EU-US Safe Harbour Invalidation and its Implications

EU privacy laws forbid sending its citizens' private data outside of the European Union, except when the location where the information is received has privacy laws in line with the EU ones. In 2000, a Safe Harbour framework (The Data Protection Directive 95/94/EC) has been established between the United States of America and the European Union, allowing US companies to send data from their European offices across the Atlantic Ocean under certain circumstances (6), but this was ruled invalid by the European Court of Justice on 6 October 2015 due to a two-year old case submitted by an Austrian privacy campaigner, Maximillian Schrems (1). The reason why Mr. Schrems complained was that his Facebook private data was being sent from Facebook Irish' subsidiary to the Facebook headquarters in US and the privacy laws in the United States did not ensure that his data was no subject to surveillance from American authorities. As he stated in the file, “in the light of the revelations made in 2013 by [Edward Snowden](https://en.wikipedia.org/wiki/Edward_Snowden) concerning the activities of the [United States intelligence services](https://en.wikipedia.org/wiki/United_States_Intelligence_Community) (in particular the [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (‘the NSA’)), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities”. Its implications are not only heavily affecting US companies, which cannot have a free movement of data among their offices, but also us, as EU citizens, and our data privacy. However, a new agreement was reached on 2 February 2016 called “EU-US Privacy Shield” that promises positive prospects for all involved parties (2).

In 2000, when The Data Protection Directive was promulgated, Internet was not as widely spread as it is today (7), thus the regulations and main principles behind the Safe Harbour scheme became questionable nowadays. The agreements were considered invalid on 23 September 2015 by General Advocate Yves Bot on the grounds that national supervisory authorities have full power and rights to stop any transfer of data that they find questionable, therefore having the ability to rule against any decision made by the Commission (8). This was the case with Maximillian Schrems, a Facebook user since 2008, who, after Edward Snowden's leaks in 2013, thought that his private data might be under surveillance by US bodies (e.g. NSA) as they were sent from Facebook's Irish subsidiary to American servers. He lodged a complaint to the Irish supervisory authority which rejected it on the grounds that the Commission issued a directive in 2000 stating that if a third party is considered to have adequate privacy laws, data can be freely moved (1). This complaint was sent further to the High Court of Ireland, which wanted to ascertain if a national supervisory authority has the right to question if the third-party country ensures adequate levels of protection. The General Advocate's decision was accepted by the Commission on 6 October 2015, making the whole scheme invalid.

The majority of people do not want their private data to be used or manipulated by any other party, including governments or federal bodies. In studies conducted by several bodies (e.g. Eurobarometer – 2011, IIPS – 2008, Deloitte - 2012) (5), 59 to 84% of the people interviewed said that disclosing personal information, such as financial, health details or even social media activity, is a big issue. Therefore, one of the main positive aspects of the Safe Harbour invalidation was the increase of privacy for EU citizens' data and the awareness among people regarding how vulnerable their personal data is. As Internet is becoming a primordial part of our daily lives, the data we share online is increasing dramatically and, without proper protection, we are subject to possible misuse or even espionage. In 2013, Edward Snowden leaked more than 1.7 million NSA classified documents, showing the world the degree of surveillance we are facing. After this event occurred, as awareness started to increase, people became more eager to protect themselves against privacy invasion and complained to different authorities both in the US and EU, among which the above-mentioned Mr. Schrems succeeded in making the ECJ rule against the Safe Harbour agreements.

Sources

["Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid"](http://curia.europa.eu/jcms/jcms/P_180250/) (press release) (Press release). Court of Justice of the European Union. 6 October 2015. p. 3. Retrieved 29 February 2016.

[EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield](http://europa.eu/rapid/press-release_IP-16-216_en.htm), issued 2 February 2016

Chris Strohm and Del Quentin Wilber (January 10, 2014). ["Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers"](http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html). [Bloomberg News](https://en.wikipedia.org/wiki/Bloomberg_News). Retrieved February 1, 2014.

<http://www.computerweekly.com/news/4500254944/EU-Safe-Harbour-ruling-requires-a-rethink-of-data-processes>,[Warwick Ashford](http://www.techtarget.com/contributor/Warwick-Ashford), [06 Oct 2015 17:30](http://www.computerweekly.com/news/4500254944/EU-Safe-Harbour-ruling-requires-a-rethink-of-data-processes)

paper <http://www.sciencewise-erc.org.uk/cms/assets/Uploads/SocialIntelligenceBigData.pdf>

comunicat <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

paper <http://www.dekunder.nl/Media/10.1007_s11192-016-1863-z.pdf>

http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf