The US Department of Commerce and International Privacy Activities: Indifference and Neglect

November 22, 2010

About this Report

This report evaluates the US Department of Commerce's international privacy programs, their efficacy, and their value to business and to consumers. The role of the Commerce Department has become more important in light of the Obama Administration's establishment of a Subcommittee on Privacy and Internet Policy in October 2010. The Subcommittee is chaired jointly by the Department of Commerce and the Department of Justice, and it is intended to promote "individual privacy," among other things.[1]

This report reviews, analyzes, and summarizes major international privacy activities of the Department of Commerce, with a focus on the Safe Harbor Framework established in 2000 with the European Union in response to the requirements of the EU Data Protection Directive. The report also considers briefly the Department's work on the Asia Pacific Economic Cooperation (APEC) Privacy Framework.

Brief Summary

The US Department of Commerce has made several high-profile forays into privacy. The most substantive efforts are the US-EU Safe Harbor and the Asia Pacific Economic Cooperation (APEC) Privacy Framework. The history of these efforts reveals the Department's primary focus, which is protecting business interests. This is not an unexpected outcome given the Department's goals and purpose. However, in looking at the potential for a broader role for the US Department of Commerce in privacy matters, an analysis of the Department's past history does not suggest that consumer protection has ever been a significant concern or priority. The Department's past history also indicates a lack of rigor regarding enforcement and compliance in the privacy programs it administers.

About the World Privacy Forum

The World Privacy Forum is a non-profit, non-partisan public interest research and consumer education group. It focuses on a range of privacy matters, including financial, medical, employment, and Internet privacy. The World Privacy Forum was founded in 2003.[2]

---

[1] "As part of the Obama Administration's commitment to promoting the vast economic opportunity of the Internet and protecting individual privacy, the National Science and Technology Council has launched a new Subcommittee on Privacy and Internet Policy. Populated by representatives from more than a dozen Departments, agencies and Federal offices, and co-chaired by the two of us, the subcommittee will develop principles and strategic directions with the goal of fostering consensus in legislative, regulatory, and international Internet policy realms." Office of Science and Technology Policy blog, October 24, 2010. <http://www.whitehouse.gov/blog/2010/10/24/white-house-council-launches-interagency-subcommittee-privacy-internet-policy>.

[2] <http://www.worldprivacyforum.org>.

Table of Contents

Introduction and Summary of Findings

The rise of privacy as an issue of international attention has taken place during the past forty years. Various agencies of the US Government have played roles on international privacy matters, including the State Department, Federal Trade Commission, Department of Homeland Security, Office of Management and Budget, the Department of Commerce, and scattered other agencies. The privacy activities of these agencies have waxed and waned over the decades. Of the US agencies, the US Federal Trade Commission has played by far the most significant role in consumer privacy issues, for example, identity theft, financial privacy, and a host of issues related to privacy and fair business practices. Historically, the Department of Justice, primarily a law enforcement agency, has never played a significant role in consumer privacy. Indeed, in its law enforcement capacity, the Justice Department is often directly antagonistic to the protection of consumer privacy.

The Department of Commerce has played an occasional but not exclusive role in representing the United States internationally, often with regard to data protection activities in Europe. This report summarizes some of the international privacy activities of the Department, with a major focus on the Safe Harbor Framework established in 2000 with the European Union in response to the requirements of the EU Data Protection Directive.

The website of the US Department of Commerce includes this description of the Department's mission:

> The U.S. Department of Commerce has a broad mandate to advance economic growth and jobs and opportunities for the American people. It has cross cutting responsibilities in the areas of trade, technology, entrepreneurship, economic development, environmental stewardship and statistical research and analysis.
>
> The products and services the department provides touch the lives of Americans and American companies in many ways, including weather forecasts, the decennial census, and patent and trademark protection for inventors and businesses.
>
> The development of commerce to provide new opportunities was the central goal at the department's beginning in 1903 and it remains a primary obligation today.[3]

The Department is composed of a dozen bureaus and offices, some of which have functions that include specific privacy responsibilities. The Census Bureau and the National Institute of Standards and Technology (NIST) engage in policy, operational, and other activities with

[3] <http://www.commerce.gov/about-department-commerce>.

privacy consequences. These functions are not within the scope of this report, which focuses on international privacy activities.

It is not a surprise that the Department of Commerce is responsive to business interests. What is surprising is that the Department's high-profile international privacy activities have been so consistently lacking in substance, rigor, and sincerity. However, it now appears from recent activities in Europe that the Department of Commerce's failure to earnestly operate the Safe Harbor program is resulting in questions about the program's value because of the Department's failure to enforce its own rules on US organizations that claim to participate in and benefit from Safe Harbor involvement.

Findings

The Department of Commerce's actions on international privacy matters have often been characterized by highly visible but ineffectively administered programs that lack rigor. As this report discusses, three separate studies show that many and perhaps most Safe Harbor participants are not in compliance with their obligations under the Safe Harbor Framework. The Department of Commerce has thus far carried out its functions regarding the Safe Harbor program without ensuring that organizations claiming to comply with the Safe Harbor requirements are actually doing so.

The Department of Commerce is co-chair of Subcommittee on Privacy and Internet Policy established by the Obama Administration in late 2010. The other co-chair is the Department of Justice. Given the Commerce Department's past deficiencies and the Department of Justice's role as a law enforcement agency, this leaves the leadership of the Subcommittee on Privacy and Internet Policy without a strong voice for consumer privacy interests.

There is no evidence that the Department of Commerce has conducted any type of audit or significant review of the Safe Harbor Framework since the program began in 2000. If there has been an audit or review, it has not been made public in any meaningful way.

Any substantive shortcomings of the Safe Harbor Framework are the joint responsibility of the Department of Commerce and the European Union and as such are beyond the scope of this report. The European Commission ordered two studies of Safe Harbor, but took no significant action based on the consistent and critical findings of the studies. A third and more recent study confirmed that serious problems continue to exist with Safe Harbor compliance by US organizations. It is apparent from these studies that the Department of Commerce has not done enough to fully carry out its Safe Harbor responsibilities.

The Department of Commerce's failure to demand compliance with Safe Harbor requirements has so undermined the value of the program that some European data protection authorities are no longer willing to rely on a participating organization's self-certification as reflected on the Department of Commerce's Safe Harbor website.

The Department of Commerce's international privacy activities since 1980 have been mostly designed to advance the interests of the American business community. Consumers in the United States and elsewhere cannot reasonably expect the Department of Commerce to pay much, if any, attention to their privacy interests.

Regarding the current position of the Department of Commerce on the newly formed Subcommittee on Privacy and Internet Policy, given the Commerce Department's past deficiencies and the Department of Justice's role as a law enforcement agency, this leaves the leadership of the Subcommittee on Privacy and Internet Policy without a strong voice for consumer privacy interests.

Early Years of Privacy at Commerce

The privacy responsibilities of the National Telecommunications and Information Administration of the Department of Commerce originated with the establishment of a privacy coordinating committee by President Jimmy Carter in 1977 as part of a presidential privacy initiative.[4] The staff that carried out the work was transferred to NTIA at the time of its establishment in 1978.[5]

NTIA's mission has always been much broader than privacy.[6] Its principal activities have been to develop telecommunications and information policy, allocate and manage federal use of radio frequencies, provide grants for public telecommunications facilities, and to carry out related activities. During the Carter Administration, NTIA's more general privacy work was part of its general responsibility to study and make recommendations on the impact of the convergence of computer and communications technology.[7]

NTIA's privacy activities diminished rapidly after 1980. According to GAO, in 1979 and 1980, there were fifteen staff positions associated with privacy activities. In 1981, the number of position was reduced to six. In 1982, there were only four privacy staff positions, and this

---

[4] For more on this history of NTIA's origins in privacy, see Robert Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, VI Software Law Journal 199 (1993), available at <http://bobgellman.com/rg-docs/rg-softwarelj.pdf>.

[5] See General Accounting Office, *Privacy Policy Activities of the National Telecommunications and Information Administration* (Aug. 31, 1984) (GGD-84-93) [hereinafter cited as "*GAO NTIA Report*"]. See also *Right to Privacy Proposals of the Privacy Protection Study Commission*, Hearings before a Subcommittee of the House Committee on Government Operations, 95th Cong., 2d Sess. 164-65 (1978) (testimony of C.L. Haslam, General Counsel, Department of Commerce).

[6] Executive Order 12,046, reprinted in *Codification of Presidential Proclamations and Executive Orders* 937 (April 13, 1945 - January 20, 1989). The reorganization combined the functions and resources of the Office of Telecommunications Policy in the Executive Office of the President and the Office of Telecommunications within the Department of Commerce.

[7] *GAO NTIA Report*.

number was reduced to one in 1983, 1984, and 1985.[8] By 1989, it appears that privacy had entirely disappeared as an activity at NTIA.

At a hearing in 1984, a former NTIA privacy staffer confirmed the agency's loss of interest in privacy. The Director of the OECD Privacy Guidelines Project testified that the NTIA privacy initiative ended when the Reagan Administration began:

> Shortly after Mr. Reagan took office, the privacy staff at NTIA was dismantled. No one associated with that effort is currently working on privacy-related issues, and most of the staff has left the Government.[9]

The principal international privacy activities of NTIA during the 1980s related to privacy guidelines adopted in 1980 by the Organization for Economic Cooperation and Development.[10] The OECD is an international organization that promotes economic and social welfare and stimulates and harmonizes efforts on behalf of developing nations. The United States is a member along with nearly all industrialized free market countries.[11]

The OECD privacy guidelines grew in importance over time and became a statement of privacy policy used by many countries as core principles for privacy legislation. NTIA took the position that voluntary adoption of the guidelines by American companies – as opposed to formal legislative or administrative action – would demonstrate a serious commitment to privacy protection. In 1981 and 1982, NTIA requested private sector endorsement of the OECD guidelines.[12] By 1983, 182 major US multinational corporations and trade associations had endorsed the guidelines.[13]

However, the sincerity and substantive value of NTIA's efforts to secure domestic corporate compliance with international privacy standards were questioned. The Director of NTIA's OECD Privacy Guidelines Project testified in 1984 that the focus of NTIA's interest was on avoiding embarrassment. As soon as the international pressure was off, NTIA's staff was no longer allowed to discuss the guidelines project with the press or to make speeches urging

---

[8] *GAO NTIA Report*.
[9] Testimony of Jane Yurow, *Privacy and 1984: Public Opinions on Privacy Issues*, Hearing before a Subcommittee of the House Committee on Government Operations, 98th Cong., 1st Sess. 115 (1984) [hereinafter cited as "*1984 Privacy Hearing*"]. See also id. at 271 (testimony of John Shattuck, National Legislative Director, American Civil Liberties Union) ("[The Reagan Administration] emasculated the one federal agency charged with developing privacy protections inside the federal government, the National Telecommunications and Information Administration.").
[10] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
[11] See *Issue Brief: An Introduction to Fair Information Practices*, World Privacy Forum, for more background on the OECD guidelines. < http://www.worldprivacyforum.org/fairinformationpractices.html>.
[12] See *Report on OECD Guidelines Program*, Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce, to Interagency Committee on International Communications and Information Policy (Oct, 30, 1981), reprinted in *International Telecommunications and Information Policy*, Hearings before a Subcommittee of the House Committee on Government Operations, 97th Cong., 1st & 2d Sess. 27-58 (1981-82) [hereinafter cited as "*International Policy Hearings*"].
[13] *GAO NTIA Report*.

corporations to comply with the guidelines.[14] The activities involving advising multinational corporations on data privacy policies were disbanded by the fall of 1982.[15] By 1983, the privacy protection aspects of the transborder data flow issue warranted only a brief mention in an NTIA report on long-range international telecommunications and information goals.[16]

It was never clear if the endorsement of the OECD guidelines by American companies had any actual effect on privacy practices at the time. A study conducted by Business International in 1983 on transborder data flows reported that European data protection authorities were skeptical of the OECD guideline endorsements. These authorities noted that the guidelines were voluntary and that the endorsements of most firms amounted to little more than lip service. A survey in connection with the Business International report found that interviewees in ten out of thirty-four US companies that had endorsed the guidelines did not even know that their firms had done so.[17] Only seven executives interviewed at the time even knew that their firms had endorsed the guidelines, and three actually strongly denied that their firms had done so.[18]

During the 1990s, the Department of Commerce played a role in developing the Clinton Administration's Global Information Infrastructure (GII) agenda.[19] NTIA, along with other Department components and other agencies of the federal government, worked on the vision to create and implement the Administration's vision for a GII. Despite many forward-looking elements to the GII, the privacy part of the agenda was not far removed from the efforts of the Reagan Administration to convince the rest of the world that the US approach to privacy was different but comparable to that of many other nations, pointing to the sectoral elements of US privacy law and diverting attention from the areas where no laws, rules, or policies existed. While the Department engaged in GII activities other than privacy, the Department continued to support the status quo and to promote voluntary and non-regulatory approaches to privacy.[20]

The US-EU Safe Harbor Agreement

[14] *1984 Privacy Hearing* at 115 (testimony of Jane Yurow).
[15] Id.
[16] National Telecommunications and Information Administration, *Long-Range Goals in International Telecommunications and Information: An Outline for United States Policy* (1983), printed as Senate Print 98-22, 98th Cong., 1st Sess.
[17] Business International, *Transborder Data Flow: Issues, Barriers and Corporate Responses* 16 (1983) (Executive Summary).
[18] "Despite Data Flow Restriction Woes, U.S. Firms Seen Lax in Data Privacy", *Computerworld*, May 9, 1983.
[19] See, e.g., *The Global Information Infrastructure: Agenda For Cooperation* (undated), available at <http://www.ntia.doc.gov/oiahome/Giiagend.txt>.
[20] *The Framework for Global Electronic Commerce* (undated), available at <http://clinton4.nara.gov/WH/New/Commerce/read.html>, ("The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution.").

With the adoption of the European Union's Data Protection Directive[21] in 1995 and its implementation in 1998, much of the concern about transborder data flows of personal information centered on the export restriction policies of the Directive. Article 25 generally provides that exports of personal data from EU Member States to third countries are only allowed if the third country *ensures an adequate level of protection*. While some countries have been found to provide an adequate level of protection according to EU standards, the United States has never been evaluated for adequacy or determined to be adequate.

The Directive contains several provisions other than the adequacy standard that allow transfer of personal information to third countries under specified conditions (e.g., unambiguous consent).[22] While these provisions solve many problems that might otherwise arise, restrictions on exports of personal data still created some significant problems and uncertainties for both US and EU businesses, including online businesses. The Commerce Department was pressured by the American business community to resolve the threats to data exports presented by the Data Protection Directive, and the Commission did not want to cause a disruption in international data flows while the Directive was being implemented in Europe.[23]

In 1998, the Commerce Department (acting through NTIA) and the European Commission entered into negotiations to create a "safe harbor" agreement that would allow for the export from Europe of personal information and for its processing by US businesses that voluntary and publicly endorse a code of conduct that the EU would accept as meeting the adequacy standard of the Directive. The negotiations, which one scholar described as lengthy and troubled,[24] lasted for two years.

The Safe Harbor framework[25] that emerged from the negotiations allows US organizations to publicly declare that they will comply with the requirements. An organization must self-certify annually to the Department of Commerce in writing that it agrees to adhere to the Safe Harbor's requirements. There are seven areas of privacy standards covering notice, choice, onward transfer (transfers to third parties), access, security, data integrity, and enforcement. Safe Harbor documentation describes the requirements and provides an interpretation of the obligations.[26] To qualify for the Safe Harbor, an organization can (1) join a self-regulatory privacy program that adheres to the Safe Harbor's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the Safe Harbor.

The Safe Harbor framework is now operated by the International Trade Administration of the Department of Commerce. The Commerce Department website maintains a list of organizations that filed self-certification letters. Only organizations that are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation are eligible to participate. This

---

[21] Council Directive 95/46, art. 28, 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 281/47), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.
[22] Article 26.
[23] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 Houston Law Review 717, 739-40 (2001), available at <http://reidenberg.home.sprynet.com/Transatlantic_Privacy.pdf>.
[24] Id. at 738.
[25] <http://www.export.gov/safeharbor/eu/eg_main_018476.asp>.
[26] <http://www.export.gov/safeharbor/eu/eg_main_018493.asp>.

limitation means that many companies and organizations that transfer personal information internationally cannot qualify for participation.

The content of the Safe Harbor Framework has been criticized on several grounds. It is not the purpose of this document to comment on the substance of the Safe Harbor agreement between the United States and the European Commission. A substantive discussion can be found elsewhere, including in documents issued by the Article 29 Data Protection Working Party (an organization of EU data protection officials established under the Data Protection Directive)[27] and by others.[28]

The question considered here is how the Department of Commerce carries out its obligations under the Safe Harbor Framework and whether the Department's activities enhance or detract from the credibility of Safe Harbor.

Safe Harbor Studies

Three studies of the Safe Harbor Framework were conducted since the start of Safe Harbor. The first study was conducted in 2001 at the request of the European Commission Internal Market DG [2001 Study].[29] The second study, completed in 2004, was also conducted at the request the European Commission Internal Market DG [2004 Study]. An international group of academics conducted the study.[30] The third study was prepared by Chris Connolly, director of an Australian management consulting company with expertise consultants in privacy, authentication, electronic commerce, and new technology [2008 Study].[31]

---

[27] See <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#safe_harbour>.

[28] See, e.g., Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 Houston Law Review 717, 739-40 (2001), available at <http://reidenberg.home.sprynet.com/Transatlantic_Privacy.pdf>; Tracey DiLascio, H*ow Safe Is The Safe Harbor? U.S. and E.U. Data Privacy Law and the Enforcement of the FTC's Safe Harbor Program*, 22 B.U.I.L.J. 399 (2004); Kyle Thomas Sammin, Any Port in a Storm: The Safe Harbor, the Gramm-Leach-Bliley Act, and the Problem of Privacy in Financial Services, 36 Geo. Wash. Int'l L. Rev. 653 (2004), available at <http://www.allbusiness.com/technology/962049-1.html>;

[29] *The Functioning of the US-EU Safe Harbor Privacy Principles*, (September 21, 2001). This study was reportedly published by the European Commission, but a copy has not been located on the EU's data protection webpage or elsewhere on the Internet. The study author is not identified in the document, but a Commission official publicly identified Professor Joel R. Reidenberg as the author, and the 2004 Study also identified Professor Reidenberg as the author. See 2004 Study at note 2.

[30] Safe Harbour Decision Implementation Study (2004), available at <http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf>. As identified in the paper, the authors are Jan Dhont, María Verónica Pérez Asinari, and Prof. Dr. Yves Poullet (Centre de Recherche Informatique et Droit, University of Namur, Belgium) with the assistance of Prof. Dr. Joel R. Reidenberg (Fordham University School of Law, New York, USA) and Dr. Lee A. Bygrave (Norwegian Research Centre for Computers and Law, University of Oslo, Norway).

[31] *The 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>.

Analysis: The 2001 Study

The 2001 Study was completed when the Safe Harbor Framework was new, and the number of organizations participating in Safe Harbor was small relative to later years. The report found one or more shortcomings with the participation of "virtually every single adherent".[32] The report's threshold observations offer a summary of the problems uncovered:

> For the few organizations that did adhere to the Safe Harbor, the collection of documents often presented an array of problematic certifications and policies. In particular and as discussed below, these problems were:
>
> (1) corporate policies were often hard to find;
> (2) companies self-certified despite non-existent or publicly unavailable policies;
> (3) companies had ambiguous and contradictory policies;
> (4) companies restricted the scope of application of their policies;
> (5) companies described their data processing activities in an incomprehensible manner;
> (6) companies provided policies of uncertain authenticity; and,
> (7) companies appeared to make false and misleading statements in their certification statements or policies.[33]

The report's conclusions are stark, finding an "abysmal level of implementation".[34] The conclusions are reproduced here in full:

> For Safe Harbor to succeed as a substitute for statutory data protection, the implementation by companies should be thorough and unequivocally compliant with the full set of principles.
>
> The trends that emerged from this detailed analysis of the information made publicly available by the companies that have certified their adherence to Safe Harbor reflect an abysmal level of implementation. One year after the effective date of Safe Harbor, the number of adherents is trivial with few major international corporations. The commitments of the few adherents are often qualified. Substantial numbers of adherents disregard important required principles (even when the trend shows majority compliance.) And, the independent recourse mechanisms lack the basic required remedies.
>
> The complexity and confusing array of privacy statements made by the certifying companies are analytical obstacles that make an objective measurement of their compliance with the Safe Harbor Privacy Principles extremely difficult for all of the criteria. The very fact that so many Safe Harbor certifications and policies were non-transparent indicates an unsatisfactory implementation of Safe Harbor.

[32] 2001 Study at 9.
[33] Id.
[34] Id at 26.

> In itself, this threshold observation also means that interested parties such as the US Department of Commerce, the European Commission, national data protection supervisory authorities and data subjects in Europe will each have a difficult time confirming the substance and applicability of policies of companies purporting to adhere to Safe Harbor.
>
> Some of the implementation problems are technical such as the failure to include specific mention of Safe Harbor in corporate policies. Others, such as the failure to stipulate data subject access and the failure to satisfy the enforcement principle, are more troubling. The magnitude of the compliance deficiencies suggests that the Safe Harbor principles will continue to be difficult to implement. Vigorous enforcement by the Federal Trade Commission might improve some aspects of the implementation by companies, but would be unlikely to increase the number of adherents.
>
> In light of the widespread failures by companies to incorporate the Safe Harbor principles in their privacy policies and to adopt conforming enforcement mechanisms, the European Commission and the US Department of Commerce might be able to advance the satisfactory implementation Safe Harbor through requiring the accreditation of privacy programs and independent dispute resolution bodies. If a privacy program fully incorporates the principles of Safe Harbor in the rules of membership, then the program could be accredited to issue a Safe Harbor compliant seal. This accreditation and seal would demonstrate satisfactory implementation of the Safe Harbor and would give the private sector a means to assure compliance with the substantive standards.
>
> Similarly, the accreditation of independent dispute resolution bodies would assure that the substantive requirements of Safe Harbor for complaint investigation and dispute resolution were met and would assure that appropriate remedies were available. Membership in an accredited privacy program and the use of an accredited dispute resolution body would efficiently demonstrate compliance with the Safe Harbor.
>
> At present, the European Commission, the US Department of Commerce and the US Federal Trade Commission face disregard and even failure by the registered organizations in their implementation of the Safe Harbor.[35]

In summary, few companies joined the Safe Harbor Framework in the first year. Those that did join had a low level of compliance with the requirements of the framework. There is no evidence from the 2001 Study that the Department of Commerce took any significant action to oversee participation in the Safe Harbor Framework or to take steps to enforce compliance with its requirements.

[35] Id. at 26-27.

A 2002 EU Commission Staff Working Paper[36] based on the 2001 Study[37] confirmed the shortcomings found in the study. One of the Working Paper's conclusions was:

> A substantial number of organisations that have self-certified adherence to the Safe Harbour do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies. Transparency is a vital feature in self-regulatory systems and it is necessary that organisations improve their practices in this regard.[38]

Although the EU acknowledged the problems and shared the results with the Department of Commerce,[39] it appears that there was no change on the part of the EU Commission or the Department.

Analysis: The 2004 Study

The 2004 Safe Harbor Study was conducted after the Safe Harbor Framework had been in place for several years, and it found 401 participating organizations. This represented a significant increase in participation from the date of the earlier study. The 2004 study found some positive and important albeit "minimal" tendencies with respect to formal Safe Harbor requirements. However, the study also found "numerous" deficiencies in the way that Safe Harbor had been implemented. The first part of the study's conclusion[40] – including what it described as "the most alarming deficiencies" – is included here in full:

> IV. Conclusions
>
> The SH implementation review indicates that although participating US organizations have made efforts to accommodate privacy concerns, important improvements are required to ensure that safeguards for personal data streams under the SH are adequate. As a general observation, the majority of the reviewed US organizations seem to have difficulties in correctly translating the SH principles into their data-processing policies. Implementation deficiencies are not necessarily the result of bad faith but likely find their origin in confusion over the obligations of SH and perhaps a different perception of what personal data protection involves. These problems can be overcome by providing better guidance on the mechanics as well as the meaning of the SH data protection principles.

---

[36] *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council 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* (2002) [SEC(2002) 196], available at <http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf>.

[37] Id at 7.

[38] Id. at 2.

[39] Id. at 8.

[40] The second part of the conclusion not reproduced here includes "possible mechanisms for improvement".

It is regrettable that the FTC's response to the questionnaire was considerably delayed and came only after repeated requests. The same can be said in respect of the 5 EU/EEA DPAs which have not answered the questionnaire. This weakness in responses does not reflect positively on the vitality of the SH.

SH participants generally scored well as regards formal requirements that need to be fulfilled in the certification process. The positive tendencies, as described in the report, are minimal but nonetheless important. They demonstrate that US organizations are sensitive to the data protection issue and are willing to invest resources in compliance. It should not be forgotten in this regard that a thorough understanding of data protection matters has also taken a long time to evolve in Europe and is an ongoing process.

1. Deficiencies Observed

From a legal point of view, however, there are numerous deficiencies in the way in which SH has hitherto been implemented. The most alarming deficiencies are as follows:

1.1 SH Principles

• Transparency and comprehensibility of notices or privacy policies were often deficient: privacy policies were generally difficult to read and were often not able to provide clear insight into data-processing activities and associated risks. While privacy policies showed important quality differences, all of them suffered from some deficiency (major or minor). The nature of the enforcement system of the SH regime may limit transparency. Exposure to liability under the SH scheme is directly linked to explicitness and clarity of announced data protection practices.

• Choice was not clearly mentioned or lacking entirely. Choice is crucial for individuals to have minimal control over the processing of personal data pertaining to them. Without effective choice, personal data can be imported, used and distributed with little restriction. Representations regarding the affordability of choice were usually missing.

• With respect to onward transfers, the status of mentioned "third parties" was not always clear (e.g. "partner", "affiliate", etc.), and as a consequence, it was neither clear if those parties were acting in their controller or processor capacity. Express commitment of third party processors to respect the SH was lacking in certain cases. Apart from these problems, the flexibility offered by this principle could be used to circumvent EU law.

• Deficiencies were found also with respect to adoption of security measures. Certain companies did not represent adopting such measures.

• Regarding data integrity, the relevance of the data for the intended use was difficult to determine, since either the "purpose", the "data type" or the "activities" conducted were not specified at all or not clearly formulated.

• The principle of access tended to be weakly implemented. The right was often limited to contact information or not offered at all. Representations regarding the affordability of access were generally missing.

1.2 Self-Certification

• The entry, "Personal information received from the EU", in the DoC self-certification form presented many disparities in the answers given by companies. Some described the activities they conduct or gave a description of their business model, some described the purposes for processing, while some described the type of data imported.

• The requirement of accurate location of the privacy policy was not entirely fulfilled. Some of the provided hyperlinks did not work, some led to the home-page of the company where it was sometimes difficult to find the proper link to the privacy policy.

• The FTC was mentioned by the companies importing human resources data as the statutory body with jurisdiction to hear claims against the companies, yet the jurisdiction of the FTC in this respect is dubious.

• Many companies claimed to be members of privacy programs that are not really privacy programs.

1.3 Privacy Programs

• The analysed privacy programs did not incorporate all SH principles (or incorporated certain SH principles deficiently).

1.4 Enforcement

Whereas no concrete cases have been analysed (given the apparent paucity of enforcement cases or complaints received by enforcement bodies), only the implementation of the enforcement principle and FAQ 11 were assessed. Therefore, any statement as to whether enforcement bodies are fulfilling their role is limited to the application of the said SH obligations either in privacy policies or by ADR organizations' description of procedural rules. The following deficiencies were revealed:

• Organizations agreed to co-operate with the DPA Panel (even if they did not process human resources data), but generally did not represent their acceptance to comply with the DPA Panel's advice. This is alarming, especially with respect to

> data imports outside the jurisdiction of the FTC (arguably the case with human resources data).
>
> • The different sanctions foreseen by FAQ 11 were not always available in the ADR mechanisms analysed.
>
> • Publicity of findings was not fully guaranteed.
>
> • For certain dispute resolution bodies/programs there was no indication or guarantee that the dispute would be heard by experts on SH or data protection. Enforcement mechanisms were insufficiently reflected in the privacy policies, and data subjects would have had to conduct extensive research to obtain information about the complaint procedure (mostly by checking the website of the privacy program/ADR organization).[41]

For many of the areas of deficiency found in the study, the shortcomings of the self-certifications should have been apparent on the face of the application. The study found that specific required elements for a Safe Harbor certification were not often included. In some instances, essential principles were omitted or stated in a deficient manner.

The study seemingly tries to avoid evaluating the role of the Department, but it still manages to comment on the limited review by the Department and the presence of inconsistencies that a good faith review should have found. The key paragraph of the study on this point states:

> It is noteworthy that the DoC spends one business day for the review of a self-certification. However, part 2 of the present study (i.e. the extensive analysis of certification pages) indicates that the certification pages published on the DoC website often contain important inconsistencies. In particular, there are problems with the exact location of the privacy policies and with references to privacy programs that are not really such programs.[42]

Overall, the problems with the Safe Harbor Framework found by the 2004 Study suggest strongly that the Department of Commerce paid limited attention to reviewing Safe Harbor documents submitted to it. This conclusion is consistent with the results of the 2001 Study, which can no longer be discounted because Safe Harbor activities were new in 2001. The same problems clearly persisted over time.[43]

---

[41] 2004 Study at 105-107 (footnote omitted).
[42] 2004 Study at 95. The study observes that some shortcoming that it found could be the result of changes made to webpages after a certification was accepted by the Department.
[43] EU Commission Staff issued a working document commenting on the 2004 Study. *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 Commerc*e (2004) [SEC (2004) 1323], available at <http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf>.

Analysis: The 2008 Study

The 2008 Study is the only independent review of the Safe Harbor Framework outside of the US or the EU. By the time of the study, there were 1,597 organizations listed as enrollees in the Safe Harbor. The study only examined the compliance of all of these organizations with respect to *one* of the seven Safe Harbor principles (Principle 7 – Enforcement and Dispute Resolution), but the study assessed compliance with Principle 7 by all 1,597 organizations and not just a sample.

The conclusions show that the general of level of compliance continued to be poor. Of the 1,597 organizations listed, the study found that only 1,109 were current members. This in itself is an astonishing finding. Another troubling finding of the study is the level of false advertising around Safe Harbor. The study found that some of the non-member companies listed on the Safe Harbor site also claimed certification by Truste or BBB when no such certification existed, and some companies went so far as to craft a fake Department of Commerce "seal."

Measuring by compliance with the single enforcement and dispute resolution principle, the study found that only 348 organizations out of the 1,597 met the requirements. It seems certain that any assessment of compliance with the other six remaining Safe Harbor requirements would have found even fewer organizations to be in compliance.

The highlights of the study are:

> Compliance:
>
> • Although the list contained 1,597 entries, only 1,109 organisations were current members of the Safe Harbor Framework. Many organisations on the list no longer exist or they have failed to renew their certification. The list also includes double entries.
> • Only 348 organisations meet even the most basic requirements of the Safe Harbor Framework. Many organisations did not have a public privacy policy, or the policy failed to even mention the Safe Harbor. A large number of organisations failed to comply with Principle 7 – Enforcement and Dispute Resolution, as they did not identify an independent dispute resolution process for consumers.
> • 209 organisations selected a dispute resolution provider that was not affordable. These include the American Arbitration Association (AAA) that costs between $120 and $1,200 per hour (with a four-hour minimum charge plus a $950 administration fee), and the Judicial Arbitration Mediation Service (JAMS) that costs $350 to $800 per hour (plus a $275 administration fee). Organisations either failed to disclose these costs or required the consumer to share these costs.
>
> False and/or misleading information:
>
> • 206 organisations claim on their public websites to be members of the Safe Harbor when they are not current members. Many of these false claims have continued for several years.

> • 36 of these 206 false claimants were also accredited by a third party as being current members of their Safe Harbor trustmark scheme (e.g. the TRUSTe Safe Harbor and BBB Safe Harbor programs), even though these organisations are not current members of the official Safe Harbor.
> • 73 organisations claimed to be members of a Privacy Trustmark Scheme (e.g. TRUSTe or the BBB Safe Harbor program) when they are not current members of those schemes, or they claimed to be members of BBB Online Privacy – a scheme that closed 18 months ago and has not accepted any complaints since June.
> • 20 organisations displayed a Department of Commerce Safe Harbor 'seal' on their website when they were not actually compliant with the Safe Harbor Framework, including numerous unauthorised seals created using graphics software.
> • 24 organisations claimed that they had been certified by the Department of Commerce or certified by the EU – when the Framework is actually based on self-certification.[44]

The result of the 2008 study found little improvement in either compliance or data quality since the two earlier EU reviews of Safe Harbor. The 2008 study observes that "the growing number of false claims made by organisations regarding the Safe Harbor represent a new and significant privacy risk to consumers."[45]

Overall, the three studies found the same problems with Safe Harbor, without any indication of improvement over time in the management of the Department's Safe Harbor activities. Indeed, a disclaimer on the Department's Safe Harbor website indicates that Department cannot guarantee the accuracy of the information it maintains.[46] It appears that the Department has made some changes to its website over the years, but there remains a lack of evidence of any substantive efforts to monitor compliance.

Recent Safe Harbor Developments

The shortcomings of the Safe Harbor Framework have come to the attention of some data protection authorities in Europe. In April 2010, the Düsseldorfer Kreis, a working group comprised of the 16 German federal state data protection authorities with authority over the private sector, adopted a resolution applicable to those who export data from Germany to US organizations that self-certified compliance with the Safe Harbor Framework. The resolution tells German data exporters that they must verify whether a self-certified data importer in the US complies with the Safe Harbor requirements.

---

[44] 2008 Study at 4-5.
[45] Id. at 16.
[46] See <https://www.export.gov/safehrbr/list.aspx> (In maintaining the list, the Department of Commerce does not assess and makes no representations to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.")

A German exporter of personal data must now obtain evidence that a Safe-Harbor-self-certification exists and that the Safe Harbor principles are complied with. In addition, an exporter has to obtain evidence showing how the importing company fulfils its Safe Harbor duties to provide notice to the individuals affected by the data processing. A certification more than seven years old is considered invalid. The exporter must also document the assessment and provide proof if requester by a data protection authority.[47]

Essentially, the action by the German state data protection authorities rejects in significant part the Safe Harbor Framework, particularly the self-certification as it appears on the Department of Commerce website. The Düsseldorfer Kreis makes this clear when it states that the reason for its action is because "comprehensive control of US-American companies' self-certifications by supervisory authorities in Europe and in the US is not guaranteed…"[48]

As a result, German data exporters must act on their own to make sure that a US organization complies with the requirements. The effect is to significantly diminish the utility of the Department of Commerce's Safe Harbor website the Department's reporting of Safe Harbor certification. If data exporters must verify compliance with Safe Harbor with the organization claiming to be in compliance, then the Commerce Department's role in the Safe Harbor process is undermined or eliminated.

In June 2010, Thilo Weichert, the Data Protection and Privacy Commissioner for the German State of Schleswig-Holstein, went further. Noting the findings of the 2008 Study (discussed earlier in this paper) and the lack of any response by the US and the EU thereafter, the Commissioner called for immediate termination of the Safe Harbor agreement.[49] Recognizing a lack of "courage" for termination, the Commissioner alternatively called on the EU to demand from the US short-term positive evidence concerning enforcement of the safe harbor principles."[50]

The actions in Germany regarding Safe Harbor came despite the first enforcement actions brought by the Federal Trade Commission. The FTC has a principal role in enforcing compliance with the Safe Harbor Framework by those who promised to comply. In October 2009, the Commission obtained consent decrees that prohibited six companies from misrepresenting the extent to which they participate in any privacy, security, or other compliance program sponsored by a government or any third party. There was no penalty imposed on the six companies for their failure to comply and no attempt to determine the consequence of the failure for consumers who

---

[47] Supreme Supervisory Authorities for Data Protection in the Nonpublic Sector (Germany), E*xamination of the Data Importer's Self-Certification According to the Safe-Harbor-Agreement by the Company Exporting Data* (revised version of Aug. 23, 2010), available at <http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf?1285316129>.
[48] Id.
[49] Press Release, *10th Anniversary of Safe Harbor – Many Reasons to Act, But None to Celebrate* (June 23, 2010), available at <https://www.datenschutzzentrum.de/presse/20100723-safe-harbor_en.htm>.
[50] Id.

were supposedly protected by the misrepresentation.[51] It is not clear why the Commission took action against these six companies after many years of inaction on Safe Harbor noncompliance.

It appears that the long-standing failures of the Department of Commerce to oversee and control participation by US organizations in the Safe Harbor Framework have undermined the credibility and value of the program.[52] It remains to be seen if there will be further rejections of Safe Harbor certifications by other EU national data protection authorities. The substantive and credibility shortcomings of the Safe Harbor Framework have increased the need for reliance on other, more expensive, mechanisms that support the export of data outside the European Union. These mechanisms including contracts and binding corporate rules.

APEC

The Asia Pacific Economic Cooperation (APEC) is a grouping of 21 member economies in the Asia Pacific Region, including Russia, China, and the United States. APEC was established in 1989 to facilitate economic growth, cooperation, trade, and investment in the region.

The Asia-Pacific Economic Cooperation (APEC) is a forum for 21 member economies in the Asia Pacific region. APEC includes Russia, China, and the United States as members. APEC adopted a Privacy Framework in 2004. The APEC Privacy Framework is largely viewed as an attempt to create a different international privacy regime as an alternative to the European Union's Data Protection Directive. Whether APEC will succeed in influencing international privacy developments in a meaningful way remains to be seen.

Whether the APEC Privacy Framework is a useful development is a debatable point, and much depends on the perspective of the person doing the analysis. Papers on the subject can be found on various sides from scholars and others.[53] A substantive analysis of APEC's privacy work is beyond the scope of this paper because it is not a direct product of the US Department of Commerce but the result of an international collaboration, with the Department being the US representative to APEC through the International Trade Administration of the Department.

However, the role of the Department of Commerce in influencing the decision of APEC to become involved with privacy is relevant here. According to one analyst, efforts by the United

---

[51] Press Release, FTC Settles with Six Companies Claiming to Comply with International Privacy Framework (Oct. 6, 2010), available at <http://www.ftc.gov/opa/2009/10/safeharbor.shtm>.

[52] The shortcomings of the Federal Trade Commission in the Safe Harbor program are beyond the scope of this report.

[53] See, e.g., Graham Greenleaf, *APEC's Privacy Framework: A New Low Standard*, 11 Privacy Law and Policy Reporter 121 (2004), available at <http://wopared.parl.net/senate/committee/legcon_ctte/completed_inquiries/2004-07/privacy/submissions/sub32ann_c.pdf>; Johanna G. Tan, "A Comparative Study of the APEC Privacy Framework- A New Voice in the Data Protection Dialogue?," 3 Asian Journal of Comparative Law (2008); Nigel Waters, *The APEC Asia-Pacific Privacy Initiative – A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation?*, Paper presented to Privacy Laws and Business International Conference (2008), available at <http://www.austlii.edu.au/au/journals/UNSWLRS/2008/59.txt/cgi-bin/download.cgi/download/au/journals/UNSWLRS/2008/59.pdf>.

States government were influenced directly by the US business community and were the "key motivation" for APEC's Privacy Framework.

> The key motivation for the development of the APEC Privacy Framework appears to stem from US business concerns regarding compliance with the EU Directive, and concerns regarding the potential expansion of the EU approach to other jurisdictions. These concerns coincided with growing interest in the US in the concept of enterprise-wide corporate privacy rules.
>
> Although this is not the sole motivating factor, and many other countries participated in the development of the APEC Privacy Framework, it is unlikely that the Framework would exist without the influence of US business interests.[54]

The same analysis points to statements on the website of an American law firm representing business on privacy matters in which the law firm effectively claims credit for developing the idea behind the APEC Privacy Framework and bringing that idea to the US government.[55] This underscores the role of the US business community in influencing the international privacy activities of the Department of Commerce.

Conclusion

The World Privacy Forum prepared this report in part because the role of the Department of Commerce in privacy may change in the near future. The Department of Commerce is co-chair with the Department of Justice on the Subcommittee on Privacy and Internet Policy established by the Obama Administration toward the end of 2010. It is not comforting to consumer privacy advocates that Department of Justice is a law enforcement agency that is often antagonistic to consumer privacy interests, that the Commerce Department has mostly represented business interests in international privacy matters, and that the Commerce Department does not have an admirable record in the areas of privacy that it currently oversees. This leaves the leadership of the Subcommittee on Privacy and Internet Policy without a strong voice for consumer privacy interests.

Report Information:

This report was published by the World Privacy Forum. It is available at <http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf>. Please check this page for updates to the report.

---

[54] Chris Connolly, Galexia, *Asia-Pacific Region at the Privacy Crossroads* § 4 (2008), available at <http://www.galexia.com/public/research/assets/asia_at_privacy_crossroads_20080825/asia_at_privacy_crossroads.html>.

[55] Id. at text accompanying note 12.

The report was first published November 22, 2010.