FTC ENFORCEMENT OF THE U.S.-EU SAFE HARBOR FRAMEWORK

BY ANNA MYERS, CIPP/US, IAPP WESTIN FELLOW
Transatlantic trade in personal information between the United States and the European Union is valued at $1 trillion annually. The invalidation of the U.S.-EU Safe Harbor Framework in 2015 disrupted this economy by making transfer of personal data from the EU to the United States much more difficult. Private companies and public officials alike hope these issues will be resolved by the newly announced EU-US Privacy Shield.

The Privacy Shield intends to incorporate the European Commission’s 13 recommendations to strengthen Safe Harbor, including improvements to the framework’s enforcement mechanisms. Like Safe Harbor, the Privacy Shield will depend on U.S. Federal Trade Commission enforcement, but with increased cooperation with the Department of Commerce and EU data protection authorities.

This study examines the FTC’s Safe Harbor enforcement record for practices and trends that may inform its efforts under the new Privacy Shield. It concludes that while the FTC’s enforcement of Safe Harbor was limited, so was European participation in providing referrals and forwarding complaints. It suggests that meaningful enforcement of the Privacy Shield will rely on more robust EU-FTC cooperation.

“The Privacy Shield intends to incorporate the European Commission’s 13 recommendations to strengthen Safe Harbor.”
FTC SAFE HARBOR ENFORCEMENT PROCESS

Under the Safe Harbor, companies self-certified compliance with a set of principles that were published by the U.S. Department of Commerce and essentially mirrored the principles set by EU data protection law. Organizations self-certified by submitting an application to the DOC including a description of their data practices, privacy policies, memberships in privacy programs, and the types of data they processed. Organizations additionally were required to renew their Safe Harbor certification annually. Preparing an annual review and submitting it for recertification could take several months.

The DOC maintained a list of all organizations that filed self-certification applications and renewals while the International Trade Administration, an agency within the DOC, reviewed every application and renewal before it was finalized. The ITA notified an organization if its application or renewal failed to meet Safe Harbor requirements or needed clarifications or updates.

Because organizations agreed to adhere to the Safe Harbor principles through the self-certification process, failure to honor those principles could be considered a deceptive act or practice in violation of Section 5 of the FTC act. To ensure its enforceability, the Safe Harbor program was specifically limited to organizations already subject to FTC jurisdiction (or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation).
In its enforcement of Safe Harbor, the FTC initiated investigations based on referrals from consumers and EU authorities as well as of its own accord. A company’s actions might be considered deceptive if it had represented adherence to the framework when in fact it did not (1) have a current certification ("technical violation") or (2) adhere to the substantive privacy principles of the framework ("substantive violation"). Failure to comply with the requirements of the framework was actionable by the FTC through administrative orders and civil penalties in an amount up to $16,000 per violation or per day in the case of a continuing violation.

As with the vast majority of FTC enforcement actions, all of the agency’s complaints under Safe Harbor so far have settled. FTC settlement orders do not typically constitute an admission by the party to the facts alleged or of liability. Settlements typically remain in effect for as long as 20 years. Settlement orders typically impose affirmative duties, such as a company no longer misrepresenting its certification or acting to implement a comprehensive privacy program. Even without monetary penalties, implementing new compliance programs to satisfy FTC settlement orders can impose substantial costs and increase consumer privacy. If a party violates a consent order, moreover, it faces civil penalties up to $16,000 per violation and further action by the FTC.

In addition, FTC enforcement can have a deterrent effect and help define “reasonable” data security practices. This is because companies pay attention to practices that the FTC chooses to pursue in its enforcement actions as guiding principles for sound privacy and data security. In the privacy industry, FTC settlements are considered useful in guiding business practices. Indeed, Daniel Solove and Woodrow Hartzog contend the FTC privacy enforcement regime is functionally equivalent to a body of common law for privacy. Case studies by the FPF demonstrated this deterrent effect FTC enforcement has in the context of the Safe Harbor.
FTC SAFE HARBOR ENFORCEMENT ACTIONS

While the FTC committed to review referrals from EU member state authorities on a priority basis, the agency did not receive any referrals until January 12, 2010, and has received just four referrals since then. Consequently, FTC enforcement of the Safe Harbor has primarily been at the agency’s initiative. FTC Bureau of Consumer Protection Director Jessica Rich cited the lack of referrals from European DPAs as a challenge to Safe Harbor enforcement.

In the years between the 2000 adoption of the U.S.-EU Safe Harbor Framework and its invalidation in 2015, the FTC brought 39 enforcement actions alleging Safe Harbor violations. Over those 15 years, Safe Harbor cases (39 actions) accounted for almost 20 percent of all privacy cases brought by the agency (202 actions, as tallied using the IAPP’s FTC Casebook; this omits FTC cases brought under the TCPA and CAN-SPAM act and eliminates double counting of cases brought under multiple legal theories).

Notably almost three-quarters (29/39) of the Safe Harbor cases were brought after 2013. The first Safe Harbor enforcement actions in 2009 occurred after a researcher filed a complaint with the FTC in 2008 alleging six companies misrepresented their Safe Harbor certification. In 2013, following Edward Snowden’s revelations about the extent of U.S. government access to data, the European Commission issued 13 Recommendations to improve Safe Harbor. Conspicuously, in the following two years, FTC enforcement of Safe Harbor peaked.

In most cases, however, the Safe Harbor violations alleged by the FTC were “technical” in nature, meaning they were related to the administrative procedures of the Safe Harbor and dealt with the mechanics of certification or recertification, as opposed to enforcement of substantive data principles.
**SUBSTANTIVE V. TECHNICAL VIOLATIONS**

*NOTE: TES Franchising LLC is represented both as a substantive and technical case in this chart because both types of violations were alleged by the FTC in its case.*

**SUBSTANTIVE VIOLATIONS**

During the Safe Harbor’s tenure, the FTC brought only four actions alleging violations of substantive Safe Harbor Principles: one action for misrepresenting how a company had agreed to settle Safe Harbor-related disputes (TES Franchising, LLC); and three for violations of the notice and choice principles (Google, Facebook, and MySpace).

Notably, the notice and choice principles are not unique to the Safe Harbor Framework but rather underlie the FTC’s enforcement powers against deceptive and unfair acts or practices under the FTC Act. Thus, in the four cases alleging substantive Safe-Harbor violations, the FTC alleged the companies’ actions also constituted deceptive or unfair acts or practices in violation of the FTC Act. Substantive Safe Harbor violations were therefore identified and enforced only when a company was investigated for other privacy-related consumer protection concerns falling within the FTC’s jurisdiction.

**TES FRANCHISING, LLC (2015)**

TES Franchising, LLC (TES) allegedly represented on its website that Safe-Harbor related disputes would be settled by an arbitration agency and would take place in Connecticut, and that costs would be split between the consumer and the company. In fact, TES allegedly agreed in its Safe Harbor self-certification to resolve disputes through European Data Protection Authorities, which do not require in-person hearings and resolve complaints at no cost to the consumer.

**GOOGLE (BUZZ) (2011)**

Google launched its social network “Buzz” in 2010. Google allegedly used information from existing Gmail users to build the social network, automatically creating Buzz profiles and establishing “followers” using Gmail contact lists, without notifying users or obtaining their consent. Google additionally allegedly made Buzz profiles public by default. Google allegedly violated its privacy policy through these actions because the policy stated that when information is used “in a manner different that the purpose for which it was collected, then we will ask for your consent prior to use.” In the complaint, the FTC alleged these actions constituted a deceptive act or practice in violation of the FTC Act and a failure to adhere to Safe Harbor principles of notice and choice. The
settlement order requires Google to obtain express, affirmative consent before sharing user information with third-parties and to institute a “comprehensive privacy program.”

**FACEBOOK (2012)**

Facebook rolled out new privacy controls in December 2009. The privacy controls pages allegedly stated that the new settings allowed users to control who could see their profile information. However, when users restricted their settings using the new controls to show information to “only friends,” those users’ information could allegedly still be accessed by platform applications their friends had installed. The FTC alleged this discrepancy failed to provide users with “sufficient notice and choice regarding their privacy” as required by the Safe Harbor Principles as well as under Section 5 of the FTC Act.

**MYSPACE (2012)**

MySpace’s privacy policy stated it did not share user data with advertisers without notice and consent as well as that it was self-certified under Safe Harbor. The FTC’s allegations arose from MySpace’s practice to provide advertisers with “Friend IDs” that could be combined with an advertiser’s tracking cookie or used to access user information such as name and profile. The FTC alleged that MySpace’s failure to comply with notice and choice principles in three instances constituted deceptive acts or practices in violation of the FTC Act and the Safe Harbor principles. Specifically, the agency alleged that MySpace’s use of the Friend IDs violated its representations that (1) it would not share personal information with third parties, (2) advertisers could not access personal information, and (3) users’ web browsing activity was anonymized before being shared with advertisers. MySpace agreed to a settlement order prohibiting further misrepresentation regarding compliance with the Safe Harbor and requiring the institution of “comprehensive privacy program.”
ALL OF THE ALLEGED TECHNICAL VIOLATIONS THE FTC ENFORCED UNDER THE SAFE HARBOR PROGRAM WERE FOR COMPANIES ALLEGEDLY MISREPRESENTING CURRENT SAFE HARBOR SELF-CERTIFICATION STATUS WHEN IN FACT THEY HAD NOT SELF-CERTIFIED IN THE FIRST PLACE OR THEIR CERTIFICATION HAD LAPSED.

While inaccurate claims of Safe Harbor membership may not rise to the level of substantive privacy violations, false claims weaken trust in the program and dilute the impact of the self-certification framework.

Previous studies indicated that there were numerous technical violations of Safe Harbor, including false claims of membership, that were not pursued:

- In 2008, a Galexia Study checked for compliance with the seventh Safe Harbor Principle on enforcement and dispute resolution. The study found that there were 206 false membership claims among the 1597 organizations on the Department of Commerce Safe Harbor list.

- A 2013 Hunton & Williams study found 427 organizations falsely claimed on their websites that they were Safe Harbor members.

- Similarly, in 2013, staff from the International Trade Administration (ITA) notified “56 percent of first-time certifiers and 27 percent of re-certifiers of the need to make clarifications or changes” to their applications.

- Research from the Future of Privacy Forum (FPF) in December 2013 estimated that 10 percent of companies misrepresented their status in the Safe Harbor program. The FPF explained, however, that inaccurate claims of membership did not indicate that Safe Harbor is ineffective nor did they necessarily impact user privacy.
While the FTC enforcement resources obviously do not enable the agency to pursue every single violation, the FTC brought enforcement actions for 36 technical violations between 2000 and 2015 against companies in a myriad of industries. All 36 of the technical cases were settled with the FTC and the settlement order barred any further misrepresentation. In all of these cases, the FTC alleged that while representing they had current Safe Harbor certification, companies in fact either (1) failed to renew their self-certification or (2) had never self-certified in the first place.

Significantly more cases alleged lapsed certifications (29/36 cases) than failure to certify in the first place (7/36 cases).

“"The FTC brought enforcement actions for 36 technical violations between 2000 and 2015 against companies in a myriad of industries."
### Types of Technical Violations by Year

Since EU Approval of the U.S.-EU Safe Harbor Framework in 2000

<table>
<thead>
<tr>
<th>YEAR</th>
<th>NUMBER OF CASES</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>6</td>
</tr>
<tr>
<td>2001</td>
<td>14</td>
</tr>
<tr>
<td>2002</td>
<td>6</td>
</tr>
<tr>
<td>2003</td>
<td>6</td>
</tr>
<tr>
<td>2004</td>
<td>1</td>
</tr>
<tr>
<td>2005</td>
<td>1</td>
</tr>
<tr>
<td>2006</td>
<td>1</td>
</tr>
<tr>
<td>2007</td>
<td>1</td>
</tr>
<tr>
<td>2008</td>
<td>1</td>
</tr>
<tr>
<td>2009</td>
<td>6 + 1</td>
</tr>
<tr>
<td>2010</td>
<td>14</td>
</tr>
<tr>
<td>2011</td>
<td>1</td>
</tr>
<tr>
<td>2012</td>
<td>9</td>
</tr>
<tr>
<td>2013</td>
<td>14</td>
</tr>
<tr>
<td>2014</td>
<td>6 + 1</td>
</tr>
<tr>
<td>2015</td>
<td>6</td>
</tr>
</tbody>
</table>

#### Self-Certification Lapsed

- COLLECTIFY LLC (2009)
- DIRECTORS DESK LLC (2009)
- EXPATEDGE PARTNERS LLC (2009)
- ONYX GRAPHICS, INC. (2009)
- PROGRESSIVE GAITWAYS LLC (2009)
- WORLD INNOVATORS, INC. (2009)
- AMERICAN APPAREL (2014)
- APPERIAN, INC. (2014)
- ATLANTA FALCONS FOOTBALL CLUB, LLC (2014)
- BAKER TILLY VIRCHOW KRAUSE, LLP (2014)
- BITTORRENT, INC. (2014)
- CHARLES RIVER LABORATORIES INTERNATIONAL, INC. (2014)
- DATAMOTION, INC. (2014)
- DDC LABORATORIES, INC. (2014)
- FANTAGE, INC. (2014)
- LEVEL 3 COMMUNICATIONS, LLC (2014)
- PDB SPORTS, LTD., D/B/A DENVER BRONCOS FOOTBALL CLUB (2014)
- REYNOLDS CONSUMER PRODUCTS INC. (2014)
- RECEIVABLE MANAGEMENT SERVICES CORPORATION (2014)
- TENNESSEE FOOTBALL, INC. (2014)
- AMERICAN INTERNATIONAL MAILING, INC. (2015)
- TES FRANCHISING, LLC (2015)
- GOLF CONNECT, LLC (2015)
- PINGER INC. (2015)
- NAICS ASSOCIATION, LLC (2015)
- JUBILANT CLINSYS, INC. (2015)
- IOACTIVE, INC. (2015)
- CONTRACT LOGIX, LLC (2015)
- FORENSICS CONSULTING SOLUTION, LLC (2015)

#### Never Self-Certified

- BALLS OF KRYPTONITE (2009)
- DALE JARRETT RACING ADVENTURE (2015)
- STERIMED MEDICAL WASTE SOLUTIONS (2015)
- CALIFORNIA SKATE-LINE (2015)
- JUST BAGELS MFG., INC. (2015)
- ONE INDUSTRIES CORP. (2015)
- INBOX GROUP, LLC (2015)
CONCLUSION

The FTC has had a mixed record in enforcement of the Safe Harbor. On the one hand, the enforcement program did pursue a large number of cases, accounting for 20 percent of the agency’s privacy enforcement actions over the past 15 years. On the other hand, most enforcement cases focused on allegations that were technical in nature, with only four cases alleging substantive violations and, even in those cases, Safe Harbor allegations mirrored identical allegations made under the FTC Act.

As the EU and U.S. finalize the Privacy Shield framework, an important issue remains the FTC’s authority to regulate U.S. companies’ data practices with regard to the information of European consumers. With the recent release of the details of the Privacy Shield, much will turn on the new mechanisms for collaboration between European authorities and the FTC and the new powers of the U.S. Department of Commerce to handle and resolve consumer complaints.