FPF

FUTURE OF PRIVACY FORUM

The US-EU Safe Harbor

An Analysis of the Framework's Effectiveness in Protecting Personal Privacy

December 2013

PREFACE FROM THE CO-CHAIRS OF THE FUTURE OF PRIVACY FORUM

As the Future of Privacy Forum (FPF) celebrates its fifth anniversary, we welcome the opportunity to participate in the discussions over trans-Atlantic privacy and, in particular, the effectiveness and utility of the EU-US Safe Harbor. For five years, FPF has been at the forefront of examining practical ways to advance responsible data practices. With an advisory board comprised of corporate privacy professionals, privacy scholars and consumer advocates, we play a unique role in the examination of contemporary privacy issues. Our current focus on the "Internet of Things," from Smart Grid to connected cars to retail analytics, is illustrative of our practical approach to protecting privacy while encouraging beneficial uses of data.

We want to thank a number of people for their input and work on this Report. FPF Fellows Joseph Jerome and Joe Newman took the laboring oar in researching and drafting. Our former colleague, Molly Crawford, who served as Policy Director when this project began, played a critical role in organizing this work. Thanks to members of the FPF Advisory Board who reviewed drafts. Thanks, too, to the government officials and business representatives whose input is reflected here, as well as to Bret Cohen and Jared Bomberg at Hogan Lovells US LLP for their editorial and production assistance.

We hope this report contributes to a constructive trans-Atlantic dialogue on ways to improve the protection of personal privacy.

Jules Polonetsky
Christopher Wolf

December 11, 2013
Washington, DC

EXECUTIVE SUMMARY

In November 2013, in the wake of the revelations about the National Security Agency's (NSA) widespread surveillance activities, the European Commission released a report critical of the United States (US) – European Union (EU) Safe Harbor program. The report found the Safe Harbor deficient in several respects and raised questions as to whether the agreement is enforced sufficiently.

The Future of Privacy Forum (FPF), a think tank seeking to advance responsible data practices, undertook its own assessment of the Safe Harbor program earlier this year as calls for revisiting the Safe Harbor grew. FPF has examined the enforcement activities and ongoing compliance work of the US Federal Trade Commission (FTC), US International Trade Administration (ITA), European Data Protection Authorities (DPAs) and third-party certification providers, and conducted in-depth interviews of executives of companies participating in the Safe Harbor program. The results of this investigation are presented in this report.

Section I of the report examines the creation of the Safe Harbor program, how it operates, and its fundamental objectives in protecting privacy rights *vis-à-vis* commercial entities. This context is important to today's debate over the NSA's access to data for national security purposes. The Safe Harbor was never envisioned as a mechanism to restrict the collection of data for national security purposes, and thus a reexamination of the program on that basis would be misfocused.

Section II discusses the significant growth of the Safe Harbor program both in the number and diversity of its members. Since its inception, the Safe Harbor has seen tremendous growth: in the last three years, more companies joined than in all the previous years combined. As of November 2013, over 4,000 companies have signed on to the Safe Harbor's privacy requirements. Additionally, the Safe Harbor now attracts companies from over 40 different industry sectors.

Section III finds that companies have taken extensive steps to comply with the Safe Harbor program. It provides case studies about Intel, Ancestry.com, and Procter & Gamble that highlight the array of compliance activities that companies must undertake. The section also outlines the role of third-parties such as TRUSTe, the Direct Marketing Association (DMA), and the Entertainment Software Ratings Board (ESRB) in helping companies achieve Safe Harbor compliance. FPF's research shows that companies spend considerable time monitoring and modifying their practices to meet the requirements of the Safe Harbor agreement. The section also points out the ITA's role in promoting Safe Harbor compliance.

Section IV finds that the Safe Harbor is effectively enforced by the FTC and third-party actors. The report shows that despite a lack of complaints from European DPAs, the FTC has used its authority to bring actions against companies for misrepresenting their membership in the Safe Harbor, and against companies that have failed to comply with substantive Safe Harbor requirements. Additionally, third-party dispute resolution providers such as TRUSTe and the

Council of Better Business Bureaus (BBB) handle complaints from EU citizens and are able to resolve many concerns without the need for legal action. The company executives we interviewed also noted that threats of FTC enforcement and damage to a company's reputation are significant drivers in ensuring diligent Safe Harbor compliance.

Section V responds to other criticisms of the Safe Harbor program, including: 1) its failure to prevent data from being accessed by the NSA; 2) the prevalence of false claims among its members; 3) a lack of transparency for individuals; and 4) the high costs associated with resolving an average Safe Harbor dispute. Some of these criticisms have been echoed by the European Commission and have cast doubt as to the EU's commitment to the Safe Harbor program. However, we find these criticisms to be misplaced or exaggerated.

- First, eliminating the Safe Harbor will not prevent the NSA from accessing EU citizens' data. The global economy, and particularly the transatlantic economy, will continue to rely on international data transfers, and when US-based companies are presented with a valid legal order from the US government for information, companies will be compelled to provide access to that data regardless of their membership in the Safe Harbor.

- Second, FPF research confirms that many companies imply they are involved with the Safe Harbor program even though their certifications have lapsed. However, this problem does not necessarily bear on the success of the program as a whole, because a company is still subject to FTC Section 5 enforcement for any substantive violations of the Safe Harbor principles committed while it claims to be a member. Absent evidence that the US companies cited as noncompliant are actually transferring data from the EU without adequate protections, it is premature to conclude that the Safe Harbor program is ineffective.

- Third, the complaints directed at the FTC misunderstand the organization's enforcement role. Even as the FTC agreed to give priority review to referrals by European DPAs, it appears that few complaints have ever been referred to the FTC. Despite this lack of involvement by the EU, the FTC on its own initiative has brought ten enforcement actions based on violations of the Safe Harbor. This suggests not a failure on the FTC's part, but rather reluctance on European DPAs to act. Moreover, the fact that the FTC does not respond directly to individual's complaints has little bearing on the success of its enforcement actions. All FTC investigations are non-public, as this secrecy facilitates the acquisition of evidence.

- Fourth, the ITA currently is engaged in the process of reducing arbitration costs. Working with dispute resolution providers, ITA has, among other things, helped dramatically reduce the costs of arbitration related to the Safe Harbor. The majority of

companies in the Safe Harbor program offer arbitration at no cost to the public. We encourage the elimination of fees for individuals seeking redress.

Section VI discusses the consequences of the EU suspending the Safe Harbor. The section shows that limiting the Safe Harbor's protections would weaken personal privacy protections for EU citizens. Under the Safe Harbor, the FTC has the capacity to enforce against US companies on behalf of EU citizens, simplifying complex jurisdictional issues. The Safe Harbor program also results in stronger investigatory and monitoring powers for the FTC. Moreover, alternatives to the Safe Harbor program as a mechanism of compliance with the EU Data Directive may not be feasible for all companies. These alternative mechanisms, including express consent, model contracts, and binding corporate rules, are either too inflexible or too difficult to implement at scale for the wide variety of companies that rely on the Safe Harbor and provide less transparency for regulators about data flows. Most critically, removing the Safe Harbor would do nothing to prevent surveillance by the US government or court orders that US companies must follow. Finally, restricting the ease of data flows between the EU and US could have a disastrous effect on the trans-Atlantic economy.

Section VII reviews the European Commission's proposed Safe Harbor reforms and recommends a number of additional measures to strengthen the Safe Harbor and further safeguard citizens' privacy. These reforms would increase membership in the Safe Harbor, provide individuals with more detailed information on how to enforce their rights, and increase collaboration between US enforcement agencies and EU DPAs.

With these reforms, as well as continued vigilance by regulators and compliance bodies, the Safe Harbor will become even more effective in safeguarding citizens' commercial privacy rights.

TABLE OF CONTENTS

I. INTRODUCTION: PRIVACY AND THE SAFE HARBOR

A. The Creation Of The Safe Harbor

With the rise of modern communications technology, data flows between countries have become instrumental in the development of nearly all areas of commerce; examples include companies that outsource human resources data or advertise overseas.[1] Organizations in both the United States (US) and the European Union (EU) benefit from online data transfers because they reduce costs and make possible client-focused advertising.[2]

However, with the benefits of new technology come new privacy risks. In the early 1990s, as the commercial "World Wide Web" was beginning to take shape,[3] many privacy advocates in EU Member States were concerned that the ease with which data could be moved across borders, combined with the difficulty of enforcing individual EU Member State privacy laws in foreign jurisdictions, would undermine the privacy of EU citizens.[4] These concerns prompted the EU to adopt the Directive on Data Protection in 1995.[5]

The EU Directive appointed a Working Party of the European Parliament to determine the adequacy of non-member countries' data protection regimes.[6] The Directive allowed the Commission to suspend all personal data flows to countries whose regimes were not deemed adequate.[7] Like nearly all countries' privacy regimes at the time, the US privacy regime was not deemed adequate.[8] However, prohibiting or significantly limiting data flows to the US would have threatened the underpinnings of all international electronic commerce – US-EU trade, for

---

[1] *See Safe Harbor Workbook*, EXPORT.GOV, http://export.gov/safeharbor/eg_main_018238.asp (last visited Oct. 9, 2013).

[2] *Id.*

[3] Tony Long, *Aug. 7, 1991: Ladies and Gentlemen, the World Wide Web*, WIRED (Aug. 7, 2007), http://www.wired.com/science/discoveries/news/2007/08/dayintech_0807 ("1991**:** The world wide web becomes publicly available on the internet for the first time.").

[4] *See Safe Harbor Workbook*, *supra* note 1.

[5] European Parliament and Council Directive 95/46/EC - on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* http://www.refworld.org/docid/3ddcc1c74.html (last visited Oct. 9, 2013) [hereinafter European Directive 95/46/EC].

[6] Robert R. Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2780 (2002), *available at* http://ir.lawnet.fordham.edu/flr/vol70/iss6/29; *Safe Harbor Workbook*, *supra* note 1.

[7] *See* European Directive 95/46/EC, *supra* note 5, at 57 ("the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited"); *Safe Harbor Workbook*, *supra* note 1.

[8] *See* Schriver, *supra* note 6, at 2785-86 ("In effect, 'the whole world' was considered noncompliant.") (citing Susan Binns, *Technical Briefing for Journalists on Data Protection – the EU/U.S. Dialogue* (Dec. 10, 1998), http://europa.eu.int/comm/internal-market/en/dataprot/backinfo/euus.htm). *See also Welcome to the U.S. –EU & U.S.-Swiss Safe Harbor Frameworks*, U.S. DEP'T OF COMMERCE, http://export.gov/safeharbor/ (last visited Oct. 9, 2013).

instance, amounted to approximately $560 billion in 2010.[9] To address the concerns about data transfers and to create a mechanism for US companies to comply with the Directive, the US Department of Commerce's International Trade Administration (ITA) and the European Commission (EC) developed the Safe Harbor program.[10]

B. The Safe Harbor Framework And Its Goals

The Safe Harbor's twin goals are to allow the flow of data between EU Member States and the US while protecting personal data.[11] Under the Safe Harbor program, which went into effect in November 2000, US companies may receive personal data about EU citizens so long as the US company certifies with the US Department of Commerce (DOC) that it adheres to the Safe Harbor privacy principles, described below.[12] The company also must be subject to the jurisdiction of either the US Federal Trade Commission (FTC) or Department of Transportation (DOT).[13] The FTC can bring enforcement actions under Section 5 of the FTC Act to challenge "unfair and deceptive practices in or affecting commerce" should the certifying company fail to live up to its Safe Harbor obligations.[14]

The obligations of the Safe Harbor program are stringent.[15] First, companies must submit a self-certification each year attesting that they are complying with the Safe Harbor program. Companies must provide follow up procedures for verifying that the attestations they make about their Safe Harbor privacy practices are implemented as represented and in accordance with the Safe Harbor principles.[16] This verification can be handled either by the company or by a designated third-party.[17] Second, they must adopt a privacy policy that is clear, concise, and easy for individuals to understand.[18] Third, companies must give adequate notice to individuals about what information is collected and how it is used, and they must give each person a

---

[9] *Safe Harbor Workbook*, *supra* note 1.

[10] *Id.*

[11] *Id.*

[12] *See id.*; Rebecca Herold, *European Union Data Protection Directive of 1995 Frequently Asked Questions*, COMPUTER SECURITY INSTITUTE ALERT (May 2002), *available at* http://www.informationshield.com/papers/EU%20Data%20Protection%20Directive%20FAQ.pdf.

[13] *See* Herold, *supra* note 12.

[14] *See Safe Harbor Workbook*, *supra* note 1; 15 U.S.C. § 45(a)(1)-(2) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.").

[15] *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated July 1, 2013) (outlining the seven Safe Harbor Privacy Principles: Notice, Choice, Onward Transfer, Access, Security, Data integrity, and Enforcement).

[16] *Safe Harbor Workbook*, *supra* note 1.

[17] *Id.*

[18] *Id.*

meaningful opportunity to opt-out of certain uses and disclosures.[19] Finally, companies must limit their onward transfer of data to only other trusted organizations, take reasonable precautions to preserve data security, take reasonable steps to ensure that data is reliable for its intended use and accessible to the public, and create effective and affordable mechanisms for processing individual complaints.[20]

Not all companies are eligible to participate in the Safe Harbor. Certain sectors are exempted from the jurisdiction of both the FTC and the DOT, and therefore may not rely on the Safe Harbor as a mechanism for complying with the EU's Directive on Data Protection.[21] The companies may still comply through other approved compliance mechanisms; for example, companies can obtain the express consent of the users providing the data, use certain standardized contractual clauses approved by the Commission (EU Model Clauses),[22] or adopt approved binding corporate rules (BCRs) that govern the international transfer of personal data.[23]

C. The Safe Harbor Under Attack

When the EU and the US originally launched the Safe Harbor, many Europeans criticized the program, considering it to be too lenient, particularly with respect to enforcement.[24] Meanwhile, US businesses initially complained that complying with the Safe Harbor was "costly, unworkable and unfair."[25] Despite these and other criticisms,[26] the agreement has contributed to

---

[19] *See id.*

[20] *See id.*

[21] *See id.*; European Directive 95/46/EC, *supra* note 5. These companies may include financial institutions, such as banks, investment houses, credit unions, and savings & loan institutions, as well as telecommunication common carriers, labor associations, non-profit organizations, agricultural co-operatives, and meat processing facilities. *Safe Harbor Workbook*, *supra* note 1.

[22] Commission Staff Working Document on the Implementation of the Commission Decisions on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (2001/497/EC and 2002/16/EC), SEC (2006) 95, *available at* http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/sec_2006_95_en.pdf ("[T]he contractual clauses provide for adequate protection of personal data.").

[23] *Overview on Binding Corporate Rules*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm (last visited Oct. 16, 2013).

[24] Schriver, *supra* note 6 at 2780-2781 (citing Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L L.J. 2024, 2048 (1999) ("From a European perspective, the key weakness of the U.S. model lies in its . . . still half-hearted approach to enforcement.")).

[25] *Id.* at 2793 (citing James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?* , 9 COMMLAW CONSPECTUS: J. COMM. L & POL'Y 145, 158 (2001)).

[26] *See, e.g.*, Commission Staff Working Document SEC (2004) 1323 of 20 October 2004 on the Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, *available at* http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf; CHRIS CONNOLLY, GALEXIA, US SAFE HARBOR – FACT OR FICTION? (2008), *available at* http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.

increased focus on privacy protection in the US and EU.[27] Moreover, the Safe Harbor has become a popular method of compliance with the EU's privacy requirements.[28]

Recently, however, revelations about the US National Security Agency (NSA) and its surveillance of EU citizens have resulted in a threat to upset the balance crafted by the Safe Harbor.[29] Specifically, leaks by former NSA contractor Edward Snowden have revealed that the NSA accessed private user data within the systems of Google, Facebook, Apple and other Internet giants.[30] Snowden's leaks showed that the NSA had collected search history, the content of emails, file transfers and live chats from millions of Internet users, including EU citizens.[31]

Some EU officials have seized on the NSA revelations in order to refocus scrutiny on the Safe Harbor. For instance, in August 2013, Viviane Reding, Vice-President of the European Commission (EC), called for a review of the Safe Harbor by year-end, calling the Safe Harbor "a loophole" that "may not be so safe after all."[32] Additionally, Jan Philipp Albrecht, a European Parliament Member, recommended that the EU discontinue the Safe Harbor program unless there is an express re-authorization following a review.[33] Jacob Kohnstamm, Chairman of the Article 29 Working Party, reminded EU Member States of their authority to suspend data flows where there is "substantial likelihood" that the Safe Harbor is being violated.[34] These criticisms

---

[27] *See* Damon Greer, *Safe Harbor—A Framework that Works*, INTERNATIONAL DATA PRIVACY LAW, May 26, 2011, at 1, *available at* http://idpl.oxfordjournals.org/content/early/2011/05/26/idpl.ipr010.full.pdf+html.

[28] *See* Brian Hengesbaugh et. al, *Why Are More Companies Joining the U.S. – EU Safe Harbor Privacy Framework?*, IAPP PRIVACY ADVISOR, Jan.-Feb. 2010, Volume 10, Number 1, at 1 (Kirk J. Nahra, ed.), *available at* http://www.bakermckenzie.com/files/Uploads/Documents/North%20America/GlobalCitizenship/ar_na_iapp_whyaremorecompaniesjoiningsafeharbor_jan-feb10.pdf.

[29] *See* Susan Neuberger Weller, *Should We Worry About Safe Harbor Being Suspended Because of the National Security Agency's (NSA) PRISM Program?*, NAT'L L. REV. (Oct. 18, 2013), http://www.natlawreview.com/article/should-we-worry-about-safe-harbor-being-suspended-because-national-security-agency-s.

[30] *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[31] *Id.*

[32] *See, e.g.*, Belinda Doshi & Robyn Chatwood, *European Union: Is "Safe Harbor" No Longer Safe? EU To Review Regime For Personal Data Transfers To The US*, MONDAQ (Aug 9, 2013), http://www.mondaq.com/x/256996/data+protection/Is+Safe+Harbor+No+Longer+Safe+EU+To+Review+Regime+For+Personal+Data+Transfers+To+The+US.

[33] Jan Phillip Albrecht, Committee of Civil Liberties, Justice and Home Affairs, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (Dec 17, 2012), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

[34] Winston Maxwell, *EU Privacy Authorities Request PRISM Details, Question National Security Safe Harbor Exception*, HOGAN LOVELLS (Aug. 19, 2013), http://www.hldataprotection.com/2013/08/articles/international-eu-privacy/eu-privacy-authorities-request-prism-details-allege-safe-harbor-breach/.

drew in part on reports from independent consulting service Galexia,[35] which published a report critical of the Safe Harbor program in 2008 entitled "The US Safe Harbor – Fact or Fiction?"[36] Galexia supplemented its study with additional findings presented at a 2013 Civil Liberties, Justice and Home Affairs (LIBE) Committee Inquiry on Electronic Mass Surveillance of EU Citizens.[37]

In November 2013, the European Commission released a report critical of the Safe Harbor agreement.[38] The Commission found that the framework has several shortcomings, including: a) a lack of transparency of privacy policies of Safe Harbor members; b) ineffective application of privacy principles by companies in the US, and c) deficient enforcement by the US.[39]

As this report will show, these criticisms of the Safe Harbor program are largely unfounded.[40] While the Safe Harbor program surely could be strengthened, as is the case with nearly every privacy regime, a close look at the experience that companies have had with the Safe Harbor reveals that the program has been largely successful in achieving its stated twin goals of protecting privacy while promoting international data transfer.[41] The success of the Safe Harbor can be seen in three distinct areas. First, the program has grown significantly since its inception, underlying the importance of trans-Atlantic data flows. Second, US companies have increased privacy protections for individuals by making modifications to their privacy practices in order to comply with the Safe Harbor's requirements. Third, there are strong enforcement mechanisms in place – in the form of both the FTC and third-party dispute resolution providers – to ensure that when individuals complain that a Safe Harbor participant is failing to live up to its obligations, such complaints are satisfactorily addressed.

Many critics have unfairly attacked the Safe Harbor based on a misunderstanding of the program and its goals, and many of the recent criticisms reflect a misunderstanding of the relationship between the program and the NSA's surveillance practices. In fact, suspending the Safe

---

[35] *About Us – Summary Profile*, GALEXIA, http://www.galexia.com/public/about/summary/ (last visited Oct. 16, 2013).

[36] CONNOLLY, *supra* note 26.

[37] Video of LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, Committee on Civil Liberties, Justice and Home Affairs (Oct. 7, 2013), *available at* http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131007-1900-COMMITTEE-LIBE.

[38] *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, at 18, COM(2013) 847 (Nov. 27, 2013), *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf [hereinafter EU Safe Harbor Recommendations].

[39] *See id.*

[40] *See* FTC Commissioner Julie Brill's Keynote Address, Forum Europe Fourth Annual EU Data Protection and Privacy Conference, Brussels, Belgium at 7 (Sep. 17, 2013), *available at* http://www.ftc.gov/speeches/brill/130917eudataprivacy.pdf ("I understand that Safe Harbor, in part because of its notoriety, is an easy target, but I ask you to consider whether it is the right target.") [hereinafter Brill Keynote].

[41] *See Safe Harbor Workbook*, *supra* note 1 (describing the Safe Harbor's twin goals).

Harbor's protections would negatively impact both the personal privacy of EU citizens and international trade. The Future of Privacy Forum (FPF) therefore suggests that rather than dismantling the Safe Harbor, the US and EU make specific reforms to the program to increase transparency and enhance efforts on both sides of the Atlantic to police compliance.

II. GROWTH OF THE SAFE HARBOR PROGRAM

The Safe Harbor program has experienced impressive growth in the number and the diversity of its members.

A. Total Participation Statistics

As of December 2013, 4,327 companies have certified compliance with the Safe Harbor program.[42] When the program launched in 2000, only four companies certified compliance.[43] By August 16, 2001, the number was still low, with 88 companies certifying compliance.[44] Although exact numbers for each year are not available, sources document that the Safe Harbor experienced a period of steady growth from 2002 to 2008, followed by a more dramatic acceleration in participation around 2009.[45]

---

[42] *Safe Harbor List*, EXPORT.GOV, https://safeharbor.export.gov/list.aspx (last visited Dec. 9, 2013).

[43] Greer, *supra* note 27.

[44] *See* Herold, *supra* note 12.

[45] *See* Commission Staff Working Document, *supra* note 22 (158 organizations were added to the Safe Harbor List in 2002 and another one hundred 156 in 2003; by November of 2003, the total number of companies that had self-certified was over 400); Damon Greer, *Safe Harbor May Be Controversial in the European Union, But It Is Still the Law*, IAPP PRIVACY ADVISOR (Aug. 27, 2013), https://www.privacyassociation.org/publications/safe_harbor_may_be_controversial_in_the_european_union_but_it_is_still_the (440 companies were members in 2004); Dan Cooper, *EU-US Safe Harbor Regime: Five Years On*, COVINGTON & BURLING DATA PROTECTION LAW & POLICY, November 2005, *available at* http://www.cov.com/files/Publication/b75b0e71-9293-445f-9685-8c1adbac4b2f/Presentation/PublicationAttachment/e98e1581-d44d-4d52-a454-8e5ffac7912a/oid64780.pdf (838 companies in 2005); Damon Greer, *The U.S.-E.U. Safe Harbor Framework*, presentation to the Conference on Cross-Border Data Flows, Data Protection, and Privacy, Washington DC, October 2007, http://www.SafeHarbor.govtools.us/documents/1A_DOC_Greer.ppt. (1,300 companies in 2007); CONNOLLY, *supra* note 26, at 4 (1,597 companies in 2008); *1746 Organizations In The U.S.'s EU Safe Harbor Program,* PRIVACY PROFESSOR (Mar. 12, 2009), http://privacyguidance.com/blog/?p=2719 (1,746 companies in 2009); Greer, *supra* note 26 (2,500 companies in 2011). Note that the numbers of participating companies in our graph will be slightly higher than actual participation due to double and triple entries on the Safe Harbor List as well as companies listed as "not current" at a given time. *See* CONNOLLY, *supra* note 26, at 7.

These growth trends are not surprising. In 2000, commentators blamed the tepid response towards the Safe Harbor on US businesses first wanting to see the consequences of abstaining from participation.[46] Other theories cited logistical challenges, bureaucratic delays, and a general reluctance to be the first to step into the spotlight.[47] These theories are consistent with the dramatic acceleration in registrations in 2007. By then, the Safe Harbor was well-established, many large companies were joining, and a "heightened awareness" had started to emerge in the business community of the importance of protecting privacy.[48] Looking at the original certification dates for the 3,328 companies listed as "current" on the DOC website as of December 2013,[49] more current companies joined in the last three or so years than all previous years combined.

---

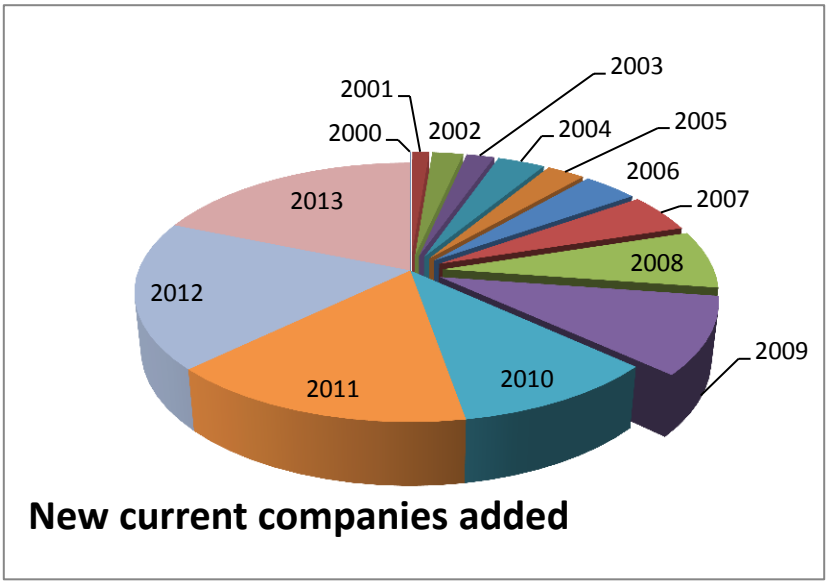
[46] Schriver, *supra* note 6, at 2793 (citing Margret Johnston, *U.S. To Kick Off Series of "Safe Harbor" Briefings*, INFOWORLD (Jan. 4, 2001), http://www.infoworld.com/artices/hn/xml/01/01/04/010104hnharbor.xml; Declan McCullagh, *Safe Harbor Is a Lonely Harbor*, WIRED NEWS (Jan. 5, 2001), http://www.wired.com/politics/law/news/2001/01/41004).

[47] *Id.* (internal citations omitted).

[48] Greer, *supra* note 44.

[49] *Safe Harbor List*, *supra* note 42.

Date	New current companies added
2000	2
2001	39
2002	71
2003	64
2004	109
2005	88
2006	126
2007	158
2008	235
2009	312
2010	341
2011	508
2012	603
2013	613



If current growth trends continue, Safe Harbor membership could grow to 6,000 participating companies by 2015.

B. Participation By Industry Sector

The Safe Harbor now attracts companies from a wider variety of industries than it did when it was first adopted.[50]

Information services and data processing-focused companies are the most represented type of industry, which is not surprising as these companies are the most directly involved in data transfer. Other major industries include: management consulting, drugs and pharmaceuticals and advertising. At least 40 other industries are also represented among participating companies.[51] The wide variety of industry sectors represented reveals the importance of data transfers for both economies.

III. PARTICIPATING COMPANIES' COMPLIANCE EFFORTS

The growth of the Safe Harbor would mean little for citizens' privacy if the companies involved did not actually adhere to the Safe Harbor's privacy principles. This section highlights a few of the many steps that US companies must take to comply with the Safe Harbor program. Companies spend considerable time changing their practices in order to comply. Moreover,

[50] Email from Christopher M. Hoff, Administrator, U.S. Department of Commerce, prepared for the European Commission (Oct. 18, 2013 10:04 EST) (current through September 23, 2013) (on file with author).

[51] *See id.*

third-party certification entities and the ITA play a vital role in ensuring that companies that wish to join the Safe Harbor program comply with its privacy requirements.

To analyze compliance efforts, the FPF has conducted in-depth interviews with key personnel responsible for Safe Harbor compliance at Intel, Ancestry.com, and Procter & Gamble.

A. Compliance Case Studies

i. Intel

Intel joined the Safe Harbor program in 2001. The company was motivated to join in part because at the time it had submitted BCRs that were still awaiting approval and the company believed it could benefit from a stable and clear legal framework to guide its data transfer practices. Additionally, Intel supported the Safe Harbor program because it saw it as a positive step in international cooperation to harmonize data transfer rules. David Hoffman, Intel's Director of Security Policy and Global Privacy Officer, worked on the initial certification process, along with Intel's General Counsel and Deputy General Counsel. Certification was handled largely in-house, although Intel also relied on public resources at the DOC's Safe Harbor website, consultations with outside counsel, and conversations with the FTC.

At the time of Intel's initial certification, the company already had a robust system in place to protect privacy. Intel performs company-wide legal compliance reviews annually and was able to incorporate the specific requirements of the Safe Harbor program into its existing compliance review framework. Nevertheless, early in the process the additional requirements of the Safe Harbor provided an impetus to enhance certain aspects of the company's program. For example, although Intel believes it was already compliant with the Safe Harbor principle of Onward Transfer when it initially certified its membership in the program, it invested more time and resources into reworking its contracts with vendors due to the Safe Harbor requirement.

David Hoffman said that the Safe Harbor adds "discipline" to the compliance review process: the fact that a company can be held responsible by the FTC for inaccurately claiming to be compliant "draws focus" to the proceedings and encourages the company to be vigilant. Intel's Director of Security Policy and Global Privacy Officer, the General Counsel, and the Deputy General Counsel hold a meeting on Safe Harbor each year prior to re-certification in order to ensure Intel is still fully compliant with the Safe Harbor program. Intel's Chief Executive Officer ultimately signs off on the certification.

Intel reported that it takes its obligations under the Safe Harbor seriously, not only because the threat of FTC enforcement is real, but also because failing to live up to the Safe Harbor program would cause significant harm to public trust in the company brand. To date, the company has not received any complaints about its compliance with the Safe Harbor.

ii. Ancestry.com

Ancestry.com is a recent addition to the Safe Harbor, first certifying in 2012. The company provides access to tools, public records, and data to help users learn more about their family history. It joined the Safe Harbor to legally transfer data between its US and foreign sites as well as to signify its commitment to privacy principles worldwide. Adam Sand, Ancestry.com's Associate General Counsel, led its Safe Harbor compliance efforts. The certification process was done in-house, though the company also relied upon information at the DOC's Safe Harbor website as well as information provided by TRUSTe and outside counsel.

When Ancestry.com first certified, it already had several security mechanisms in place to protect user data, and the company's privacy policies and practices were already accessible. To comply with the Safe Harbor's privacy requirements, the company compared the Safe Harbor's requirements to its existing procedures, identified gaps, and worked to resolve them. Ancestry.com relies on TRUSTe to verify its compliance with worldwide privacy principles including the Safe Harbor, provide alternative dispute resolution, and assist with its annual recertification. Compliance efforts required Ancestry.com to develop a more comprehensive system to allow for compliance auditing.

Ancestry.com's website provides clear instructions about how individuals can bring complaints about the company, and includes the Safe Harbor logo, which links to the DOC Safe Harbor website. Users can also contact TRUSTe for more information. To date, however, the company has received no complaints from users with regard to its compliance with the Safe Harbor.

Adhering to worldwide privacy principles and the Safe Harbor are a critical part of Ancestry.com's business. The company notes that a number of digitization projects of historical records from Europe would be in jeopardy if the Safe Harbor did not exist, and that user trust is an essential part of Ancestry.com's success.

iii. Procter & Gamble

The Procter & Gamble Company (P&G) joined the Safe Harbor in 2001. P&G joined the Safe Harbor because the program simplified its administrative burden for personal data transfers internally between various P&G subsidiaries and with outside service providers, and allowed P&G to complete those transfers without first getting authorizations from numerous EU DPAs. Joining the EU Safe Harbor Program also was a way to communicate to EU citizens, employees, and regulators that the company's privacy principles and practices are consistent with the privacy requirements in the EU Data Directive.

P&G's Global Privacy Office leads the annual review of P&G's Global Privacy Compliance Program. Prior to the annual Safe Harbor recertification, the P&G Privacy Office assesses the company's Global Privacy Compliance Program and reviews key compliance metrics with responsible executives. Privacy Office personnel present the Compliance Program review findings and support for recertification to the Vice President of General Internal Audit, who approves and signs the annual recertification. P&G then submits the Safe Harbor recertification

to the DOC. Preparing the annual review and submitting the recertification is a process that lasts several months and involves high-level executives within the company.

In addition to its annual recertification, P&G's Global Privacy Office works with key functions within the company to regularly review the company's business processes and compliance controls to assess privacy risks and address any identified gaps. P&G relies on the Council of Better Business Bureaus' (BBB) EU Safe Harbor dispute resolution program to handle EU and Swiss privacy complaints. P&G also relies on EU Model Clauses for transfers to third-party service providers that are not Safe Harbor-certified.

P&G operates and has employees in almost all EU countries. P&G collects data from individuals in EU countries via its websites and consumer inquiry services for business purposes such as providing requested offers, products and services, and improving its products and services. As a result, efficient transfer of data within and out of the EU is vitally important to the company. Specifically, P&G argues that the efficient data flow provided by the Safe Harbor is a critical enabler of innovation, efficient business operations and the growth of P&G's business. P&G also views as essential the trust of those who have provided their personal data to the company and considers the FTC to be an effective enforcer should the company fail to live up to its Safe Harbor obligations.

B. Role Of Third-Parties In Achieving Safe Harbor Compliance

As part of their compliance efforts, many companies also participate in third-party Safe Harbor certification programs. These third-party certification providers, such as TRUSTe,[52] the Direct Marketing Association (DMA),[53] and the Entertainment Software Ratings Board (ESRB)[54] are increasingly important players in the Safe Harbor system. This report examines the practices of two third-party certification providers: TRUSTe and the ESRB.

i. TRUSTe

TRUSTe offers one of the leading programs to help companies comply with the Safe Harbor's privacy requirements.[55] This program steadily has gained members for years:[56]

---

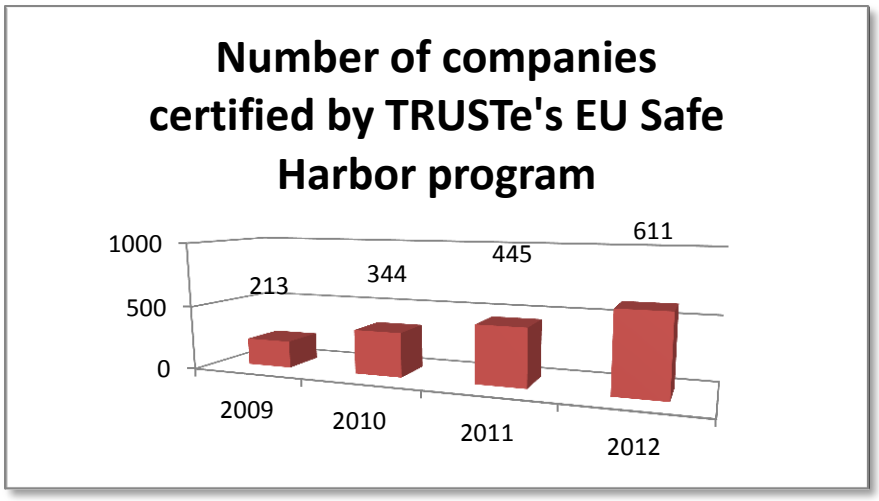
[52] *EU Safe Harbor*, TRUSTE, http://www.truste.com/products-and-services/enterprise-privacy/eu-safe-harbor-seal (last visited Nov. 4, 2013).

[53] *DMA International Safe Harbor Program for Business*, DMA, http://thedma.org/services/dma-international-safe-harbor/ (last visited Nov. 4, 2013).

[54] *ESRB Privacy Certified*, ESRB, http://www.esrb.org/privacy/index.jsp (last visited Nov. 4, 2013).

[55] *EU Safe Harbor Datasheet*, TRUSTE, http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=T5V6OKX8-7 (last visited Nov. 4, 2013).

[56] Email from Saira Nayak, Director of Policy, TRUSTe (Oct. 18, 2013) (on file with author).



All TRUSTe compliance programs, including verification of compliance with the EU Safe Harbor framework, begin with an assessment of a company's data collection practices.[57] This assessment consists of a manual review of these practices, the company's own attestations and interviews, and monitoring of ongoing compliance through TRUSTe's proprietary technology.[58] Once the assessment is complete, TRUSTe provides the client with a report that details which aspects of a client's existing practices or privacy policies must be changed to qualify for TRUSTe certification.[59]

TRUSTe's core Privacy Program Requirements satisfies the principles of the EU Safe Harbor Framework.[60] For example, TRUSTe requires that all companies bearing the TRUSTe mark or "seal" only use data for the purposes stated at the time of collection, and state as such in their privacy policies, provide choice for secondary uses that were not agreed to at the time of collection, and give individuals access to their personally identifiable information for the purpose of updating, correcting, or deleting it. TRUSTe also requires that companies take the steps required under the Safe Harbor Framework to finalize their certification, including registering with the DOC and adding a statement to their privacy policies discussing compliance with the EU Safe Harbor framework.[61]

Once the TRUSTe seal is awarded, TRUSTe monitors ongoing compliance through proprietary technology and an annual renewal process. Individuals can file a complaint by fax, mail, or online (by clicking on the TRUSTe EU Safe Harbor seal). Once a complaint is filed, TRUSTe

---

[57] *2012 TRUSTe Transparency Report*, TRUSTE (2013), http://www.truste.com/about-TRUSTe/transparency-report; Interview with Saira Nayak, Director of Policy, TRUSTe (Nov. 21, 2013).

[58] *Id.*

[59] *Id.*

[60] *See Safe Harbor Overview*, *supra* note 15.

[61] *Id.*

will initiate an investigation,[62] which may lead to enforcement actions, including suspension and, in rare cases, termination of the company's relationship with TRUSTe.

ii. The Entertainment Software Ratings Board (ESRB)

Although not as large as TRUSTe, the ESRB's Privacy Certified program has provided assistance with Safe Harbor applications for the past few years.[63] Ten of the ESRB's member companies have self-certified compliance with the Safe Harbor. Nine of these companies are interactive entertainment gaming companies; one is a virtual shopping site where parents can create accounts for their children.

ESRB conducts an in-depth review for compliance with the Safe Harbor program. A detailed compliance report outlines any required changes that must be made in order to achieve compliance. The ESRB also recommends changes based on industry best practices. Next, the ESRB reviews and proposes any necessary changes to the client's privacy policy. These policy changes may include the addition of language crafted and reviewed with the DOC. When the client company submits its application to the DOC, it notifies the ESRB, which then can be called upon to confirm that it is working with the company.

From start to finish, including the Department's approval of the application, the ESRB's certification process usually takes 1-2 months, although it may take longer, especially if portions of websites or applications must be rebuilt.

C. The ITA's Role In Promoting Safe Harbor Compliance

The US government actively seeks to ensure Safe Harbor compliance, and the ITA plays a vital role in overseeing the operation of the Safe Harbor program.[64] ITA staff review every Safe Harbor certification and annual recertification before it is finalized, and if a company's certification or recertification fails to meet Safe Harbor requirements, ITA staff contacts the company to notify them of needed clarifications or changes. In 2013, ITA staff notified 56 percent of first-time certifiers and 27 percent of recertifiers of the need to make clarifications or changes.[65]

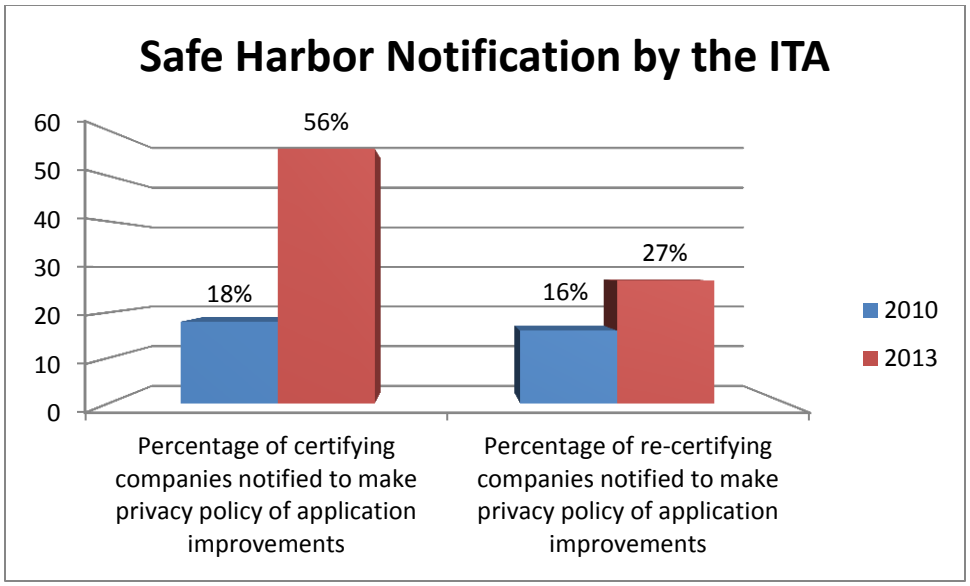
---

[62] TRUSTe may also initiate a compliance investigation based on the results of its technological monitoring, a regulator inquiry, or a media report.

[63] Letter from Dona J. Fraser, Vice President, Privacy Certified, ESRB (Oct. 11, 2013) (on file with author).

[64] State of Operation of the Safe Harbor Framework: 2013, Working Draft, U.S. Int'l Trade Admin. (on file with author).

[65] *Id.*



The ITA makes available a number of resources to companies that choose to become members, and companies also use the guides on the DOC's Safe Harbor website to achieve compliance.[66]

The company case studies, ongoing oversight by certification providers, and the ITA's increased oversight show that companies must take substantial steps to safeguard user privacy before they join the Safe Harbor program.

IV. COMPLAINTS AND ENFORCEMENT ACTIVITIES

The Safe Harbor's privacy principles are enforced by a variety of entities: specifically, the FTC, EU DPAs, and third-party dispute resolution providers such as TRUSTe and the BBB EU Safe Harbor program.[67] Companies that certify with the Safe Harbor are encouraged to resolve any complaints directly with individuals, but if the parties are unable to resolve their dispute, the Safe Harbor requires companies to provide readily available and affordable independent recourse mechanisms.[68]

This section discusses enforcement actions taken by the FTC and the European DPAs, and it highlights how third-party dispute resolution providers successfully have addressed complaints from European citizens about the privacy practices of Safe Harbor members.

---

[66] *Id.*

[67] *See Safe Harbor Workbook*, *supra* note1 ("How and Where Will the Safe Harbor Program be Enforced").

[68] *FAQ 11—Dispute Resolution and Enforcement*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018383.asp (last updated May 7, 2012).

A. FTC Enforcement Activities

The Safe Harbor is backed up by government enforcement of the federal and state unfair and deceptive statutes in the US.[69] If a company fails to abide by its public commitment to the Safe Harbor, it is immediately exposed to liability under the FTC Act and similar state statutes.[70] Under Section 5 of the FTC Act, for instance, the FTC can bring an action for equitable relief, including the ability to seek financial restitution, divestiture, and rescission.[71]

When the Safe Harbor was established, the FTC pledged to review any Safe Harbor complaints referred to it by either an EU Member State or a third-party self-regulatory organization on a priority basis.[72] To date, the FTC has received few complaint referrals from either EU Member States or third-party dispute resolution providers.[73] The FTC instead has pursued enforcement actions against companies for violating the Safe Harbor on its own initiative.[74] The FTC has brought ten separate enforcement actions for Safe Harbor violations and appears to have additional enforcement action planned for the near future – the Commission considers Safe Harbor enforcement to be a "top enforcement priority."[75]

In addition to the FTC's power to seek equitable relief,[76] it can impose steep penalties – up to $16,000 per violation or up to $16,000 per day in the case of a continuing violation – against companies that violate their settlement agreements.[77] As a result, settlement agreements are an essential tool used by the FTC to protect citizens on both sides of the Atlantic.[78]

---

[69] *U.S.-EU Safe Harbor Overview*, *supra* note 15.

[70] *Id.* ("Where an organization relies in whole or in part on self-regulation in complying with the Safe Harbor Privacy Principles, its failure to comply with such self-regulation must be actionable under federal or state law prohibiting unfair and deceptive acts or it is not eligible to join the safe harbor.").

[71] *See generally* Eugene Kaplan, *The Federal Trade Commission and Equitable Remedies*, 25 AM. U. L. REV. 173, 173-4 (1975) (discussing the FTC's broad power to design consent decrees in actions involving unfair and deceptive trade practices).

[72] *See, e.g.*, *FAQ 11*, *supra* note 68; Letter from Robert Pitofsky, Fed. Trade Comm'n, to John Mogg, European Comm'n at 2 (July 14, 2000), *available at*

http://export.gov/static/sh_en_FTCLETTERFINAL_Latest_eg_main_018455.pdf.

[73] Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework at 3 (Nov. 12, 2013), *available at* http://www.ftc.gov/os/closings/publicltrs/131112europeancommissionsafeharbor.pdf.

[74] FTC Chairwoman Edith Ramirez, Protecting Consumers and Competition in a New Era of Transatlantic Trade, Address of October 29, 2013, at 7, http://ftc.gov/speeches/ramirez/131029tacdremarks.pdf.

[75] Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework *supra* note 73, at 4.

[76] *See* 15 U.S.C. § 45(l)-(m) (2012).

[77] 15 U.S.C. § 45(1), as modified by the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461k (2012); *See, e.g.*, Complaint, US v. Google, Case No: 12-cv-04177-HRL at 12, http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf ("Each misrepresentation to Safari users by Google that it would not place the DoubleClick Advertising Cookie or collect or use interest category information…constitutes a separate violation for which Plaintiff seeks monetary civil

i. Balls of Kryptonite

In July 2009, the FTC brought its first enforcement action against an American company for violating the Safe Harbor principles. Balls of Kryptonite was a California-based consumer electronics retailer that actively sold merchandise in the UK.[79] In addition to falsely implying to customers that it was located in the UK and that its goods were intended for sale within the UK, Balls of Kryptonite also made false and misleading representations about its membership in the Safe Harbor.[80] On its website, Balls of Kryptonite stated that it had self-certified with the DOC and that it complied with the Safe Harbor when in truth, the company had never self-certified.[81]

The FTC argued that falsely claiming to be certified under the Safe Harbor violated the FTC Act regardless of the company's actual data privacy practices.[82] The FTC required Balls of Kryptonite to comply with the FTC Act and subsequently barred the company from making any further misrepresentations about the Safe Harbor.[83] This settlement also included a separate $500,000 fine.[84]

ii. The FTC's false membership settlements

Three months after bringing action against Balls of Kryptonite, the FTC announced settlements with six additional companies over charges that the companies had deceptively claimed membership in the Safe Harbor.[85] The FTC had alleged that Collectify LLC; Directors Desk LLC; ExpatEdge Partners LLC; Onyx Graphics, Inc.; Progressive Gaitways LLC; and World

---

penalties.") The FTC takes the position that each consumer record violation can be assessed a separate penalty under the FTC Act.

[78] Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), http://ftc.gov/opa/2012/08/google.shtm. Because of the FTC's initial settlement with Google, for example, the Commission was later able to levy a $22.5 million penalty, its largest penalty ever, against Google for violating its post-settlement privacy assurances. *Id.*

[79] Complaint, FTC v. Karnani, FTC File No. 092-3081, http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf.

[80] *Id.* at ¶¶ 8-9 (p. 3).

[81] *Id.* at ¶¶ 31-33 (p. 8).

[82] Anita Ramasastry, *The EU-US Safe Harbor Does Not Protect US Companies with Unsafe Privacy Practices*, FINDLAW (Nov. 17, 2009), http://writ.news.findlaw.com/ramasastry/20091117.html.

[83] Stipulated Final Order, FTC v. Karnani, FTC File No. 092-3081 at 4, http://www.ftc.gov/os/caselist/0923081/110609karnanistip.pdf.

[84] Press Release, Fed. Trade Comm'n, FTC Settlement Bans Online U.S. Electronics Retailer from Deceiving Consumers with Foreign Website Names (June 9, 2011), http://ftc.gov/opa/2011/06/bestbrands.shtm.

[85] Press Release, Fed. Trade Comm'n, FTC Settles with Six Companies Claiming to Comply with International Privacy Framework (Nov. 6, 2009), http://www.ftc.gov/opa/2009/10/safeharbor.shtm.

Innovators, Inc., deceived consumers by representing certification under the Safe Harbor program when in fact their certifications had lapsed.[86]

The six companies were involved in a variety of different industries, from online software and consulting services to medical equipment and list brokering services.[87] Each company had a privacy policy on its website that mentioned Safe Harbor membership, despite the fact the companies had allowed their annual certifications to lapse for significant periods of time.[88] The DOC listed these companies as "not current" members of the Safe Harbor during those periods, which allowed the FTC to easily ascertain that the companies were not in compliance with the Safe Harbor framework.[89]

Under the settlement agreements, all six companies are prohibited from misrepresenting the extent to which they participate in any privacy, security, or other compliance program sponsored by a government or any third-party.[90] The settlements further impose a series of compliance monitoring and reporting requirements on each company.[91] The companies must submit written reports to the FTC detailing the manner and form of their compliance, and are required to retain and make available to the FTC all documents relating to compliance for five years.[92] The settlement orders are effective for a period of twenty years.[93]

iii. Google, Facebook, and Myspace

Following these cases, the FTC began bringing enforcement actions that alleged specific violations of the Safe Harbor's privacy principles. In settlements agreed to by Google, Facebook, and Myspace, the FTC required each company to develop and implement comprehensive privacy programs and undergo regular independent audits for a period of twenty years.[94] Additionally, the Google and Facebook agreements required these companies to obtain

---

[86] *Id.*

[87] *Id.*

[88] *See, e.g.,* Complaint, *In re Collectify, Inc.*, File No. 092-3142 at 3; Complaint, In re Progressive Gaitways, Inc., File No. 092-3141. at 3-4.

[89] Press Release, *supra* note 85.

[90] *Id.*

[91] *See, e.g.,* Agreement Containing Consent Order, *In re Collectify, Inc.*, FTC File No. 092-3142 at 2-4 (Oct. 6, 2009), *available at* http://www.ftc.gov/os/caselist/0923142/091006collectifyagree.pdf.

[92] *Id.* at 3

[93] *Id.* at 4.

[94] Agreement Containing Consent Order, *In re Google Inc.*, FTC File No. 102-3136 at 7 (Mar. 30, 2011), *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf; Agreement Containing Consent Order, *In re Facebook, Inc.*, FTC File No. 092-3184 at 8 (Nov. 29, 2011), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf; Agreement Containing Consent Order, *In re Myspace LLC*, FTC File No. 102-3058 at 6 (May 8, 2012), *available at* http://www.ftc.gov/os/caselist/1023058/120508myspaceorder.pdf.

express affirmative consent from their users before making certain changes to their data sharing practices.[95]

1. The Google Buzz settlement

In 2011, the FTC brought a complaint against Google alleging that it had engaged in a variety of deceptive practices, and violated its own privacy promises during the launch of the company's Google Buzz social network in 2010.[96] When Google launched Google Buzz, it appeared to offer its Gmail users an option to opt-in to use Buzz. However, the FTC alleged that even users who attempted to opt-out still could have their information exposed to other Buzz users and could automatically be enrolled in Buzz without further notice.[97] The FTC further argued that Buzz "did not adequately communicate that certain previously private information would be shared publicly by default,"[98] and that information could be disclosed without customer permission.[99]

In addition to claiming that these actions were deceptive practices under Section 5 of the FTC Act, the FTC charged Google with violating the substantive principles behind the Safe Harbor.[100] Unlike the FTC's earlier actions, Google maintained a current, up-to-date self-certification with the Safe Harbor, and Google's privacy policy also explicitly stated that the company complied with the program.[101] According to the FTC, the launch of Buzz demonstrated that Google "did not adhere to the US Safe Harbor privacy principles of Notice and Choice" on behalf of its European users.[102]

Through Google Buzz, Google transferred data collected from Gmail users in Europe to the US for processing and to populate the Buzz social network.[103] According to the FTC, the launch of Buzz violated the Safe Harbor's privacy requirements because Google failed to gives its users notice before using information collected from Gmail.[104] Moreover, using that information to

---

[95] *Id.*

[96] *See, e.g.*, Complaint, *In re Google Inc.*, FTC File No. 102-3136 at 5-6 (Mar. 30, 2011), http://ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf.

[97] *Id.* at 3.

[98] *Id.*

[99] *Id.* at 4.

[100] *Id.* at 6-8.

[101] *See id.* at 7.

[102] *Id.* at 7-8. Specifically, the Safe Harbor requires that US companies that receive data about European consumers must (1) provide individuals with notice about how their data will be collected and used, and (2) offer individuals an opportunity to opt out of having their personal information disclosed to third-parties or be used for a purpose incompatible with the purpose for which the data was originally collected and consented to. *Id.* at 7.

[103] *Id.* at 7.

[104] *Id.* at 7-8.

build a social network like Buzz was incompatible with the purposes for which users originally gave that information, and Google failed to obtain the required user consent.[105]

The FTC's settlement with Google garnered significant media attention at the time and put companies on notice that they must comply with the Safe Harbor's requirements.[106] In addition to prohibiting any further misrepresentations about Google's compliance with the Safe Harbor, the settlement specifies that Google must obtain express, affirmative consent before sharing user information with third-parties.[107] Google now must to institute a comprehensive privacy program;[108] the program requires Google to (1) address any privacy risks related to the development and management of new or existing products and services and (2) protect the privacy and confidentiality of covered information.[109] Google also agreed to conduct regular, independent audits of its privacy program for the next twenty years.[110]

FTC Chairman Jon Leibowitz noted that this was "a tough settlement" that would ensure that Google "honor[s] its commitments to consumers and build[s] strong privacy protections into all of its operations."[111] Even without imposing direct monetary penalties, the FTC settlement nevertheless imposed substantial costs on Google's operations going forward.[112]

2. The Facebook settlement

The FTC brought a similar action against Facebook in August 2011. The FTC's complaint against Facebook contained eight counts, alleging Facebook failed to comply with privacy promises it had made to users over a period of years.[113] In particular, the FTC focused on a series of incidents through which Facebook's data practices resulted in the publication of previously private information and the sharing of user data with advertisers or third-parties

---

[105] *See id.* at 8.

[106] *E.g.*, Bianca Bosker, *Google's FTC Settlement Over Privacy Breach Makes History*, HUFFINGTON POST (Mar. 30, 2011), www.huffingtonpost.com/2011/03/30/googles-ftc-privacy-settlement-buzz_n_842490.html; Joe Mullin, *In Unprecedented Move, FTC Will Make Google Get Users' OK to Share Data*, PAIDCONTENT (Mar. 30, 2011), paidcontent.org/2011/03/30/419-google-deal-with-ftccompany-must-get-user-opt-in-before-sharing-data/.

[107] Settlement Order, *In re Google Inc.*, FTC File No. 102-3136 at 4, *available at*

http://ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

[108] *Id.* at 4.

[109] *Id.*

[110] Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://www.ftc.gov/opa/2011/03/google.shtm.

[111] *Id.*

[112] Katy Bachman, *FTC Goes After Google Over Social Network Buzz*, ADWEEK (Mar. 30, 2011), www.adweek.com/news/advertising-branding/ftc-goes-after-google-over-social-network-buzz-126102?page=2.

[113] Complaint, *In re Facebook, Inc.*, FTC File No. 092-3184, http://ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.

without appropriate notice or consent.[114] Similar to the Google action, the FTC alleged that Facebook failed to comply with the Safe Harbor, specifically its Notice and Choice principles.[115]

In response to the FTC's complaint, Facebook agreed to implement a comprehensive privacy program like the one required of Google.[116] The program addresses privacy risks and protects the privacy and confidentiality of users' information. For the following twenty years, the company agreed to undergo independent, third-party audits every other year to certify Facebook's program meets or exceeds the standards set in the FTC's order.[117] Facebook also is required to obtain affirmative express consent from users before enacting changes that would override their privacy preferences. It is barred from allowing access to information from deleted accounts after thirty days. Finally, the company is prohibited from misrepresenting the privacy or security settings it offers users.[118]

In a public statement, Facebook CEO Mark Zuckerberg admitted that the company had made a "bunch of mistakes."[119] He also announced the creation of two new corporate privacy officer positions to demonstrate the company's commitment to privacy moving forward.[120]

3. Myspace and Friend IDs

---

[114] The FTC focused on the following incidents in particular:

1. In December 2009, Facebook changed its website so that certain previously private information such as a user's Friends List was made public without warning or user approval;
2. Facebook represented that third-party apps had only limited access to user information, when in fact, apps could access nearly all of a user's personal data;
3. Facebook told users they could restrict information sharing to limited audiences such as "Friends Only," but selecting this option would not prevent user data from being shared with third-party applications their friends used;
4. Users' personal information was being shared with advertisers despite Facebook's promises to the contrary;
5. Facebook claimed that information from deactivated or deleted accounts would be inaccessible, but content remained accessible even after users removed their accounts.

The FTC further criticized Facebook's "Verified Apps" program for claiming to certify the security of third-party apps when, in fact, the program required no further action to verify application security other than Facebook's usual process for looking at applications. This charge, however, was not incorporated into the FTC's Safe Harbor complaint. Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.

[115] Complaint, *In re Facebook, Inc.*, FTC File No. 092-3184 at 19, http://ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.

[116] Agreement Containing Consent Order, *In re Facebook, Inc.*, FTC File No. 092-3184 at 8 (Nov. 29, 2011), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

[117] Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), www.ftc.gov/opa/2011/11/privacysettlement.shtm.

[118] *Id.*

[119] Mark Zuckerberg, *Our Commitment to the Facebook Community*, FACEBOOK (Nov. 29, 2011), https://www.facebook.com/notes/facebook/our-commitment-to-the-facebook-community/10150378701937131.

[120] *Id.*

One year later in May 2012, the FTC announced a settlement with Myspace based on charges alleging that the company misled its users about how their personal information was shared with advertisers.[121] According to the FTC, Myspace provided advertisers with "Friend IDs," persistent unique numerical identifiers of users who viewed particular pages on the site.[122] Friend IDs could be used in many cases to obtain both the user's Myspace profile and full name.[123] This information could then be combined with an advertiser's tracking cookie in order to learn detailed information about a user, including their broad web-browsing activities.[124]

Myspace's privacy policy stated that it did not share user data with advertisers without giving notice and obtaining consent, but the use of Friend IDs effectively provided advertisers easy access "to, at minimum, the user's basic profile information, which for most users includes their full name."[125] According to the FTC, this practice also violated the Notice and Choice privacy principles of the Safe Harbor.[126]

Like Facebook and Google before it, Myspace agreed to implement a comprehensive privacy program designed to protect user information, and to obtain biennial, independent assessments of its program for twenty years.[127] The settlement also prohibits the company from misrepresenting the extent to which it complies with a privacy program such as the Safe Harbor.[128]

B. European Enforcement Activities

European DPAs are intended to play a vital role in ensuring the efficacy of the Safe Harbor. The DPAs are national centers for data protection in each EU Member State. In addition to providing the FTC with complaint referrals, DPAs can help resolve disputes for EU citizens.[129] Complaints from EU Member States were envisioned as one of the primary mechanisms by which the FTC would evaluate compliance with the Safe Harbor and whether companies violated Section 5 of the FTC Act prohibiting unfair or deceptive practices.[130] The EC also recognized that the FTC

---

[121] Complaint, *In re Myspace LLC*, FTC File No. 102-3058 (Aug. 30, 2012), http://www.ftc.gov/os/caselist/1023058/120911Myspacecmpt.pdf.

[122] *Id.* at 1.

[123] *Id.* at 3-4. According to the FTC, the full names of 84% of Myspace users could be determined in this manner.

[124] *Id.* at 4.

[125] *Id.* at 5.

[126] *Id.* at 8.

[127] Press Release, Fed. Trade Comm'n, Myspace Settles FTC Charges That It Misled Millions of Users About Sharing Personal Information with Advertisers (May 8, 2012), http://www.ftc.gov/opa/2012/05/myspace.shtm.

[128] *Id.*; Agreement Containing Consent Order, *In re Myspace LLC*, FTC File No. 102-3058 at 3 (May 8, 2012), *available at* http://www.ftc.gov/os/caselist/1023058/120508myspaceorder.pdf.

[129] *See FAQ 11, supra* note 68.

[130] *See id.*

"is not there to take up large numbers of individual cases," but instead, serves as a backstop to ensure self-regulatory bodies and European DPAs can enforce and encourage compliance.[131]

As a result of EC's decision to embrace the Safe Harbor, an informal data protection panel was established by a collection of DPAs to investigate and resolve complaints by individuals against companies for violating the Safe Harbor.[132] Additionally, companies can elect to use the data protection panel as their dispute resolution provider.[133] As of 2013, FPF's research finds that approximately 1,712 companies under the Safe Harbor name European DPAs as their dispute resolution provider in some capacity.

The precise method in which European DPAs and the informal data protection panel operate to oversee the Safe Harbor is unclear. A 2004 report by the EC looked at the implementation of the Safe Harbor and noted that no one had yet referred a complaint to the panel.[134] The report cited "the lack of general information" about the panel's existence on both sides of the Atlantic as a primary reason for this, and suggested more public-facing efforts to educate the public about the data protection panel.[135] The FTC reports that the EU DPA panel has since received only four complaints, and has not resolved any of them.[136] Nearly a decade later, the panel continues to lack a public-facing website, and it seems unclear how European citizens can interact with the panel. Information about the panel's existence is relegated to several documents available on the EC's page.[137] According to the panel's standard complaint form, the panel will provide advice on the substance of a complaint within 90 days and will notify the complaining individual about the status of any complaint.[138] Individuals seeking information about the procedures used by the panel to handle complaints are only provided "some basic information in the form of a Q&A."[139] However, this note was initially written in July 2005, and appears not to have been updated

---

[131] *How Will the "Safe Harbor" Arrangement for Personal Data Transfers to the US Work?*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm#7 (last updated Oct. 9, 2012).

[132] DATA PROTECTION PANEL (July 25, 2005), http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_safe_harbour_en.pdf (citing 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council).

[133] *Id.*; *see also FAQ 5 - The Role of the Data Protection Authorities*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018378.asp (last updated May 7, 2012).

[134] Commission Staff Working Document, *supra* note 26.

[135] *Id.* at 12.

[136] Interview with Guilherme Roschke, Federal Trade Commission (Dec. 5, 2013).

[137] European Commission, *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/ (last updated July 16, 2013). Information about the Data Protection Panel is located under the section regarding the US Safe Harbor.

[138] Standard Complaint Form (Alleging Failure to Comply with "U.S. Safe Harbor Privacy Principles" Annexed to Commission Decision 2000/520) (2013), *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/files/ussh/complaint_form_20130206_en.pdf.

[139] *See* DATA PROTECTION PANEL, *supra* note 132.

since.[140] As a result, the EU DPA panel has not effectively made itself "readily available" to EU citizens.[141]

Before January 12, 2010, the FTC had not received a single complaint from an EU Member State regarding Safe Harbor compliance,[142] and has received only four since.[143] It is unclear whether this reflects either broad compliance with the Safe Harbor or inadequate investigatory and educational efforts on behalf of European DPAs.[144] FPF reviewed the national DPA websites of eight major EU Member States, and found that states are providing their citizens with varied and inconsistent information about the Safe Harbor. Basic information about the Safe Harbor varies greatly from one DPA's website to the next. Some websites, such as France's Commission nationale de l'informatique et des libertés (CNIL) and the UK's Information Commissioner's Office (ICO), provide extensive information about the Safe Harbor, whereas other countries, including the Austrian, Dutch, Italian and Spanish DPAs, provide very little. FPF's review also uncovered Safe Harbor resources that included broken or misdirected links, which suggests more could be done to education EU citizens by DPAs.

C. Third-Party Dispute Resolution Mechanisms

While the FTC serves to police the most systemic privacy violations, third-party compliance and dispute resolute providers are responsible for investigating and resolving most individual complaints and disputes that arise under the Safe Harbor and cannot be resolved internally within the company. European DPAs are the most frequently listed independent dispute mechanism under the Safe Harbor,[145] but third-party providers also play an important role in enforcing the

---

[140] *See id.*

[141] *Cf.* EU Safe Harbor Recommendations, *supra* note 38, at 19 ("ADR should be readily available . . .").

[142] Letter from Donald S. Clark, Secretary, Federal Trade Commission, to Chris Connolly, Galexia (Jan. 12, 2010), *available at* http://www.ftc.gov/os/caselist/0923140/100119directorsdesklletterconnolly.pdf. The recourse body responsible for human resources data-the EU Data Protection Panel-has received one complaint to date from a Swiss citizen concerning human resources data. EU Safe Harbor Recommendations, *supra* note 38, at 10.

[143] Interview with Guilherme Roschke, *supra* note 136.

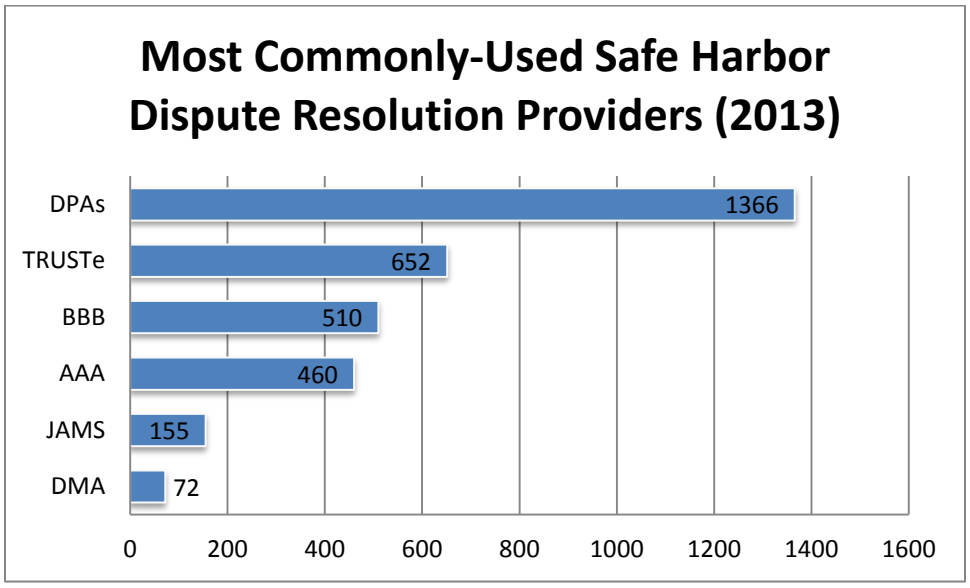
[144] For example, according to the Commission nationale de l'informatique et des libertés's (CNIL) 2011 Activity Report, most companies were found to be acting in good faith with regard to data protection practices. Out of 385 audits conducted in 2011, CNIL notes that only 15 were conducted on multinational companies that were granted access to transfer data outside the EU. CNIL concluded that, "these audits [had] not revealed any major lack of compliance with the authorizations granted, or any unsupervised transfers." COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 2011 ACTIVITY REPORT 64-66 (2012), http://www.cnil.fr/fileadmin/documents/en/Cnil-RA2011-EN/files/assets/downloads/files/CNIL-AR2011.pdf.

Similarly, in 2012, ICO's enforcement actions focused largely on violations by the public sector. ICO imposed 25 total fines, the vast majority of which were imposed for data security breaches. No enforcement proceedings were brought involving international data transfers. *E.g.*, FIELD FISHER WATERHOUSE, ICO ENFORCEMENT ACTION TRACKER: 2012--THE YEAR OF THE SECURITY BREACH FINE (2013), https://www.privacyassociation.org/media/pdf/knowledge_center/FFW-ICO_Enforcement_Action_Tracker_2012.PDF.

[145] *See Safe Harbor List*, *supra* note 42.

Safe Harbor. These organizations have the authority to apply sanctions in cases of non-compliance, publicly release non-compliance determinations, and force participating companies to delete data in the event of certain violations.[146]

TRUSTe and the BBB EU Safe Harbor program are the most commonly used third-party resolution providers, though other organizations active in Safe Harbor enforcement include the American Arbitration Association (AAA), the Direct Marketing Association (DMA), the ESRB, and JAMS (formerly Judicial Arbitration and Mediation Services).[147]



For the most part, these dispute resolution providers are designed to be used after an individual has made a good faith attempt to resolve a complaint directly with a company.[148] Providers offer complaint forms that ask for basic information about the nature of the complaint, responses

[146] *U.S.-EU Safe Harbor Overview*, *supra* note 15.

[147] *Safe Harbor List*, *supra* note 42. Statistics compiled by downloading the list of "current" organizations on the export.gov website as of October 2013, and sorting based on number of times a given entity was listed as an organization's dispute resolution provider.

[148] *See, e.g.*, *File a Complaint with BBB EU Safe Harbor*, COUNCIL OF BETTER BUSINESS BUREAUS, http://www.bbb.org/council/eusafeharbor/bbb-eu-safe-harbor-dispute-resolution-program/how-to-file-a-complaint-with-bbb-eu-safe-harbor/ (last visited Dec. 5, 2013). The European Data Protection Panel encourages individuals "to avail themselves of the consumer / user complaints services or contact points offered by the organisation which they consider has breached the 'Safe Harbor Privacy Principles.'" Standard Complaint Form (Alleging Failure to Comply with "U.S. Safe Harbor Privacy Principles"), Annexed to Commission Decision 2000/520) (2013), *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/files/ussh/complaint_form_20130206_en.pdf. Note that TRUSTe does not require any contact with the business prior to submitting a complaint through their service. Interview with Saira Nayak, Director of Policy, TRUSTe (Nov. 21, 2013).

received from the company, and the individual's desired resolution;[149] as described below, many providers now allow individuals to file their complaints online, as well.

i. TRUSTe EU Safe Harbor Program Alternative Dispute Resolution

TRUSTe provides the most commonly-used independent, third-party dispute resolution program.[150] European citizens have easy access to an online complaint intake system, and dispute resolution is provided to them at no cost.[151] TRUSTe considers the dispute resolution program to be a key component of its privacy management program, as it helps monitor compliance and ensure companies remain accountable for their privacy practices.[152]

After receiving a complaint or a regulator's inquiry, TRUSTe may initiate an investigation into the company's privacy practices; investigations of companies using TRUSTe's Safe Harbor certification program also may arise through routine scanning of a participating company's practices or press coverage.[153]

In 2012, TRUSTe responded to over 9,000 customer complaints against participating companies. 656 of those complaints were made by EU Member States or their citizens. Of that number, 428 ultimately were dismissed because they didn't involve violations of TRUSTe's compliance programs.[154] Of the remaining disputes, most were resolved through education activities, and four complaints required companies to makes changes to their privacy practices.[155]

ii. Council of Better Business Bureaus' BBB EU Safe Harbor Program

The BBB EU Safe Harbor dispute resolution program provides an online mechanism for EU citizens to bring complaints about potential Safe Harbor violations.[156] Individuals can access the mechanism directly on the BBB EU Safe Harbor website, or by means of a link placed in the

---

[149] *See, e.g.*, *Safe Harbor Line Complaint Handling Form*, The DMA Safe Harbor Program Guide for Consumers, http://www.dmaresponsibility.org/SafeHarbor/consumerassistance.shtml (last visited Oct. 15, 2013).

[150] *See Safe Harbor List*, *supra* note 42.

[151] *See TRUSTe Feedback and Resolution System*, TRUSTE https://feedback-form.truste.com/watchdog/request (last visited Nov. 29, 2013).

[152] TRUSTe, TRUSTE TRANSPARENCY REPORT 2012, at 11, *available at* http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=A94G2BBP-381.

[153] *Id.* at 11-12.

[154] *Id.* at 22. According to TRUSTe, 207 complaints were outside the scope of its compliance program, 86 received no consumer response, 82 required no action, and the remainder constituted largely duplicate complaints or provided no method for contacting the complainant. Although TRUSTe does not currently have numbers of specifically Safe-Harbor-related complaints, the organization plans to include a Safe Harbor-specific breakdown for their future data starting in 2014.

[155] *See id.*

[156] *BBB EU Safe Harbor*, THE COUNCIL OF BETTER BUSINESS BUREAUS, http://www.bbb.org/council/eusafeharbor/bbb-eu-safe-harbor-dispute-resolution-program/ (last visited December 5, 2013).

privacy policies of participating companies.[157] The program provides for the settlement of complaints with BBB EU Safe Harbor staff assistance, and also offers individuals the option of independent arbitration.[158] All of these services are provided free of charge to the public. In 2012, the BBB reviewed 121 complaints specifically relating to the Safe Harbor.[159]

Of the 121 complaints reviewed, the vast majority were outside of the program's jurisdiction.[160] For example, 103 complaints either did not involve a company participating in the BBB Safe Harbor program or were filed by a non-European consumer. Two complaints included insufficient information for the BBB EU Safe Harbor staff to act, and the complainants did not respond to the BBB EU Safe Harbor's request for additional information. Seven complaints did not relate to the company's privacy practices, and one complainant had not attempted to resolve the dispute with the company.

Eight cases were eligible for resolution in 2012.[161] Seven of those cases were settled by the BBB EU Safe Harbor staff to the individual's satisfaction. The remaining complaint was referred to an independent arbitrator at the individual's request, and a decision was issued in 2013.[162] The BBB EU Safe Harbor program experienced a similar complaint volume in 2011, resolving three cases to the individual's satisfaction and experiencing similar rates of complaints providing insufficient information or falling outside the program's jurisdiction.[163]

iii. Other third-party dispute resolution mechanisms

In addition to TRUSTe and the BBB EU Safe Harbor, other organizations run active dispute resolution programs. The DMA's Safe Harbor program is open only to members of the DMA.[164]

---

[157] Since 2011, BBB EU Safe Harbor has required new program participants to include specific language in their online privacy policies, including this "complaints" link, as a condition of acceptance into the program. *Privacy Policy Requirements*, THE COUNCIL OF BETTER BUSINESS BUREAUS, http://www.bbb.org/council/eusafeharbor/about/where-do-i-start/privacy-policy-requirements/ (last visited Dec. 6, 2013).

[158] *BBB EU Safe Harbor Procedure Rules*, THE COUNCIL OF BETTER BUSINESS BUREAUS http://www.bbb.org/council/eusafeharbor/about/rules/ (last visited Dec. 6, 2013). The Rules provide that participating companies who fail to implement the program's settlement agreements or independent arbitration decisions will be referred to the appropriate government agency (generally, the Federal Trade Commission), and the fact of the referral will be published in the program's annual Procedure Report. To date, no such referral has been required.

[159] THE COUNCIL OF BETTER BUSINESS BUREAUS, BBB EU SAFE HARBOR, 2012 PROCEDURE REPORT (2013), *available at* http://www.bbb.org/us/storage/16/documents/2012AnnualProcedureReport.pdf.

[160] *Id.* at 2.

[161] *See id.*

[162] *Id.*

[163] BBB EU SAFE HARBOR, 2011 PROCEDURE REPORT (2012), *available at* http://www.bbb.org/us/storage/16/documents/eu-safe-harbor/EU-Safe-Harbor-Annual-Complaints-Report-2011.pdf.

[164] DMA SAFE HARBOR PROGRAM REVIEW, DIRECT MARKETING ASSOCIATION 2 (Sept. 2013), http://thedma.org/wp-content/uploads/sh-status-report-sept2013.pdf.

The organization's Safe Harbor line received 121 complaints between January 2012 and August 2013.[165] Of the seven complaints it received from European consumers, three failed to identify the company being complained about, and another involved a technical support matter about a company not a member of the DMA, which was referred back to the company.[166] The remaining three complaints involved disputes about email opt-out programs with a DMA member, and each of the complaints was subsequently resolved by the DMA.[167]

Other dispute resolution programs have not received any complaints. According to the ESRB, it has not received any complaints under its Safe Harbor program, nor have any of the ten companies to which it provides dispute resolution services made the ESRB aware of any compliance problems.[168] Likewise, JAMS has yet to be called upon to resolve any disputes arising under the Safe Harbor.[169]

V. RESPONDING TO OTHER SAFE HARBOR CRITICISMS

In addition to the charge that US authorities are not ensuring compliance with the Safe Harbor agreement, officials in Europe recently have focused on the framework's law enforcement and national security exceptions. Moreover, some critics argue that the Safe Harbor is poorly enforced, rife with "false claims and non-compliance,"[170] lacking in transparency,[171] and too costly for the average person to resolve a dispute.[172] These criticisms have cast doubt as to the EU's commitment to the Safe Harbor program.

FPF conducted an independent examination of these issues and other criticisms of the program and found them to either be factually inaccurate or reflect a misunderstanding of how the Safe Harbor is designed to work.

---

[165] *Id.*

[166] *Id.* at 3-4.

[167] *Id.* at 2.

[168] Email from Dona J. Fraser, Vice President, Entertainment Software Rating Board (ESRB) (Oct. 11, 2013) (on file with author).

[169] Email from Kimberly Taylor, Senior Vice President and Chief Operating Officer, JAMS (Nov. 25, 2013) (on file with author). AAA has not responded to FPF's inquiries for information.

[170] Nikolaj Nielsen, *Hundreds of US Companies Make False Data Protection Claims*, EUOBSERVER.COM (Oct. 8, 2013), http://euobserver.com/justice/121695 (quoting Committee on Civil Liberties, Justice and Home Affairs, EUROPEAN PARLIAMENT/EPTV (Oct. 7, 2013), http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131007-1900-COMMITTEE-LIBE.).

[171] Chris Connolly, Galexia, *EU/US Safe Harbor–Effectiveness of the Framework in relation to National Security Surveillance*, Speaking / background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on "Electronic mass surveillance of EU citizens", Strasbourg (Oct. 7 2013), *available at* http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf.

[172] Connolly, *supra* note 171, at 6.

A. Suspending The Safe Harbor Over US Government Access To Data Misconstrues Its Purpose And Will Not Address European Citizens' Underlying Concerns

Scrutinizing the Safe Harbor over concerns about government access misconstrues the purpose of the Safe Harbor. The Safe Harbor is intended to bring US data practices in line with the EU Data Directive. The Directive does not apply to matters of national security or law enforcement.[173] Article 3 of the Directive states: "This Directive shall not apply to the processing of personal data…[with respect to] operations concerning public security, defen[s]e, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."[174] Thus, the Safe Harbor always had been envisioned as protecting the privacy of EU citizens within only the *commercial* privacy context.[175] It should come as no surprise then that the Safe Harbor specifically provides exceptions to the Safe Harbor's privacy principles "to the extent necessary to meet national security, public interest, or law enforcement requirements."[176]

Moreover, eliminating the Safe Harbor will not prevent the US government from accessing EU citizens' data. US-based companies that are presented with a valid legal order from the US government for information will nonetheless be compelled to provide access to that data regardless of their membership in the Safe Harbor. As a matter of policy, companies are pushing back against overbroad or unnecessary government information requests,[177] but most companies will be legally compelled to comply with US laws that authorize government access.[178] Companies can and should provide more information to European citizens about their obligation

---

[173] Directive 95/46/EC, *supra* note 5, at (43).

[174] *Id.*

[175] *See* Brill Keynote, *supra* note 40, at 6-7.

[176] U.S. DEP'T OF COMMERCE, U.S.-EU SAFE HARBOR FRAMEWORK: GUIDE TO SELF-CERTIFICATION 11 (2009), http://www.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf. *See also* Letter from Ciara O'Sullivan, Senior Compliance Officer, Irish Data Protection Authority, to Europe-v-facebook.org (July 23, 2013), *available at* http://www.europe-v-facebook.org/Response_23_7_2013.pdf (Irish DPA relying on the national security exception in the Safe Harbor to dismiss a consumer complaint about NSA surveillance).

[177] *"We Need to Know" Coalition Letter*, CTR. FOR DEM. & TECH. (July 18, 2013), https://www.cdt.org/weneedtoknow (major companies like Apple, Google, Microsoft, Facebook, Twitter and Yahoo! supported a call for increased transparency about government information requests).

[178] *See, e.g.*, *Verizon Exec Slams Google, Microsoft, Yahoo for NSA Lawsuit Grandstanding*, ZDNET (Sep. 17, 2013), http://www.zdnet.com/verizon-exec-slams-google-microsoft-yahoo-for-nsa-lawsuit-grandstanding-7000020769/ ("Stratton, the former chief operating officer of Verizon Wireless, said the company is "compelled" to abide by the law in each country that it operates in"); Michael Phillips & Matt Buchanan, *How Lavabit Melted Down*, NEW YORKER (Oct. 7, 2013), http://www.newyorker.com/online/blogs/elements/2013/10/how-lavabit-edward-snowden-email-service-melted-down.html (explaining how pressure from courts compelled one company to shut down rather than comply with a government subpoena); Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud* (2012), *available at* http://hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique.

to comply with US government data requests, but the existence of a national security exception does not by itself reflect a failure of the Safe Harbor to achieve its goals.

The EC has suggested that any legitimate national security exception be used "only to the extent that it is strictly necessary or proportionate."[179] The Commission has not offered any further guidelines as to what would constitute what is "necessary" or "proportionate," and none of the regulators that enforce the Safe Harbor, including the FTC, are in a position to determine the scope of this exception.

Absent a more comprehensive agreement between the EU and the US regarding government surveillance, the only way to address these concerns would be to prohibit all transfer of data into the US. The damage this would cause to the trans-Atlantic economy would be considerable, and would do little to help EU officials influence US surveillance programs. Limiting the Safe Harbor would therefore be a misplaced effort to address larger questions about the scope of the NSA's surveillance operations.[180]

B. Claims Made By Non-Current Companies Are Not Necessarily Relevant To Personal Privacy

Speaking at the LIBE hearing in October, 2013 Chris Connolly of Galexia argued that "[i]t would be dangerous to rely on Safe Harbor to manage any aspect of the specific national security issue we face now without first addressing the broader issue of false claims and non-compliance."[181] FPF's research reveals that approximately 10% of companies have not accurately represented their status in the Safe Harbor program, but FPF cautions that the impact of this problem should not be overblown.

Connolly found that there were 427 inaccurate claims of compliance in September 2013.[182] Out of 4,277 companies in the Safe Harbor at the time of FPF's study, an analysis of the privacy policies of the approximately 975 companies listed as "Not Current" on the Safe Harbor List reveals that 446 of them (approximately 10%) make some reference to the Safe Harbor in their policy. This number is similar to the number of "inaccurate" claims mentioned at the September 2013 hearing, although not all of these companies are necessarily subject to FTC enforcement under Section 5.[183] Although FPF's research confirms that some companies' claims of

---

[179] EU Safe Harbor Recommendations, *supra* note 38, at 20.

[180] Erin Mershon, *U.S. to EU: Don't scapegoat Safe Harbor over NSA*, POLITICO (Nov. 7, 2013), http://www.politico.com/story/2013/11/us-european-union-safe-harbor-nsa-99495.html.

[181] Connolly, *supra* note 171; Giusy Cannella, *LIBE Series 6: Safe Harbor under scrutiny by the European Parliament*, ACCESS BLOG, (Oct. 15, 2013), https://www.accessnow.org/blog/2013/10/15/libe-series-6-safe-harbour-under-scrutiny-by-the-european-parliament.

[182] *Id.*

[183] Only 294 of these organizations actually make a clear claim to be active, compliant participants in the Safe Harbor program; the other 152 organizations contain a policy that only evidences a commitment to follow the

membership are inaccurate or outdated, this fact should not lead to the conclusion that the Safe Harbor as a whole is ineffective.

The Galexia methodology recorded a "false claim" whenever a given company allowed its annual Safe Harbor re-certification to lapse but did not change its public statement to remove its claim of membership.[184] In fact, a company's annual certification may have lapsed due to paperwork errors, such as delays in remitting payment of the necessary processing fee, or the company simply forgetting about its annual obligation to renew its certification. A non-current company may be also listed as noncurrent because it has withdrawn from the Safe Harbor program: the company may have chosen to use other approved data transfer mechanisms, merged with another company, ceased data transfer with the EU, or shut down altogether.

It is important to note that if a company claims in its privacy policy to abide by the Safe Harbor Principles and its practices are inconsistent with the substantive requirements of the framework, the FTC can bring an enforcement action against that company *regardless* of whether or not its certification is current.[185] So long as the company makes a claim to be compliant with the Safe Harbor principles, the FTC retains its enforcement hook.

Moreover, so long as the non-current organization's privacy claims are not *deceptive* – the companies may still be abiding by the Safe Harbor principles in practice – then the lapsed certification does not bear on user privacy. Absent evidence that the US companies cited as noncompliant are actually transferring data from the EU without adequate protections, it is premature to conclude that the Safe Harbor program is ineffective.

Nevertheless, false claims of membership in the Safe Harbor program create confusion in the marketplace, undercut trust in the program, and are violations of the FTC Act. FPF therefore calls on the FTC to conduct a thorough review of these claims and take appropriate enforcement actions.

C. The Perceived Lack Of Transparency At The FTC Misunderstands The Organization's Enforcement Role

At the October LIBE hearing, Connolly also criticized the FTC for not responding to individual complaints. He pointed out that the FTC does not provide information about its process or the

---

"Principles" of the Safe Harbor without actually maintaining their active membership. A company can subscribe to the underlying principles of the Safe Harbor such as Notice and Choice without being active participants in the program; therefore the policies of these non-current participants are not necessarily inaccurate.

Moreover, of the 294 companies that clearly make a claim to be compliant, only 180 companies have been noncurrent for more than a year. It is likely that many of the 114 companies that only recently lapsed are either in the process of having their certification approved, or are waiting to see if the Safe Harbor program will be suspended before resubmitting their certification. That leaves only 180 companies who can be considered "serious" violators.

[184] *See* Connolly, *supra* 171, at 4.

[185] EU Safe Harbor Recommendations, *supra* note 38, at 12.

contact details of the person managing the complaint, and it has no obligation to explain the decisions it makes.[186] This criticism misunderstands the role of the FTC within the Safe Harbor program.

The Safe Harbor agreement never envisioned the FTC to be the initial point of contact for EU complaints with respect to Safe Harbor compliance. Rather, the framework is designed so that European citizens should report problems to their local DPA, who would refer the complaint to the FTC.[187] Even as the FTC agreed to give priority review to referrals by European DPAs, it appears that few complaints have ever been referred to the FTC. Despite this lack of involvement by the EU, the FTC on its own has brought ten enforcement actions based on violations of the Safe Harbor.[188] This suggests not a failure on the FTC's part, but rather reluctance on European DPAs to act.

Likewise, the fact that the FTC does not respond directly to individual complaints has virtually no bearing on the success of its enforcement actions. All FTC investigations are non-public.[189] These investigations must be secretive in order to facilitate the acquisition of evidence. Individuals do not necessarily expect full transparency so long as the offending business practices are ended.

D. Concerns About The Costs Of Arbitration Are Being Addressed By The ITA

We have seen that, in the past, certain companies selected as their dispute resolution mechanism arbitration providers that were too expensive for individuals, discouraging complaints. In 2008, for instance, the American Arbitration Association (AAA) charged between $120 and $1,200 per hour (with a four-hour minimum charge) to resolve individual complaints.[190] These rates can discourage the average individual to pursue a claim.

Over the past two years, the ITA took on the problem of expensive dispute resolution providers and worked with a number of companies, including the AAA, to develop a Safe Harbor-specific program which reduced AAA's cost to individuals from several thousands of dollars to a flat fee of $200.[191] Additionally, the fees for the BBB, DMA, EU DPAs, and TRUSTe all are $0.[192]

---

[186] *See* Connolly, *supra* 171, at 4.

[187] *See* Schriver, *supra* note 6, at 2813.

[188] *Infra* § IV.A.

[189] *Federal Trade Commission Resources for Reporters*, FED. TRADE COMM.'N, http://www.ftc.gov/opa/reporter/ (last visited Nov. 6, 2013). However, if a company itself announces that it is the subject of an FTC investigation, the FTC can confirm that fact.

[190] Draft ITA State of Operation of the Safe Harbor Framework: 2013, ITA working draft (on file with author).

[191] *Id.*

[192] *Id.*

FPF welcomes the trend and encourages the elimination of fees for all complaints. Individuals should not have to go out-of-pocket to resolve their privacy claims.

VI. CONSEQUENCES OF A SUSPENDED SAFE HARBOR

As described above, some members of the European Parliament are calling for a suspension or curtailing of the Safe Harbor agreement.[193] This report has thus far focused on the growth of the Safe Harbor program, the significant amount of work companies have done in achieving compliance, and the measures regulatory bodies and organizations have taken to enforce the rules. However, all of that progress would be lost or severely hampered if the Safe Harbor program were suspended.

As described in Section II above, the Safe Harbor has grown significantly in the past three years.[194] Note in particular the 613 companies that joined the program just within the last year, presumably in reliance on the assumption the program would continue.[195] Many of these companies have expended significant time and resources into joining the Safe Harbor program,[196] and that investment would be wasted if the Safe Harbor were suspended or its protections removed.

Moreover, if the Safe Harbor were discontinued, the negative impact on both personal privacy and international trade would be serious. First, jettisoning the Safe Harbor would mean removing an important player to enforce privacy protection for EU data subjects – namely, the FTC.[197] Second, alternative transfer mechanisms to the Safe Harbor program may not be feasible for all companies. Rather, limiting Safe Harbor protection would only destroy critical US and EU privacy protections.

A. Lack Of Comparable Enforcement Regimes

The Safe Harbor is unique among the available data protection compliance regimes in that, unlike other data transfer mechanisms, the Safe Harbor gives the FTC authority to police US companies on behalf of EU citizens.[198] Dismantling the Safe Harbor and its requirement that

---

[193] *Infra* § I.C; Christopher Wolf, *Has the LIBE Committee Torpedoed the Safe Harbor?*, IAPP PRIVACY PERSPECTIVES (Oct. 21, 2013), https://www.privacyassociation.org/privacy_perspectives/post/has_the_libe_committee_torpedoed_the_safe_harbor; Giusy Cannella, *LIBE Series 6: Safe Harbour Under Scrutiny By The European Parliament*, ACCESSNOW (Oct. 15, 2013), https://www.accessnow.org/blog/2013/10/15/libe-series-6-safe-harbour-under-scrutiny-by-the-european-parliament.

[194] *Infra* § II.A.

[195] *See id.*

[196] *Infra* § III.

[197] Wolf, *supra* note 193.

[198] Brill Keynote, *supra* note 40, at 7.

companies publicly commit to compliance would result in a significant loss of FTC oversight.[199] In such a scenario, the FTC would no longer be able to bring enforcement actions for the benefit of EU citizens, nor would it be able to monitor US companies for their compliance, resulting in less transparency and less protection for individuals.[200]

Additionally, if the FTC were unable to regulate companies that undermined EU citizen privacy, it would fall on the EU Member States to enforce the EU Data Directive. Suing US companies with no physical presence in the EU could result in jurisdictional chaos.[201] Likewise, without the FTC monitoring US companies' compliance efforts, violations would be much harder to investigate and detect.[202] In the alternative, EU Member States could focus their regulatory efforts on EU companies transmitting data to the US. However, this would place an unfair burden on EU companies, who could be held responsible any time a US recipient of personal data committed a violation. EU companies would likely react to this fundamentally unfair regime by either limiting trade with the US, or including broad indemnity provisions into future data transfer agreements, either of which would significantly burden business in both the US and EU.

B. Lack Of Feasible Data Transfer Alternatives

Suspending the Safe Harbor would force US companies seeking to comply with the EU Data Protection Directive to revert to other compliance methods such as express consent, EU Model Clauses or BCRs.[203] While these mechanisms may be adequate to comply with the EU Data Directive,[204] not all companies can realistically implement them.

i. Problems with mass adoption of express consent

The express consent method requires the US company to obtain the express consent of any EU citizen about whom the company wishes to transfer data.[205] Relying solely on this method is not practical for many companies. First, larger companies would find it extremely difficult to obtain express user consent on such a large scale. Furthermore, even if consent were obtained, it would not necessarily be enough for compliance: recent opinions by DPAs have held that many

---

[199] *Id.*

[200] *See id.*

[201] *See id.;* Marc H. Greenberg, *A Return to Lilliput: The* LICRA v. Yahoo! *Case and the Regulation of Online Content in the World Market*, 18 BERKELEY TECH. L.J. 1191, 1191 (2002), *available at* http://www.btlj.org/data/articles/18_04_05.pdf (discussing, for instance, the heated jurisdictional dispute that arose when French authorities brought suit against Yahoo!'s internet auction service for maintaining online auctions and information sites about Nazi memorabilia).

[202] *See* Brill Keynote, *supra* note 40, at 7.

[203] Hengesbaugh et. al, *supra* note 28, at 1.

[204] *See id.*

[205] *Id.*

instances of consent, particularly by employees, are not "freely given" and therefore invalid.[206] Gaining the affirmative, "freely given" consent of all European internet users and employees would be practically impossible; companies would have to significantly scale back their data transfers under this method.

ii. Problems with mass adoption of EU Model Clauses

EU Model Clauses are model agreements a company can sign to govern its data transfers.[207] The major problem with relying on EU Model Clauses for all data transfer from the EU to the US is that such contract privisions fail to provide sufficient flexibility for companies with unique business models. All EU Model Clauses "must be copied verbatim and strictly adhered to," and any revisions must be individually approved by each European DPA.[208] Compared to the Safe Harbor program, EU Model Clauses have particularly inflexible rules with respect to onward transfer of data to third-parties, prohibiting transfers unless the recipient also agrees to the model contractual terms.[209] In the context of court orders in e-discovery or litigation, or in the case of data transfers that are necessary to perform a contract, such strict rules would be extremely difficult for a company to comply with.[210] Given the wide variety of companies that rely on the Safe Harbor,[211] such rigid contractual clauses would stifle trade, prevent innovative uses of data, and, for small businesses in particular, hamper their ability to provide basic operational support for their business.

Additionally, EU Model Clauses are inserted into purely *private* agreements between companies, and are therefore significantly less transparent than privacy policies under the Safe Harbor program. Heightened use of EU Model Clauses would deprive EU regulators of the benefit of transparent documentation found in the Safe Harbor's requirements.

iii. Problems with mass adoption of Binding Corporate Ruels

BCRs effectively constitute full-blown privacy programs for a company to follow.[212] While BCRs are appropriate for large global organizations with the resources and expertise to develop and enforce them,[213] they would not be a workable solution for smaller companies. Binding

---

[206] *See id.*

[207] *See* Kelsey Finch, *Treacherous Waters: What the World Would Look Like Without Safe Harbor*, IAPP PRIVACY TRACKER (Oct. 22, 2013), https://www.privacyassociation.org/privacy_tracker/post/treacherous_waters_what_the_world_would_look_like_without_safe_harbor.

[208] *Id.*

[209] Hengesbaugh et. al, *supra* note 28, at 6.

[210] *Id.*

[211] *Infra* § II.A.

[212] Finch, *supra* note 207.

[213] Hengesbaugh et. al, *supra* note 28, at 5.

corporate rules must be legally enforceable, taking into account the legal systems of each country where they may be applied; additionally, all BCRs must be submitted for approval to the DPA in each member state from which data would be transferred.[214] Getting all the EU Member States aligned and supportive of a single policy has been described as an "administrative nightmare";[215] if the over 3,000 current Safe Harbor member companies submitted their own BCRs for approval, it would grind the system to a halt.

Moreover, BCRs only cover intra-agency data transfers, and do not cover transfers to or from unaffiliated parties (*e.g.*, service providers, business partners, M&A parties).[216] As of 2013 there were fewer than 50 companies for which the BCR cooperation procedure was closed.[217] While there have been some positive efforts made to streamline the BCRs approval process,[218] until such procedures are edified it would make little sense to rely on BCRs over the much more practical Safe Harbor program.

VII. RECOMMENDATIONS FOR IMPROVEMENTS

Although this report concludes that the Safe Harbor framework is successfully achieving its goals, there are several ways in which the parties to the agreement could improve its effectiveness. The EC's recent report on the Safe Harbor made 13 recommendations to reform the U.S. privacy framework.[219] This section analyzes those 13 recommendations and makes additional recommendations for EU and US policymakers to consider.

A. The EC's 13 Recommendations

i. Safe Harbor participants should publicly disclose their privacy policies.

FPF agrees that Safe Harbor participants should clearly disclose their privacy policies online. The FTC, ITA, and third-party certification providers should routinely check for compliance.

---

[214] Finch, *supra* note 207.

[215] Cynthia J. Larose, *European Union: Discussing Binding Corporate Rules: An Interview With Sue Foster (Video)*, MONDAQ (Oct. 18, 2013), http://www.mondaq.com/unitedstates/x/269608/data+protection/Discussing+Binding+Corporate+Rules+An+Interview+With+Sue+Foster (statement of Sue Foster).

[216] Hengesbaugh et. al, *supra* note 28, at 2.

[217] *See List of companies for which the EU BCR cooperation procedure is closed*, EUROPEAN COMMISSION: JUSTICE, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last visited Nov. 5, 2013).

[218] Larose, *supra* note 215.

[219] EU Safe Harbor Recommendations, *supra* note 38.

ii. Privacy policies of participants should always include links to the Department of Commerce's Safe Harbor list of current members.

FPF agrees that Safe Harbor participants should always include links to the DOC Safe Harbor list of current members.

iii. Safe Harbor companies should publish the privacy conditions of all contracts with subcontractors.

FPF opposes requiring participants to publish the privacy conditions of all contracts with subcontractors, provided the participant's privacy policy provides individuals with all relevant privacy rights. This is more than entities directly covered by laws promulgating the EU Data Protection Directive are required to do. Requiring these disclosures would place an unnecessary burden on participants, would do little to improve privacy, and could discourage adoption of the Safe Harbor. It is incumbent upon participants to ensure compliance, including through the use of subcontractors, regardless of the publication of contract language.

iv. The Department of Commerce should clearly indicate on its website all companies which are not current members.

FPF agrees that the DOC should clearly indicate on its website all companies that are not current members, assuming that refers to lapsed participants in the program. FPF further recommends that the DOC should describe, in general, the reasons why a company may be inactive, including the fact that companies still may be in compliance with the EU Data Directive employing other legal mechanisms. To the extent the DOC knows the reasons for a company's inactive status, it should strive to include this information online to better inform the public.

v. Safe Harbor privacy policies should include links to dispute resolution bodies.

FPF agrees that privacy policies of participants should include links to dispute resolution bodies or an indication that an EU DPA is empowered and designated to adjudicate disputes. It also would be helpful on the EU side to include an active link to a site containing information related to the EU Data Protection Panel, and/or contact information for the citizen's relevant national DPA.

vi. Alternative dispute resolution mechanisms addressing Safe Harbor disputes should be affordable and readily available.

FPF agrees that alternative dispute resolution mechanisms should be affordable and readily available. The DOC has worked with alternative dispute resolution providers to significantly lower the cost of these programs. The Department should continue to reduce the costs of these

services and work with companies to address any problems that arise, with the goal of creating zero-cost arbitration for all affected individuals.

vii. The DOC should monitor the transparency and effectiveness of alternative dispute resolution bodies.

FPF agrees that the DOC should monitor the transparency and effectiveness of alternative dispute resolution bodies.

viii. A certain percentage of Safe Harbor-certified companies should be subject to ex officio *investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements).*

FPF supports strong oversight of the Safe Harbor program but opposes requiring a fixed percentage of participants to be subject to an official compliance review each year. Imposing a fixed percentage would create metrics for enforcement agencies that emphasize quantity over quality, and would divest the agencies of their regulatory discretion. Moreover, allowing an enforcement body such as the FTC to investigate a company's privacy practices without any prior complaint or reasonable suspicion would create an unreasonable burden on business, waste government resources and lead to abusive "fishing expeditions" into the privacy practices of thousands of US businesses.

ix. Safe Harbor participants found not to be in compliance should be reinvestigated the following year.

FPF opposes rigid enforcement procedures as they unnecessarily tie the hands of enforcement agencies. While enforcement agencies should pay close attention to participants that have a history of non-compliance, mandating that each of these companies be reviewed every year following an issue of non-compliance may take an enforcement agency away from more pressing enforcement problems. As demonstrated by the FTC, serious non-compliance can result in a twenty-year reporting requirement.

x. The DOC should notify appropriate EU DPAs when there are concerns about a company's compliance with Safe Harbor.

FPF opposes prescriptive enforcement guidelines. The DOC and the FTC should share information with EU DPAs as appropriate, and data sharing is encouraged, but the DOC should not have to share information at the outset of all compliance investigations. Moreover, the priority accorded EU officials in bringing enforcement concerns to the attention of the FTC (which is charged with Safe Harbor enforcement) is a valuable compliance tool.

xi. False claims of Safe Harbor participation should continue to be investigated.

FPF agrees that false claims of Safe Harbor participation should continue to be investigated. False claims of participation are enforceable under Section 5 of the FTC Act. FPF further agrees with the EC that false claims weaken the credibility of the system as a whole and should be immediately removed from companies' websites.

xii. The privacy policies of Safe Harbor participants should include disclosures about the extent to which US law allows public authorities to access personal data.

FPF agrees that privacy policies should include certain disclosures about exceptions to data practices for law enforcement and national security purposes. FPF recommends that companies provide general information about these practices and consider including references to the statutory provisions that mandate these disclosures, to the extent that they are permitted by law. DOC also might provide guidance or a model statement to be included in all privacy policies of Safe Harbor participants concerning compliance with national security-related data requests.

xiii. Safe Harbor's national security exception should allow disclosures of personal data only as strictly necessary and proportionate to address national security concerns.

The issue of appropriate national security access to personal data transcends the Safe Harbor and should be resolved separately from discussions of the Safe Harbor. Any adjustments should be made separately from Safe Harbor negotiations on *commercial* privacy practices, for example in government talks focused on national security needs.

B. Suggestions For Improving Membership

Although the growth of the Safe Harbor is encouraging, there is still room for improvement. To encourage membership, the EU and US should work together to identify and educate companies of the benefits of Safe Harbor membership.

Improved self-help screening tools should be developed to assist companies – particularly smaller ones – in determining whether they should self-certify to the Safe Harbor. This could help companies determine whether they need to register as part of their privacy compliance efforts. Additionally, more administrative resources should be allocated to the DOC for handling the many new members.

C. Suggestions For Ensuring Compliance

As demonstrated above, companies who wish to certify their compliance with the Safe Harbor program frequently have to undertake significant changes to their data practices before they can become members. Nevertheless, additional screening and monitoring could help to ensure those companies in the Safe Harbor are better equipped to handle their obligations.

FPF recommends the appointment of a "Safe Harbor Master," housed in the ITA, to coordinate with and assist companies who wish to join the Safe Harbor program. The Safe Harbor Master could help companies determine if it makes sense to join the Safe Harbor program given their actual data practices.[220] Once the company is a member, the Master could continue to monitor the company to make sure they are complying (*e.g.*, reviewing policies to make sure they are accurate), issuing guidance to participants and, in cases of recalcitrance, referring targets to the FTC for enforcement. The Master also could prepare annual reports for the EU and coordinate efforts between ITA and FTC.

FPF also recommends that the ITA continue to take an active role in monitoring companies, even when no complaints are filed. More administrative resources should be allocated to the ITA to carry out this task. Furthermore, the ITA and FTC should work together to develop tools and resources to assist businesses – particularly small and mid-sized entities – with their compliance efforts. Efforts to raise awareness of Safe Harbor issues, such as the FTC's dedicated Safe Harbor resources on its Business Center website, should be lauded and expanded upon.[221]

Lastly, companies should be encouraged to make internal changes to ensure that annual Safe Harbor obligations are complied with. For instance, companies should create a dedicated email account to receive Safe Harbor-related materials so that changes in personnel do not cause lapses in later years. Having a generic contact will also make the recertification process with the DOC more efficient.

D. Suggestions for Enhancing Enforcement

i. Improved Tools and Resources in the US

It is critical that individuals understand how and where they can bring complaints. On this account, parties on both sides of the Atlantic can do more to educate individuals about their rights.

---

[220] The DOC has advised FPF that their Safe Harbor Team currently provides prospective applicants with advice on participation.

[221] *U.S.-EU Safe Harbor Framework*, FED. TRADE COMM.'N, http://www.business.ftc.gov/us-eu-safe-harbor-framework (last visited Dec. 6, 2013).

The DOC's Safe Harbor website serves as clearinghouse of information about the Safe Harbor.[222] Both company privacy policies and European regulators direct individuals to explore Export.gov for more information, but the current site lacks easy-to-use tools to help individuals understand exactly how they can take advantage of the Safe Harbor. Specifically, the site's Safe Harbor landing page provides little information that would help individuals. The site states that it is intended "to provide information an organization would need to evaluate–and then join–the U.S.-EU Safe Harbor program."[223]

Individuals are likely overwhelmed by both the amount and substance of the material available on the Export.gov site. None of the available materials offer individuals a common-sense guide to their rights under the Safe Harbor, or explain how they can have their complaints addressed. DOC should create a dedicated Safe Harbor site directed at lay persons. Considering the site is servicing citizens of EU Member States, language options other than English also should be provided.

Furthermore, the site should make it much easier for individuals to locate company-specific information. Currently, an entirely separate "List" page offers a function for determining whether or not companies are Safe Harbor members, but searching companies is done via a cluttered user interface.[224] A small icon offers users the ability to download a spreadsheet of the entire Safe Harbor list, but this option is easy to miss and hardly user-friendly.[225] Rather, the site should contain an intuitive and easily searchable database, sortable by company name and/or brand, and with important links and contact information highlighted. Additionally, companies that intentionally leave the Safe Harbor program should be allowed to explain why and have that information also included as part of the Safe Harbor list.

Another suggestion would be to require companies participating in the Safe Harbor to include on their public-facing privacy policies an embeddable widget that would contact the DOC server and display the current status of the company's Safe Harbor membership. Such a widget would provide a clear warning to individuals if, for example, the company fails to renew its annual recertification.

ii. Improved Company and Third-Party Transparency

Companies also should provide more transparency about their Safe Harbor commitments. Today, companies generally state they abide by the Safe Harbor and direct individuals to the DOC's Safe Harbor website both to view the company's certification and to learn more about the

---

[222] *Welcome to the U.S.-EU Safe Harbor,* EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018365.asp (last updated April 11, 2012).

[223] *Id.*

[224] *Safe Harbor List*, *supra* note 42.

[225] *Id.*

program. Companies should pay particular attention to and provide up-to-date information about their dispute resolution provider. Privacy policies should indicate an email address within the company to send complaints and information on how to contact either the DPA or third-party dispute resolution provider.

A corollary recommendation is for third-party dispute resolution providers to require companies using their services to conspicuously provide individuals with their up-to-date contact information in the company's privacy policy. Many, though not all, of the third-party dispute resolution providers require this information to be displayed; more problematic, however, is that this information is sometimes found in a different section of the company privacy policy from the contact information to direct complaints internally. This creates confusion and may make it difficult for individuals to know where they can direct complaints, particularly when a company relies on a third-party service that lacks a dedicated Safe Harbor program.

iii. Increased EU participation

European DPAs also can do more to educate their citizens about the Safe Harbor. As discussed above, the amount and substance of information about the Safe Harbor varies widely among DPA websites.[226] While every DPA website that FPF has visited provides clear contact information for individuals to bring complaints, specifically tracking Safe Harbor-related inquiries could help regulators understand the program's failings. While the informal European data protection panel has established a standard Safe Harbor complaint form, there is no reasonable way for an average EU citizen to find this form.[227] It is not easily discovered through Google searches, the EC's website, or through any of the DPA sites that were analyzed. As noted above, the FTC has not yet received any substantial number of referrals from the EU DPAs, despite the FTC's commitment to priority enforcement.[228]

---

[226] *Infra* § IV.B.

[227] A basic web search for "standard form violation safe harbor" produced no results. A search for "complaint safe harbor" lead to links by the BBB, TRUSTe, and the DMA, but nothing from the DPAs. FPF checked the European Commission's website and found a form, but only after applying the following numerous steps:

1. A-Z index
2. Data Protection
3. Documents
4. All documents
5. International Transfers
6. Commission Decisions on the adequacy of the protection of personal data in third countries.
7. US-United States-Safe Harbor
8. Standard Complaint Form.pdf

[228] Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework, *supra* note 73, at 3.

The FTC "welcome[s] referrals from authorities in member states, which have a critical role to play in monitoring and reporting possible Safe Harbor violations," and "welcome[s] further initiatives from the EU authorities to conduct investigations, and to refer case files and share evidence with the FTC."[229] The EC should therefore encourage EU DPAs to refer complaints to the FTC when they believe the Safe Harbor has been violated. Because the Safe Harbor framework was designed with this in mind, and because DPAs have priority with the FTC, DPAs should take advantage of this process.

Lastly, information about the Safe Harbor should be standardized as much as possible across companies, DPAs, and US regulators. The FTC has a strong history of public education efforts and processing individual complaints, and may be well positioned to assist with encouraging user-friendly tools and resources.

VIII. CONCLUSION

It would be unwise at this stage of the Safe Harbor to pull back on this effective program. EU citizens' privacy will suffer if restrictions are imposed on the Safe Harbor. There have been healthy and increased growth rates in membership in the Safe Harbor program, a more stringent commitment by industry to data security to stay in compliance with the Safe Harbor's privacy rules, and significant enforcement actions by the FTC coupled with ongoing monitoring by the ITA and third-party dispute resolution services. While there have not been many complaints from the EU DPAs thus far with respect to Safe Harbor enforcement, the FTC and third-party certification providers have shown both the capacity and the willingness to respond to complaints and to enforce against companies who fail to live up to their Safe Harbor obligations. Moreover, suspending the Safe Harbor will not address EU concerns about the NSA's surveillance activities.

Before undermining the Safe Harbor agreement that has thrived for over a decade, FPF urges officials in the EU to take a dispassionate view of the Safe Harbor program – especially in comparison to the enforcement tools that are or would be available if the Safe Harbor is suspended – and look to other means to bolster the Safe Harbor and further protect EU citizens' privacy. The EU examination of the Safe Harbor has served a useful purpose. There is room for improvement. And, together, people concerned about privacy in the EU and the US can work together to implement those improvements.

[229] *Id.* at 5.