FAQs

1. But Facebook says they have never granted 'mass access' to the NSA?

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 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.

2. Isn't there a new Safe Harbor planed?

The European Commission has tried to update the current safe harbor system since the disclosures by Edward Snowden, but has met very strong resistance by the US government.

While there are continuous signs that the European Commission and the United States are close to a new deal, there has so far been a number of severe delays in the process and numerous deadlines in 2014 and 2015 have expired so far without any results.

It also remains questionable if an updated safe harbor would address other shortcomings of the current safe harbor system, which go beyond cases of mass surveillance. A large number of independent reviews equally identified countless shortcomings when it comes to commercial data usage of US companies under Safe harbor (e.g. the European Commission's reviews in 2002 and 2004, reviews by multiple groups of Data Protection Authorities, like the Article 29 Working Party and the German DPAs, as well as independent researchers like the Galexia Report). In the procedure before the CJEU the plaintiff has also submitted a review (PDF) that identified the numerous shortcomings of the safe harbor system in addition to the issue of mass surveillance.

There is a certain chance that an invalidation or a severe limitation of the 'safe harbor' by the Court will bring the ongoing discussions with the US to a whole new level.

"If the Court sets the red lines, this may provide the backbone for European attempts to get proper protection for EU citizens that lacked so far. We mainly witnessed nice speeches and anger letters by our politicians – but I doubt that they impressed anyone over the Atlantic. Maybe a Court ruling that may stop certain data flows will do the trick. It is also not unlikely that the US industry will line up in Washington to get better protection for EU data to regain easier access to EU data."

3. Isn't there a new "Umbrella Agreement" and "Judicial Redress Bill" planed?

The EU and the US have recently agreed on a new "umbrella agreement". The umbrella agreement only covers data that was exchanged between EU and US authorities in the framework of law enforcement and not national security. Data that was exchanged between EU and US companies and later forwarded to US authorities are also not covered.

The agreement has also just been presented, but it remains to be seen if will be signed. I would add that the agreement, even if it is in place would not cover access by national security authorities, which is subject to our case.

The judicial redress bill is also far from being signed into law. Like the 'umbrella agreement' this proposed US law has a very limited scope and gives EU citizens only a very narrow protection that is far from the rights US citizens enjoy in the EU. I would also mention that it does not make the Privacy Act applicable to EU persons, as this a common misunderstanding.

A leaked version of the agreement and the proposed judicial redress bill has already attracted criticism by notable individuals like the former Data Protection Commissioner of Germany, Peter Schaar (link) and EPIC (link).

4. How should data transfers to the US be limited in practice?

The case mainly concerns outsourcing of data processing operations by EU companies to US companies (e.g. if a European entity outsources data processing into a US cloud service).

It does not concern other forms of data flows (e.g. emails sent to the US, orders made or all data flows that do not constitute "personal data").

EU law generally prohibits the transfer of personal data to non-EU countries, to ensure that EU data stays within a protected sphere. To still 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'.
- 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 privileges 'special status' that allows free flows of data from the EU, but will still be able to use more limited 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)[1] were so far granted this status. All of these countries have - unlike the US - special data privacy laws.

In the case of the financial data provider "SWIFT" the solution was that EU data was only stored within Europe and access by US authorities was regulated through EU-US mutual assistance treaties. An equal solution may be an option for many US "cloud" providers that want to offer services in Europe, but are unable to bridge the gap between EU privacy rights and US surveillance laws. See Wikipedia > SWIFT for more on the SWIFT situation.

[1] See current list: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm