users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access."[105] The Cookie Directive called on Member State data protection authorities to increase their enforcement tools in order to fully assure that companies are getting actual consent for this type of online tracking.[106] Subsequently, the EU's expert Article 29 Working Party has given companies more information on how these tracking technologies are collecting personal information, requiring genuine consent.[107]

As a consequence of the Cookie Directive, in "light of the highly invasive nature of [marketers' profiling] cookies vis-à-vis users' private sphere, Italian and European legislation requires users to be informed appropriately on their use so as to give their valid consent."[108] Italy's implementation of the Cookie Directive subjects violators to heavy fines.[109] Another national authority, in the UK, implemented this law by making clear that user consent cannot be obtained from notice through privacy policies that are "hard to find or difficult to understand."[110] The UK authority also made clear that cookies that are combined with personal information implicate higher legal standards and should cause companies to consider minimizing and anonymizing all the information they process, especially if the processing is not for the benefit of the people it regards.[111] Measures like these ones show that industry standard online tracking technologies are not considered harmless or anonymous under EU law, and EU consumers expect heightened Notice before such tracking.

The reasonable EU consumer would be materially misled by assertions by Safe Harbor data marketing and profiling companies that claim their information is not re-identifiable. This is both because the definition of anonymous varies widely between German and British law, but also because it can be seen that many forms of anonymization have been proven to be ineffective against re-identification. Standards in the EU that are considered necessary for actual

---

[103] Directive 2009/136/EC, of the European Parliament and the Council, 2009 O.J. (L 337/11), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Dir_2009_136_EN.pdf

[104] See one Member State's implementation of the Cookie Directive. Italian Data Protection Authority, Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies – May 8 2014, at 1, *available at* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/3167654 ("the provisions on the use of cookies also apply to similar tools such as web beacons, web bugs, clear GIFs or others, which allow identifying users or terminals and fall accordingly under the scope of this decision").

[105] Cookie Directive, *supra* note 103, para 66.

[106] *Id.*

[107] *See* Article 29 Data Protection Working Party, *Working Document 02/2013 providing guidance on obtaining consent for cookies*, 1676/13/EN (Oct. 2, 2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.

[108] Italian Data Protection Authority, *supra* note 104, at 2.

[109] *Id.* at 4–5 (ranging from € 6000 to € 120,000 for different violations).

[110] *See* UK Information Commissioner's Office, Cookies Regulations and the New EU Cookie Law, http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies (last visited Mar. 30, 2014).

[111] *Id.*

anonymization, including damaging the overall data set by removing information from profiles and considering whether someone is identifiable when one data set is combined with another company's records, are not even considered best practices by the U.S. companies at issue here—their stated abilities to find and match consumers with advertisers do not allow for effective privacy protection if it undercuts the bottom line. Routine online tracking technologies used by these companies are not anonymous. As a result, EU consumers cannot help but be misled when they are told their data is anonymized to the point of no longer falling under data protection laws. If they were told the truth about the weakness of this protection it would affect their decision to divulge personal information and to seek legal redress.

2. Privacy policies that misrepresent companies' practices with EU consumer data

There are factual misrepresentations about company procedures across the spectrum of privacy policies provided by the companies at issue in this request for investigation. The attached company profiles, introducing 30 companies' inconsistent statements to EU consumers and actual practices advertised to customers should provide FTC with a starting point to investigate such violations. While these summaries cannot provide a full analysis of the course of dealing between consumers and these companies, when paired with FTC's existing analysis of similar companies' lack of transparency, it is evident that these data marketing and profiling companies are adopting misleading policy statements in spite of Safe Harbor commitments.

In March 2014 FTC released a report on data brokers,[112] including two companies[113] that are part of the Safe Harbor and are at issue in CDD's request for investigation. This is not the first time data brokers have failed to rise to FTC's standards: "In the nearly two decades since the Commission first began to examine data brokers, little progress has been made to improve transparency and choice."[114] FTC's definition of data brokers—"companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products . . ."[115]—covers many, but not all, of the data marketing and profiling companies at issue in this request for investigation. At the very least it applies to Acxiom, Adara Media, SDL, Bizo, BlueKai, Datalogix, Merkle, Neustar, Turn, and Xaxis. Other companies that do not fall under the FTC definition nonetheless tell EU consumers one thing and their customers another, as is touched on in the summaries accompanying this request.

The FTC report's findings demonstrate why many data marketing and profiling companies that claim to be participating in the Safe Harbor are violating their duties of Notice and Choice as a normal part of their daily business, resulting in patterns of deception that merit sanction and an end to their participation in the Safe Harbor. As the report found "to the extent that data brokers offer consumers explanations and choices about how the data brokers use their data, that information may be difficult to find and understand."[116] This echoes a Senate committee report that recently found "data brokers that sell data for marketing purposes operate with minimal

[112] FTC, Data Brokers, *supra* note 48.
[113] Datalogix and Acxiom, *see id.* at 8.
[114] *Id.* at 57.
[115] *Id.* at 3.
[116] *Id.* at 3.

transparency."[117] That lack of transparency violates Notice and Choice duties of the Safe Harbor framework, and is evident in the difficult to find and understand privacy policies of the companies at issue here.

Both the companies' identities and the personal information profiles they maintain remain obscured from EU consumers, making Notice impossible when it is required under Onward Transfer (i.e. when data brokers acquire EU consumer personal information and use it as a controller). "Because these companies generally never interact with consumers, consumers are often unaware of their existence, much less the variety of practices in which they engage."[118] They also infer information about consumers,[119] creating additional personal information that is the product of sophisticated analysis of information troves from both online and offline sources.[120] Once consumer data is collected and processed, data brokers sell sensitive information to clients.[121] "All of this activity takes place behind the scenes, without consumers' knowledge."[122] Under the Safe Harbor, especially Choice and Onward Transfer duties, these practices require frequent clear disclosures and opportunities to opt out/in before information is used, but this is apparently not these companies' practice.

Choice is severely limited by these companies' ineffective mechanisms for opting out and lack of clarity about the mechanisms. Data brokers selling marketing products do not generally provide consumers with the right to review their data nor the possibility of correcting that information; and while the majority of marketing data brokers FTC studied allowed a consumer opt out of some sort, this was found to be difficult for consumers to find and understand.[123] Moreover, "data brokers that provide consumers with the ability to opt out convey some limitations regarding opt outs to consumers, but do not convey others, which could confuse consumers."[124] Plus, it is worth noting that these companies are collecting more sensitive information[125] that, under Choice, requires affirmative opt ins by consumers before information is used for new purposes—FTC's report did not mention a single marketing data broker offering such an opt-in mechanism.

Further, in violation of meaningful Choice, marketing-focused data brokers do not cease to transfer and use information on consumers who do successfully opt out under the mechanisms provided.[126] The companies instead keep all the data, in order to facilitate the limited opt-out, but

---

[117] *Id.* at 7.
[118] *Id.* at i.
[119] *Id.* at iv, vii.
[120] *Id.* at iv–v. FTC reported that none of the data brokers it investigated received information directly from consumers, *id.* at 11, however the companies at issue in this request for investigation do gather information about users' activities online directly from them and combine this with known information to profile EU consumers further. See company profiles accompanying this request for examples.
[121] *Id.* at 19; *id.* at 24–25 (listing numerous forms of sensitive information that data customers can purchase and "append" to records they have on their existing customers).
[122] *Id.* at vii.
[123] *Id.* at iii.
[124] *Id.* at 43.
[125] *Id.* at 19 (they all collect information "such as a person's name, address, home ownership status, age, income range, or ethnicity").
[126] *Id.* at 43.

also to sell in non-marketing services[127] and some of the companies "might continue to use the suppressed information in products that display data in aggregated, anonymous form."[128] Ultimately, FTC found "data brokers' opt outs do not clearly convey whether the consumer can exercise a choice to opt out of all uses of consumer data, and therefore, consumers may find the opt outs confusing."[129] This is not providing sufficient clarity or mechanisms to give EU consumers Choice—indeed, even after opt out the data is still available to the company and its customers in another format, possibly identifiable, and individual profiles continue to exist that could be lost in a data breach or transferred in a merger.

Once data brokers have compiled this information, they provide the data to their clients.[130] Such action implicates Choice or Onward Transfer. Data marketing and profiling companies both collect and disseminate personal information to and from third parties. For example, FTC's report showed that the data brokers it investigated bought data about consumers from commercial sources such as retailers and browsing activity from online advertising networks[131] such as those at issue in this request for investigation. Furthermore, "each data broker utilizes multiple sources for similar data. For example, one of the data brokers in [the FTC] study obtains consumers' contact information from twenty different sources."[132] Data brokers are collecting a few discrete data points about each consumer from different sources, then combining that information to form detailed profiles of them with information from other sources.[133] This other information often comes from, and is later sold to, other data brokers.[134] "Accordingly, it would be virtually impossible for a consumer to determine how a data broker obtained his or her data; the consumer would have to retrace the path of data through a series of data brokers."[135] But under the Safe Harbor there should be sufficient Notice and Choice for EU consumers to understand and opt out (or opt in, more likely) of this type of reselling. It is the duty of these companies to provide this information clearly so that EU consumers can easily understand where the information is going and any new uses data brokers have invented for it.

FTC found practices that would make even "processors" into violators under the Safe Harbor framework, because they are not certain of the relevant commitments of their data sources undertook under Notice and Choice. Most data brokers in FTC's report do not contractually require data sources to warrant that consumers have been given proper Notice and Choice,[136] indicating that companies are unaware of what uses EU consumers have consented to. Only one of the

---

[127] *Id.* ("For example, among the three data brokers that sell risk mitigation and marketing products, one data broker's opt-out disclosures did not clearly convey that the opt out is limited to just the marketing products, which comprise a small percentage of the data broker's business.")
[128] *Id.* As can be seen in the foregoing analysis, it is questionable if FTC's use of "anonymous" would be accepted by an EU consumer.
[129] *Id.* at 49.
[130] *Id.* at 3.
[131] *Id.* at 13–14.
[132] *Id.* at 14.
[133] *Id.* at iv.
[134] *Id.*; *see also id.* at 12 ("The [nine] data brokers [FTC investigated] identified nearly twenty-five other data brokers from which they obtain state and local government information.")
[135] *Id.* at 46.
[136] *Id.* at 16 ("Only two of the data brokers insert contractual provisions requiring the data source to warrant that either it or its sources provided consumers with notice that their information would be shared with third parties and an opportunity to opt out of that sharing.").

companies studied actually performed a cursory inspection of its data sources' websites to be sure that the data source complied with Notice and Choice.[137] By contrast, all the data brokers FTC investigated bind downstream data customers with contracts regarding use of their marketing products.[138] The existence of these contracts with third parties does not necessarily demonstrate protections required under the Choice and Onward Transfer duties, and FTC seems to have found these contracts insufficient in this regard.[139] Further, as can be seen in the attached company profiles, in the 30 companies' marketing materials they allude to detailed personal data that they are making available to others, while FTC's report suggests they are not all contractually binding other companies to abide by the Safe Harbor.

Significantly, all data brokers are engaged in profiling consumers[140] and selling those profiles, either individuals or lists of individuals who fit within a consumer category.[141] These segments of consumers are premised on "vast array"[142] of sensitive data, such as age, income, interest in and need for medications, or ethnic minority status.[143] As discussed above, such profiling is the type of data processing that Directive 95/46/EC, and by extension the Safe Harbor, seeks to control.

Nevertheless, data brokers manipulate their data sets and audiences in diverse ways far beyond profiling individuals. Information they derive and categories they create are kept secret from data subjects and are regarded as proprietary information.[144] Data brokers also serve as middle-men companies matching registration information from one site with marketing objectives of another company.[145] Companies with access to offline data also "onboard" that data and segment, match, and target consumers online using the various forms of personal information available to the companies.[146] These are complex uses of data serving distinct purposes, and unless these practices and their reasoning are clear to EU consumers there is a potential violation of the FTC Act.

As deception regarding company practices will depend on the totality of statements made to EU consumers by each company, it is CDD's object in this request for investigation and attached profiles to provide FTC with particular examples of potentially deceptive statements in order to prompt a broader investigation by the agency. The different representations and business models are too many to list and describe in this section, so FTC's existing findings on like companies have been presented to show that there is a pervasive problem among these data companies that undercuts Notice and Choice. To the extent that all of the listed companies similarly fail to describe their purposes and practices, or accept data from companies that have not given proper Notice of

[137] *Id.* at 16–17.
[138] *Id.* at 41.
[139] FTC's list of conditions in these contracts, while it does include complying with U.S. statutes and industry standards, does not mention Safe Harbor controls. *See id.*
[140] *Id.* at 22 (companies either store their data in profiles based on known individuals, or in a manner that allows them to produce profiles on individuals when needed).
[141] *Id.* at 19, 25.
[142] *Id.* at 47.
[143] *Id.* at 19–20, 47.
[144] *Id.* at 42.
[145] *Id.* at 26–27.
[146] *See id.* at 27–29.

third party data use, they have violated the Safe Harbor's affirmative duty to truthfully and clearly offer such information plus a meaningful opportunity to opt out. The materiality of such deceptions is clear: as FTC found, consumers cannot understand what these companies are doing nor where their personal information is going without a major change in the way disclosures are made. In light of these findings, FTC should build on its report and actively investigate these data marketing and profiling companies for Safe Harbor violations.

3. Statements that imply a company is in compliance with the Safe Harbors despite the fact that the company in question has been acquired, or has merged, and has not updated its disclosures to comply with Notice and Choice requirements attendant to mergers and acquisitions

Companies that were Safe Harbor members but are in the process of merging or being acquired seem to be violating a central tenant of the Safe Harbor framework by not offering Notice and Choice to EU consumers. Safe Harbor FAQ 6 requires companies that have been acquired or merge, to notify the DOC in advance—giving the agency supervising self-certification all necessary information to determine if the company will: (1) assure compliance with the Safe Harbor; (2) re-self-certify; or (3) delete all personal information collected under a previous Safe Harbor membership.[147] But this is not merely a duty to privately report to DOC, as the same FAQ then says: "Any misrepresentation to the general public concerning an organization's adherence to the Safe Harbor Principles may be actionable by the Federal Trade Commission or other relevant government body."[148] Since FAQ 6 specifically notes the problems with merging companies as well as continued compliance with the Safe Harbor in that context, companies that are planning to merge who do not disclose to EU consumers the plan for protecting personal information are violating their Notice and Choice duties by omission.

Companies that have been bought out often must rejoin the Safe Harbor as a successor organization or delete all data that was previously received under the auspices of a Safe Harbor membership.[149] This is significant for companies identified herein that have been acquired but whose parent is not a Safe Harbor member, such as Jumptap and Millenial Media. To the extent that such companies have not recertified with DOC, their membership in the Safe Harbor has lapsed and all representations to the public that they are members are false statements subject to FTC enforcement action. Moreover, insofar as the acquired/merged companies continue to use any information previously acquired, they are in violation of a duty to delete they committed to under Safe Harbor FAQ 6.

A company that foresees a merger that would bring it out of compliance with the Safe Harbor that does not notify EU consumers about its plan to comply or delete all information is materially deceiving consumers. This can be seen from the fact that it is envisioned as a problem in FAQ 6 and the fact that the Article 29 Working Party highlighted such mergers/acquisitions as a potential threat to data privacy in the Safe Harbor framework.[150] Since such a transaction moves

[147] Commission Decision of 26 July 2000, *supra* note 13, Annex II (FAQ 6).
[148] *Id.*
[149] *Id.* Annex IV (Subsection C), Annex II (FAQ 6).
[150] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Opinion 7/99*, *supra* note 18, at 4.

all of an EU consumer's personal information to an entity that the consumer never dealt with in the first place, unless there is additional Notice and Choice before the data transfers, the potential for a consumer to lose control of their information is high. Such violations of Safe Harbor are clear cases that FTC should not delay in investigating and sanctioning.

IV. CONCLUSION

The companies CDD has highlighted in this request for investigation's attached summaries are operating in the same space and with the same policies as the more longstanding data brokers, which FTC has been wary of for some time: "Despite the Commission's past recommendations, lack of transparency and choice remain a significant source of concern about this industry."[151] Although FTC did not address Safe Harbor responsibilities in its recent report, this submission does just that, and the commitments that all of these data marketing and profiling companies have made under the Safe Harbor framework make FTC oversight and enforcement a viable solution to the identified problems. Should the caretakers of the Safe Harbor fail to strengthen their oversight and bring companies in line with Safe Harbor commitments it is possible that the Safe Harbor framework will cease to exist under authority the EC reserved in its 2000 approval. On behalf of EU consumers and the future of American businesses it is contingent on FTC to bring greater transparency and choice to online industries—protecting the privacy rights of millions.

Hudson B. Kingston
Legal Director
Center for Digital Democracy
1621 Connecticut Ave. NW, Suite 550
Washington, DC 20009
(202) 986-2220

[151] FTC, Data Brokers, *supra* note 48, at vii.