CJEU: First reaction to AG's opinion on NSA "PRISM" scandal Facebook's EU-US data transfers under "Safe Harbor" not legal

The following statement is a first response after only an initial review of the advocate general's opinion on the 'safe harbor' / Facebook / PRISM case (C-362/14) delivered today.

This document may be updated (click here for the latest version). All updates can also be found on twitter (@maxschrems and @europevfacebook) as well as on europe-v-facebook.org.

Please also check the Fact Sheet (PDF) for factual details and the FAQs (PDF).

Today the advocate general (AG) of the European Court of Justice (CJEU) has delivered his non-binding opinion on the NSA/PRISM spy scandal, which may have major implications for EU-US data flows and US internet companies operating in Europe.

The case deals with Facebook's sharing of data with the NSA under the "PRISM" spy program, but may equally apply to other tech giants like Apple, Google, Yahoo and Microsoft. The final ruling by 15 judges of the highest court in the European Union is expected later this year. In the majority of cases the ECJ follows the AG's non-binding opinion.

First Reaction. Schrems (plaintiff): *"After an initial review of the advocate general's opinion of more than 40 pages it seems like years of work could pay off. Now we just have to hope that the judges of the Court of Justice will follow the advocate general's opinion in principle."*

AG: 'Safe Harbor' invalid. The advocate general had a number of options to answer the questions by the Irish High Court. *"It is great to see that the advocate general has used this case to deliver a broad statement on data transfers to third countries and mass surveillance."*

The advocate general has found that the current privileged status of the United States through the so-called 'safe harbor' system is violating EU law. US Companies that receive data from the EU do not provide an 'adequate protection' only because they self-certified under 'safe harbor'.

EU law generally prohibits the "export" of personal data outside of an area that provides adequate privacy protection. While the US does not provide an 'adequate protection' the EU allowed US companies to 'self-certify' to the 'safe harbor privacy principles' and thereby be considered to provide 'adequate protection'.

The advocate general has further found that mass surveillance systems used by the United States constitute a privacy violation that would not only violate the standards set out in EU's data protection directive 95/46/EC, but also the standards of the EU's Charter of Fundamental Rights. The advocate general therefore concluded that the current 'safe harbor' deal, which allowed US companies a privileged status to export EU data to the US, should be found invalid by the court.

The advocate general has also called into question the enforcement system of the 'safe harbor' that relies on private arbitration and the Federal Trade Commission.

"As the advocate general has very much relies on fundamental rights arguments this clarification may, if confirmed by the court, be binding not only for the European Commission but also for the European Legislature in the ongoing reform of the EU's data protection laws and would ensure that there is a very clear red line. This finding has also an important impact on the negotiations between the EU and the US regarding a new 'safe harbor' system, as it must be now assured that the mass access of national security agencies to EU data transferred to the US needs to be definitely excluded."

Irish DPC could not rely on 'Safe Harbor' and was not 'absolutely bound'

Part of the question referred by the Irish High Court, also concerned the role of the Irish Data Protection Commissioner (DPC) and his duty to protect citizens.

The AG has found that the Irish DPC could not simply rely on the 'safe harbor' in a case where there were massive doubts about the protection it provides. It must investigate complaints filed with his office.

In the recent years, the Irish DPCs have hardly made any formal decisions. Only 3.2%[1] of all complaints received by current DPC Helen Dixon in 2014 lead to a formal decision by the DPC. Under the previous DPC Billy Hawkes rates were between 2% and 4% (see chart). All other complaints are "informally resolved".

Schrems: "What the DPC calls 'informally resolved' is in fact a euphemism for complaints that are simply not processed in violation of Irish and EU law. Citizens simply get an informal email by the DPC saying that their case is not dealt with, just like in this case on PRISM.

Affected Business

Currently 4.410 US companies have an active 'safe harbor' certification, including almost all major IT companies. The list includes companies involved in the PRISM scandal (Microsoft, Apple, Google, Facebook, AOL, Yahoo) but also almost all other large IT names (e.g. Adobe, Akamai, Amazon, eBay, HP, IBM, Intel, Oracle or Twitter).[2]

If the court follows the opinion of AG Bot, these companies would have to find another legal basis to transfer data from the EU to the US, including so-called "Binding Corporate Rules" (BCRs) or "Standard Contractual Clauses", which are provided for in the data protection directive. While the "Safe harbor" system did generally not allow for review by European authorities, these other legal instruments are subject to individual review by independent European Data Protection Authorities.

Schrems: "*If the safe harbor system is gone, it is very likely that the data protection authorities in the 28 EU member states will not allow data transfers to US companies that are subject to mass surveillance laws. This is may have major commercial downsides for the US tech industry.*"

[1] See Annual Report 2014, Page 6 (27 formal decisions of 829 complaints concluded in 2014).
[2] Detailed List available online: https://safeharbor.export.gov/list.aspx

European businesses are legally prohibited from outsourcing the processing of personal data to contractors that do not provide adequate protection. The case may therefore especially affect US providers of cloud and online services, operating on the European market, while service providers who are compliant with EU privacy laws may be able to benefit from a decision by the court.

Schrems: *"This finding, if confirmed by the court, would be a major step in limiting the legal options for US authorities to conduct mass surveillance on data held by EU companies, including EU subsidiaries of US companies."*

Conflict EU/US law

Multinational companies must comply with applicable national laws. If US law requires access for mass surveillance and EU constitutional rights prohibit just that, the companies are caught between two stools. So far this problem was mainly solved because European authorities and politics looked the other way.

In a similar US case concerning access to individual emails – not mass surveillance – (Microsoft v. USA, see Wikipedia) US authorities have ordered Microsoft USA to disclose emails stored in a data centers in Ireland, leading to an ongoing court procedure about the extraterritorial application of US orders. Microsoft has cited Directive 95/46/EC as one of the reasons I could not deliver the relevant data under US law.

Schrems: *"One could almost feel bad for multinational being trapped between the different laws, if they wouldn't have developed these structures with the main aim of using differences in national laws to pay almost no taxes. It is somewhat ironic, that a corporate structure that was to a large extent chosen to avoid taxes may now fall on their heads."*

Limited number of EU-US data transfers affected

Schrems: „*The approach the advocate general has proposed is balanced and protects the fundamental rights of the users and the free flow of data. I am sure lobby groups will again predict the 'end of the internet'. In fact this case only addresses outsourcing of data from a European to a US company if the data is shared for mass surveillance."*

"Special Status": EU law generally prohibits the transfer of personal data to non-EU countries, to ensure that EU data stays within a protected sphere. To continue to allow data flows with other countries the law knows two systems:

- Article 25 of Directive 95/46/EC provides for a *free flow* of data to countries that provide 'adequate protection', without any individual review by EU authorities.
- Article 26 provides for a more limited flow of data to the rest of the world.

If the 'safe harbor' system for the US is invalidated, the roughly 4.400 US companies that are 'safe harbor certified' will only lose their privileged 'special status' that allows free flows of data from the EU, but will still be able to use other forms of data transfers under Article 26.

Almost all other major trading partners of the EU operate without any privileged status under Article 26. Overall only four non-European countries (Argentina, Canada, Israel and New Zealand)[3] were so far granted this status. All of these countries have - unlike the US - special data privacy laws.

"Self-certification under safe harbor gives US companies an extremely unfair advantage over all other players on the European market that have to stick to much stricter EU law. Removing 'safe harbor' would mainly mean that US companies have to play by rules that are equal to those their competitors already play by and that they cannot aid US mass surveillance."

The end of this privileged status would not mean that personal data cannot be transferred between the EU and the US. The 'safe harbor' does mainly apply to outsourcing of processing of personal identifiable information from the EU to the US. Most transfers of personal data between the EU and the US, like communication, hotel bookings, bank transfers and almost all other forms of necessary data transfers, are always possible under a long list of exceptions in the current EU law.

However, companies that participate in US mass surveillance and provide for example cloud services within the EU and rely on data centers in the US may now have to invest in secure data centers within the European Union.

Currently this could be a mayor issue for Apple, Facebook, Google, Microsoft or Yahoo. All of them operate data centers in Europe, but may need to fundamentally restructure their data storage architecture and maybe even their corporate structure.

If these providers cannot ensure an 'adequate protection' through other legal instruments, European business customers would also need to transfer their processing operations to providers that ensure the full protection of hosted personal data. EU businesses are liable if they use services that do not comply with EU privacy laws. A number of large European providers have promoted themselves as a privacy friendly alternative to US tech companies.

Some US companies, like twitter[4] already expected that it may become harder for US companies to freely transfer data from the European Union and that it may be necessary to invest in secure European data centers.

Facebook's involvement in PRISM

The Irish High Court has found as a matter of fact, that Facebook did participate in mass surveillance in the United States and EU data is made available to US authorities (see judgement).

The Irish High Court has even found that "*only the naive or the credulous could really have been greatly surprised*" over these forms of mass surveillance. The court further found that "*that personal data transferred by companies such as Facebook Ireland to its parent company in the United States is thereafter capable of being accessed by the NSA in the course or a mass and*

[3] see current list: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[4] See the Annual Report of Twitter: http://files.shareholder.com/downloads/AMDA-2F526X/4048899054x0xS1564590-15-1159/1418091/filing.pdf p. 25.

indiscriminate surveillance of such data. Indeed, in the wake of the Snowden revelations, the available evidence presently admits of no other realistic conclusion."

Facebook had every freedom to join the procedure as a "notice party" but decided to remain silent in the procedure. This may have been a bad decision on the side of Facebook.

The fact that the NSA runs mass surveillance systems and US tech firms aid these programs was also not really disputed in the procedure.

Facebook typically claims the opposite in public statements (*"Mark and others clearly stated that the claim was false"*), but has not delivered any credible argument - let alone evidence - that it is not subject to US mass surveillance laws like e.g. § 1881a FISA. In most statements they only refer to blog posts by their CEO as evidence.

In fact Facebook is very likely bound by "*gag orders*" and is not allowed to confirm such cooperation with US authorities. Facebook spokespersons, which make such statements, typically do not have the necessary security clearance to know about such programs themselves.

Final Thanks.

The case brought by Mr Schrems mainly relied on the documents unveiled by Edward Snowden and was crowdfunded by more than 2.000 donors via www.crowd4privacy.org.

"I would like to use this opportunity to express my deep respect for the work of Edward Snowden, Glenn Greenwald and Laura Poitras who have made these mass surveillance systems public. Without their work and the donations of more than 2000 people, this issue would not be before the EU's top court today."

The plaintiff is being represented by an international team of lawyers including Prof. Herwig Hofmann (University of Luxemburg), Noel J. Travers (Senior Counsel at the Irish Bar) Paul O'Shea (Barrister at the Irish Bar) and Gerard Rudden of Ahern Rudden Solicitors, Dublin, and supported by data protection law expert, Prof. Franziska Boehm (University of Münster).