US-EU Privacy Shield: Winners and Losers

An Analysis by Robert Gellman and Pam Dixon

April 6, 2016

The Analysis in Brief:

This substance of this analysis is about the new EU-US Privacy Shield, with contextual background and an analysis of how this new proposal compares to the old Safe Harbor agreement. The analysis includes a discussion of winners and losers in Privacy Shield, and discusses its potential future.

About the Authors:

Robert Gellman is a privacy and information policy consultant in Washington DC. (www.bobgellman.com.) Pam Dixon is the Founder and Executive Director of the World Privacy Forum and a privacy researcher. Gellman and Dixon are the authors of *Online Privacy A Reference Handbook* (ABC CLIO, 2011) as well as co-authors and authors of numerous and well-regarded privacy-focused research, articles, and analysis.

About the World Privacy Forum:

The World Privacy Forum is a non-profit public interest research and consumer education group focused on the research and analysis of privacy-related issues. The Forum was founded in 2003 and has published significant privacy research and policy studies in the area of health, online and technical privacy issues, self-regulation, financial, identity, and biometrics among other areas. WPF has testified before Congress, and is featured frequently in the press on privacy-related issues. For more information please visit www.worldprivacyforum.org.

US-EU Privacy Shield: Winners and Losers

The European Union and the United States government recently announced a new transatlantic program called the EU - US Privacy Shield, to replace the existing Safe Harbor Framework. Both programs allow US companies to export personal information from Europe to the US. This is a complicated, ongoing story, with multiple winners and losers, lots of wheels still in motion, and a great deal of uncertainty. You can't understand the winners, losers, or other issues without a bit of history.

Brief Background

Under the EU Data Protection Directive[1] (as well as the forthcoming EU General Data Protection Regulation[2]), it is illegal to export personal information from an EU Member State to a third country unless the third country ensures an *adequate level of protection* for privacy. There are some other justifications for data export as well, but the main issue here surrounds the general-purpose *adequate level of protection* standard.[3] The policy behind the restriction is simple. If personal information can be sent to another country that has no privacy controls, then the EU privacy restrictions could be easily evaded.

The EU found that some countries (e.g., Canada, Australia, Switzerland, and others) have an adequate level of protection, so data exports to these countries are not restricted.[4] The US does not currently have an adequacy determination, and it is unlikely at this point that the EU would find that the US meets the adequacy standard. The sectoral approach to regulation in the US has served well in a few areas, but much less so generally. It has left plentiful loopholes and gaps in consumer protection. Having an omnibus privacy law would take care of these problems, but the likelihood of that happening in the US is very slim for the foreseeable future.

When the original EU data protection directive took effect in 1998, everyone recognized that a broad ban on data exports to the US would create major problems. The solution came in the form of the US-EU Safe Harbor agreement.[5] US companies could self-certify that they comply with the privacy requirements in the Safe Harbor agreement, and data exports to those companies would then be legal. That arrangement solved the immediate problem of the lack of adequacy in the US. The EU treated the Safe Harbor standards as providing an adequate level of protection for US companies self-certified in the Safe Harbor.

Over the years, Safe Harbor suffered from rusty compliance and a lack of oversight, among other issues. Three separate studies found uncomfortably high levels of non-compliance and oversight

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en.
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R0045&from=EN.
[3] See Articles 25 and 26 of the Data Protection Directive.
[4] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.
[5] http://www.export.gov/safeharbor/.

of Safe Harbor.[6] The FTC eventually brought a few cases about noncompliance, but it did not impose penalties. In 2010, German Data Protection authorities began to publicly question the value of the Safe Harbor, but there was no response to change or update the agreement from the Department of Commerce or from the European Commission.[7] In short, the Safe Harbor process became increasingly problematic in terms of privacy, but its political and economic usefulness remained intact.

In 2013, a privacy black swan event rattled Safe Harbor and started a process that led to its eventual unraveling. Edward Snowden, a former employee of the US Central Intelligence Agency, released a series of classified documents revealing the extent of US global surveillance activities. These disclosures had many consequences, one of which is that the "Summer of Snowden" grew into a winter of European discontent with US surveillance policies. Although the Safe Harbor agreement has nothing to do with the Snowden disclosures, many in the EU began to look with fresh eyes at a broad range of US privacy issues. The long-standing and well-documented Safe Harbor shortcomings went from being the subject of ignored reports to being among the targets of visceral European anger over the Snowden revelations.

A lawsuit brought by German citizen Max Schrems against Facebook over its export of his personal information to the United States sparked the final collapse of Safe Harbor. (Facebook was self-certified in Safe Harbor). The relevancy of the Schrems lawsuit is that it resulted in a decision by the Court of Justice of the European Union in October 2015[8] which held the Safe Harbor framework was invalid. The scope of the Court's decision was unexpected by almost everyone who followed the proceedings.

The compliance failures of companies in the Safe Harbor had nothing to do with the Court of Justice's decision. Instead, the decision turned in large part on the possibility of unrestricted information sharing with the US Government. The Court found that US authorities were able to access personal data transferred to the US under the Safe Harbor beyond what was "strictly necessary and proportionate to the protection of national security." For this and other reasons, the European Court killed the Safe Harbor agreement. It was clear to most observers that the Snowden revelations were a major factor in the result.

The European Court's decision created panic and a demand for quick action by US businesses, the Department of Commerce, and the European Commission. The immediate problem was how to justify data exports from the EU to the US. The other available substitute methods for data exports – binding corporate rules (BCRs) and model contracts[9] – take considerable time to implement.

---

[6] The World Privacy Forum report titled *Many Failures – A Brief History of Privacy Self-Regulation* (2011) summarizes and includes citations to these studies. See text accompanying notes 73-85. https://www.worldprivacyforum.org/2011/10/report-many-failures-a-brief-history-of-privacy-self-regulation/.

[7] 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), http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf?1285316129.

[8] http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=en.

[9] See http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm and http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

This brings us to the Privacy Shield, the replacement for the now-invalidated Safe Harbor.[10] We are not going to consider whether the Privacy Shield – which is still in process – will withstand scrutiny from the European Court. Some think that the Court will strike it down, possibly along with other methods for satisfying EU privacy standards like BCRs and model contracts. Others disagree.

Here, we want to focus more on the winners and losers if the Privacy Shield does become final and is not invalidated by the EU Court. We think that our analysis yields surprises.

General Assessment of the Privacy Shield

Both the Privacy Shield and the Safe Harbor documents are long and complex. A complete summary would exhaust the patience of most readers. We offer instead some general conclusions.

There were two glaring problems with the Safe Harbor. First, there was not nearly enough active oversight of company self-certification or company compliance. To address this, the Privacy Shield enhances oversight, adding requirements that should have been a part of Safe Harbor all along. The Department of Commerce has an expanded role in the Privacy Shield as an active participant. This is a positive change. In Safe Harbor, the Department was more of a passive recipient and reporter of company self-certifications. Under the Privacy Shield, the Department must verify many of the self-certification elements.

In addition, the Department must post more extensive public information about current and former Privacy Shield participants. The Department must also actively look for false claims of participation. The list of new requirements is long and impressive. It will take a considerable time before anyone can grade how well the Department carries out its obligations, but one thing is certain: if the Privacy Shield is finally approved, oversight and compliance requirements will be much more rigorous. For their part, companies under the Privacy Shield must do more to demonstrate that their self-certifications are genuine. Companies can also seek independent verification of compliance, although we suspect that only a few companies will choose the independent verification route.

The second glaring problem with the old Safe Harbor regime was the lack of meaningful enforcement. Aggrieved consumers could seek arbitration in some cases, but consumers could be forced to pay arbitration costs in the thousands of dollars. The Safe Harbor defined roles for the Federal Trade Commission, the EU Data Protection Authorities, and others. Except for a few cases brought late in the game by the FTC, none of the overseers took any real actions, other than the rejection of unsupported Safe Harbor certifications by German data protection authorities.

One of the problems with the old Safe Harbor is that companies could just drop out of Safe Harbor to avoid further actions.[11] This created a compliance and enforcement no-win zone. And

[10] https://www.commerce.gov/privacyshield.
[11] See generally https://www.ftc.gov/news-events/press-releases/2014/06/ftc-approves-final-orders-settling-charges-us-eu-safe-harbor.

to be fair, there were few complaints by EU consumers before Max Schrems brought his action against Facebook through the Irish Data Protection Commissioner. We do not really know if the existing Safe Harbor enforcement methods might have worked, but the odds that any consumer would pay for arbitration would likely were always tiny.

Without going into the details, enforcement of the Privacy Shield has an improved structure and should be much more robust as a result. Consumers who seek arbitration pay nothing. Agencies in the US and the EU must step up their responses to complaints. Companies must give more notices of their privacy practices, provide consumers with opportunities to opt-out of direct marketing and other uses and disclosures, and have written agreements with their business associates when they share personal data exported from Europe. A company that enters the Privacy Shield cannot drop out and simply forget its promises. A company that exits the program must still comply with its promises for data already subject to the Privacy Shield. In short, Privacy Shield has more substantive indicia of a meaningful privacy protection program than the Safe Harbor ever did.

Perhaps the major problem in revising Safe Harbor to meet the standards set out by the European Court is addressing national security activities. And this is the crux of the Safe Harbor – Privacy Shield problem. How could any agreement that seeks to allow day-to-day *business activities* affect *national security activities* of US intelligence agencies? Solving this problem was the main obstacle to finding a replacement for Safe Harbor that the European Court will accept. The response to this challenge has several elements.

First, the State Department agreed to create a Privacy Shield Ombudsperson who will have procedural obligations regarding complaints. However, the Ombudsperson's influence will be minimal. The Ombudsperson can refer matters to the Privacy and Civil Liberties Oversight Board. Regrettably, the PCLOB's power was trimmed late last year, and it does not possess as much authority as it once did.

Second, the General Counsel in the Office of the Director of National Intelligence provided a lengthy letter describing the rules, limits, and civil liberties protections that apply to signals intelligence collections activities. The description does not appear to include anything substantively new, but it is a useful reference. US National security surveillance is not wholly unrestricted, but no one really knows about the extent of compliance with the rules. Surveillance activities are classified, making any communications about functions, failures, or changes unlikely absent more leaks.

We feel obliged to mention the Judicial Redress Act just signed into law in the US.[12] Technically, the Act is not part of the Privacy Shield, but it came at the same time and in response to the same need to find a compromise. The stated goal of the law is to give European citizens rights under the US Privacy Act of 1974. Instead of dealing with the problem fairly, the Judicial Redress Act offers the appearance of rights but no actual rights. It is a cynical law that we predict will ultimately fool no one in Europe unless they choose to fool themselves because

[12] Public Law No. 114-126 (02/24/2016), https://www.congress.gov/bill/114th-congress/house-bill/1428/text?q={%22search%22%3A[%22judicial+redress+act%22]}&resultIndex=1.

of political expediency. If someone in the EU ever pursues remedies under the Judicial Redress Act, the Act's lack of utility will be made clear by US courts.[13]

Presumably, the idea is that something here might persuade the EU Court to allow the Privacy Shield to pass muster. The Court's reaction– and the future of Privacy Shield – remain the great unknown.

Privacy Shield Winners and Losers

It is too early to identify with any certainty the winners and losers in the Privacy Shield process. There is a chance that the EU may not give final approval, and there's perhaps a greater chance that the EU Court of Justice will kill the Privacy Shield on the same grounds as Safe Harbor. If that happens, it may be difficult to find another solution, a major crisis could result, and a different list of winners and losers will emerge.

As written, however, almost everyone involved in the Privacy Shield process is both a winner and loser in some respect. Here is a preliminary scorecard for the some of those affected by the Privacy Shield.

US Department of Commerce – The Department is a winner because it produced an agreement that its clientele in the American business community desperately wanted. However, the Department is also a loser because it now has to run a privacy program that requires considerable resources and has the potential to create conflicts with some of the businesses seeking to obtain the benefits of the Privacy Shield. The Department must build an infrastructure, procedures, assign staff, and take other actions to comply with Privacy Shield. It will be a significant undertaking that takes up time, staff, budget, and more.

US Business – American multinational companies – and especially Internet giants – are winners because they needed a replacement for Safe Harbor. They export data from Europe to the US for a variety of legitimate purposes. While there are other ways to meet EU standards, all are expensive, cumbersome, and time-consuming. Further, full compliance with EU privacy standards (instead of the mixed bag of privacy standards that are part of Privacy Shield) would interfere with some business models. However, US Business is also a loser because the Privacy Shield requirements are stricter in important ways than Safe Harbor. Participants in the new scheme will need more notice, more contracts, more management attention, and more lawyers. Many companies currently in the old Safe Harbor may not join the Privacy Shield because of the added burden. Companies that sign up for the Privacy Shield will be likely to have a very good business justification for doing so.

---

[13] For more on the Act's deficiencies, see Ed Hasbrouck's recent post on PapersPlease.org, (Why the Judicial Redress Act is Worthless, https://papersplease.org/wp/2016/02/25/why-the-judicial-redress-act-is-worthless/.) For background on the general problem, see an earlier post by Robert Gellman, ("Foreigners' Privacy Rights in the US: Little More than a Gesture", Privacy Laws & Business, August 2014, http://bobgellman.com/rg-docs/rg-PL&B-PA-Gesture-14.pdf).

EU Consumers – EU consumers are winners because the overall privacy protections of Privacy Shield have the potential to be much better than that those of Safe Harbor. The substantive protections are enhanced, reflecting some advances in data protection in recent years. It is reasonable to think that US companies in the Privacy Shield will be more likely to comply with their promises. EU consumers will also have better remedies, should they choose to use them. EU consumers are also losers in a small way because the EU data protection establishment spent enormous time and resources on fixing Safe Harbor rather than paying attention to privacy shortcomings at home.

US Consumers – American consumers may be potentially better off because companies in the Privacy Shield are more likely to stop having two-tiered privacy standards, with better privacy protection for Europeans and lesser protections for Americans. A few larger companies have already come to the realization that it is better for all to apply the same reasonably high set of privacy standards to all their customers rather than pay the overhead of two sets of policies. American consumers may also benefit because more American companies might decide that the US would be better off with a general-purpose privacy law applicable throughout the US. A general omnibus privacy law that meets EU adequacy standards would make Privacy Shield unnecessary. We are not holding our breath, however, waiting for passage of that law.

American consumers are also losers in the Privacy Shield calculus. The Federal Trade Commission spent enormous time and resources trying to satisfy the European data protection regulators on behalf of the American business community. While active on EU matters, the FTC could not fulfill its mission of protecting American consumers as well as it might have. There is one additional issue. The FTC promised to "give priority" to Privacy Shield referrals and to other Privacy Shield matters. This concerns us. While it is still too early to know exactly what this means operationally, will Europeans really be treated preferentially over Americans by the FTC? If European consumers file Privacy Shield complaints in large numbers, would American consumers find the FTC to be less responsive to their privacy and consumer protection needs? In an ideal world, if there were torrents of EU complaints, the FTC would get additional funding to meet all of the new demands. But the FTC doesn't have many friends in the Congress right now, and more funding is highly unlikely.

European Commission – The European Commission is a winner because it managed to reach agreement on a replacement for Safe Harbor with the US. Whether the Commission will succeed in having that agreement accepted by all relevant parties and courts in the EU remains to be seen, but it is a success for now. However, the Commission's ability to weave among the different pressures that affect its data protection activities may be further circumscribed. If EU consumers and consumer groups start looking at other international data flows and at the adequacy of other instruments that support data exports, the Commission will have considerably more work to do in the coming years.

Early Conclusions about Privacy Shield

Some form of general solution to the EU-to-US data export problem is still necessary in today's world. Safe Harbor was the first stopgap response, and Privacy Shield is the second. If companies trying to do the right thing were cut off without enough time to find another solution, it would be disruptive to both business and consumers. The problem is a legitimate one, and there is still a need for accommodation. Neither side is entitled to its own way.

The reality here is that the Safe Harbor had been in place for a long time. The process had broken down in many areas, especially in the area of compliance, enforcement, and consumer redress. Eventually, the privacy chickens came home to roost. We would have been happier had the European Court thrown out Safe Harbor because of its inherent shortcomings and its lack of compliance. But the EU Court found another basis, and it established a much harder standard to understand and to address.

It is not clear that either the EU Court or the Safe Harbor/Privacy Shield structure is the right place to decide what the US considers to be national security activity. We do not know any more than anyone else what the EU Court will do with the next case.

The inherent difficulty of dealing with the national security issue in this context had some positive consequences for privacy. The Privacy Shield process had no hope of making any substantive changes to US national security activities. Because Privacy Shield had nothing meaningful to offer on national security, it instead addressed the shortcomings of commercial transfers allowed under the Safe Harbor agreement. That was doable whereas national security was beyond reach. Another reason for the strengthening of Privacy Shield is the role played by data protection authorities.

In the end, we would have been happier had the Privacy Shield agreement come with a reasonable sunset. American companies should have been given adequate time – perhaps five or ten years – to find other routes to solve their data export problem. With enough time, companies could solve their problems in other ways, and the need for a generic solution like Privacy Shield would slowly disappear. As it stands, the one certainty at hand is that there is likely to be a third act in this drama sometime in the future.

Document History:

Version 1.0: First Public release April 6, 2016.

Updates to this work will be posted at www.worldprivacyforum.org