Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework

(November 12, 2013)

Staff of the U.S. Federal Trade Commission ("FTC") appreciates the opportunity that European Commission ("EC") Vice-President Viviane Reding has offered us to provide input on the EC review of the U.S.-EU Safe Harbor Framework.[1] This framework provides a way for businesses to transfer personal data from the EU to the U.S. in a manner consistent with EU law.[2] The U.S. Department of Commerce administers the framework, and the FTC provides an enforcement backstop.

Since the establishment of the Safe Harbor in 2000, the FTC has been committed to the effective operation of the program. In our previous exchanges with the EC, we have addressed issues such as the FTC's enforcement powers; jurisdiction over employment data; the sectoral exemptions to our jurisdiction; and educating European Union consumers on Safe Harbor. We have also met on many occasions with our EU colleagues to exchange views on Safe Harbor in person. Recently, Vice-President Reding raised a number of issues regarding the program's administration, redress, and enforcement. Today we continue the discussion and welcome further dialogue about improvements to Safe Harbor.

Our comment begins by putting Safe Harbor enforcement in the context of the FTC's overall privacy enforcement program. We then highlight our Safe Harbor enforcement activity over the years. Finally, we offer thoughts on how to improve the program going forward, including our role in administration, redress, and enforcement of Safe Harbor, with an emphasis on the importance of international enforcement cooperation. Importantly, because the FTC's role in the Safe Harbor program focuses on enforcement, this comment emphasizes the issues raised with respect to enforcement.

The FTC's Privacy & Data Security Program

The FTC is the leading U.S. consumer protection agency focused on commercial sector privacy. The FTC has authority to prosecute unfair and deceptive practices that violate consumer privacy as well as more targeted privacy laws that protect financial and health information, information about children, and credit information.

The FTC has unparalleled experience in consumer privacy enforcement. Our enforcement actions have addressed practices in offline and online environments. We have brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, Microsoft, and Myspace, as well as lesser-known companies. We have sued businesses that spammed consumers, installed spyware on computers, failed to secure consumers' personal information, deceptively tracked consumers online, violated children's privacy, unlawfully collected information on consumers' mobile devices, and failed to secure Internet-connected

[1] This Comment reflects the views of FTC staff, and not necessarily those of the Commission or any Commissioner.

[2] See generally Dep't of Commerce, U.S.-EU Safe Harbor Overview, available at http://export.gov/safeharbor/.

devices. The resulting orders have typically provided for ongoing monitoring by the FTC, prohibited further law violations, and subjected the businesses to substantial financial penalties for order violations. Moreover, FTC orders do not just cover individuals who may have complained about a problem; rather, they protect all consumers dealing with the business. In the cross-border context, the FTC has jurisdiction to protect consumers worldwide from practices taking place in the United States.[3]

To date, the FTC has brought 134 spam and spyware cases, 108 Do Not Call cases against telemarketers, 97 Fair Credit Reporting Act lawsuits involving credit-reporting problems, 47 data security cases, 44 general privacy lawsuits, and 21 actions under the Children's Online Privacy Protection Act ("COPPA"). In addition to these cases, we have also issued and publicized warning letters when appropriate.[4]

This privacy enforcement is complemented by our policy work and research into existing and emerging commercial privacy issues. For example, last year the FTC issued a privacy report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,[5] which sets forth an overarching privacy framework built on three core principles: privacy by design, simplified consumer choice, and greater transparency. Shortly, we will host a workshop to explore consumer privacy and security issues posed by the Internet of Things.[6] We are also working on a report that examines the data collection and use practices of the data broker industry. We strive to address new privacy issues, such as children's apps,[7] facial recognition,[8] and big data.[9] We have also addressed mobile challenges, exploring mobile security,[10] mobile privacy disclosures,[11] and mobile payments.[12]

---

[3] Congress has expressly confirmed the FTC's authority to redress harm abroad caused from within the United States. See 15 U.S.C. § 45(a)(4).

[4] See, e.g., Fed. Trade Comm'n, Press Release, FTC Warns Data Broker Operations of Possible Privacy Violations (May 2013), http://www.ftc.gov/opa/2013/05/databroker.shtm; Fed. Trade Comm'n, Press Release, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 2013), http://ftc.gov/opa/2013/04/tenant.shtm.

[5] See Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[6] Fed. Trade Comm'n, Internet of Things: Privacy and Security in a Connected World http://ftc.gov/bcp/workshops/internet-of-things/.

[7] Fed. Trade Comm'n, Mobile Apps for Kids: Disclosures Still Not Making the Grade (Dec. 2012), available at http://www ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; Fed. Trade Comm'n, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (Feb. 2012), available at

The FTC employs consumer and business education to bolster its privacy enforcement. Accompanying many of our cases are materials educating consumers on how they can help protect themselves.[13] Similarly, we provide businesses with compliance guides and information, using lessons learned from our enforcement actions and study of industry practices.[14] For example, we recently provided businesses worldwide with information about how to comply with our updated children's privacy regulations under COPPA.[15] These regulations apply to all websites and online services directed to children in the United States.

We emphasize the FTC's history of strong privacy enforcement because the FTC applies the same vigorous approach to protecting European consumers through enforcement of the U.S.-EU Safe Harbor Framework.

FTC Enforcement of the U.S.-EU Safe Harbor Framework

The FTC is strongly committed to vigilant Safe Harbor enforcement. As the number of companies participating in Safe Harbor has increased, so have our enforcement efforts. To date, we have brought ten Safe Harbor cases.[16] When Safe Harbor was established, the FTC committed to review on a priority basis all referrals from EU member state authorities.[17] While the Framework contemplated that EU data protection and other authorities would provide us with such referrals, we received none for the first ten years of the program, and only a few over the past three years. We accordingly decided to seek to identify, on our own initiative, any Safe Harbor violations in every privacy and data security investigation we conduct.

This proactive enforcement is how FTC staff discovered the Safe Harbor violations of Google, Facebook, and Myspace.[18] These cases demonstrate the enforceability of Safe Harbor certifications and the repercussions for non-compliance. The orders against Google, Facebook, and Myspace require these companies to implement comprehensive privacy programs that must address the risks related to new products and services, and protect the privacy and confidentiality of personal information. The program must identify foreseeable material risks, and have controls to address these risks. The companies must submit to ongoing, independent assessments of their privacy programs, and these are to be reported regularly to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in Safe

---

[13] *See* Fed. Trade Comm'n, *Consumer Information: Privacy and Identity*, http://www.consumer ftc.gov/topics/privacy-identity.

[14] For a general view of the FTC's business education efforts, see the Fed. Trade Comm'n, *BCP Business Center*, http://business ftc.gov/privacy-and-security/.

[15] Fed. Trade Comm'n, Press Release, *FTC Sends Educational Letters to Businesses to Help Them Prepare for COPPA Update* (May 2013), http://www.ftc.gov/opa/2013/05/coppa_education.shtm.

[16] A list of U.S.-EU Safe Harbor cases is available at http://business.ftc.gov/legal-resources/2840/35.

[17] *See* Letter from Robert Pitofsky, Fed. Trade Comm'n, to John Mogg, European Comm'n (July 14, 2000), available at http://export.gov/static/sh_en_FTCLETTERFINAL_Latest_eg_main_018455.pdf.

[18] *Google Inc.*, No. C-4336 (F.T.C. Oct. 13, 2011), available at http://www ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf; *Facebook Inc.*, No. C-4365 (F.T.C. July 27, 2012), available at http://www ftc.gov/os/caselist/0923184/120810facebookdo.pdf; *Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012), available at http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf.

Harbor or similar programs. The FTC can enforce these orders by seeking civil penalties; indeed, last year, Google paid a record $22.5 million civil penalty to resolve allegations it had violated its order.[19] The FTC orders against Google, Facebook, and Myspace help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.[20]

Our cases have also focused on false claims of Safe Harbor participation. We take false claims of registration seriously; such issues have been the subject of seven enforcement actions.[21] Most of these cases involved problems with companies that joined Safe Harbor but then continued to represent themselves as members without renewing the annual certification. If a company's privacy policy promises Safe Harbor protections, that company's failure to make or maintain a registration, is not, by itself, likely to excuse that company from FTC enforcement of those Safe Harbor commitments.

In the FTC's hands, Safe Harbor is a significant tool for the protection of the privacy of

> enforcement pipeline. You can expect to see more enforcement actions on this front in the coming months.[23]

Although Safe Harbor is an effective and functioning tool for the protection of the privacy of EU citizens' data transferred to the United States, we are committed to looking for ways to improve its efficacy.[24] We also have followed with interest the discussions within the European Parliament Committee on Civil Liberties, Justice and Home Affairs about Safe Harbor.[25] We have also noted the increased attention Safe Harbor has received in the context of the ongoing discussion on national security access to information. We would like to address several issues about how to improve the implementation of the Safe Harbor Framework, including administration, redress, and enforcement:

1. We share the EC's interest in increasing transparency and we support the Department of Commerce's efforts to improve the administration of the registration and technical systems of the Safe Harbor website. The FTC takes seriously misrepresentations about Safe Harbor membership, as reflected by the cases it has brought in this area. At the same time, in assessing the performance and efficacy of Safe Harbor, it may be useful to distinguish procedural registration requirements from the substantive Safe Harbor promises made by companies about how they will protect the privacy of their customers. The FTC has long enforced the privacy promises companies make, ensuring that consumers are not deceived. As noted above, if a company's privacy policy promises Safe Harbor protections, that company's failure to make or maintain a registration is not by itself likely to excuse that company from FTC enforcement of those Safe Harbor promises.

2. Safe Harbor is a top enforcement priority. We have opened numerous investigations into Safe Harbor compliance and have Safe Harbor matters in the enforcement pipeline. In all of our privacy investigations, we continue to proactively examine whether there is a Safe Harbor violation. We welcome referrals from authorities in member states, which have a critical role to play in monitoring and reporting possible Safe Harbor violations. We welcome further initiatives from the EU authorities to conduct investigations, and to refer case files and share evidence with the FTC. As it committed at the outset of the Safe Harbor program, the FTC will give priority consideration to these referrals.

3. When the FTC brings a successful Safe Harbor enforcement action, our orders will continue to prevent future misrepresentations regarding Safe Harbor and other privacy programs. We will systematically monitor compliance with Safe Harbor orders, as we do with all our orders. W1.15 Td[(e)-1 Tw r-0.00025 0nh all our or[ve p 7cwr rts.

Importantly, our orders will continue to protect all consumers worldwide that interact with a business, not just those consumers with specific complaints.

security issues. Thus, in addressing national security, as Commissioner Julie Brill recently stated, Safe Harbor is an "easy target" but perhaps is not the "right target."[29]

Within the context of commercial sector transfers, we urge that Safe Harbor continue to be evaluated on its merits. Unlike the other EU data transfer mechanisms, Safe Harbor provides an effective enforcement tool for the FTC. Safe Harbor also is a transparent system; the companies committing to it are listed publicly, which is not the case, for example, with companies using model contract