Initial Response

This is an initial response to the decision by the CJEU, after a first review of the judgement.
Please check twitter (@maxschrems) and europe-v-facebook.org for further updates.

Schrems: *"I very much welcome the judgement of the Court, which will hopefully be a milestone when it comes to online privacy. This judgement draws a clear line. It clarifies that mass surveillance violates our fundamental rights. Reasonable legal redress must be possible.*

The decision also highlights that governments and businesses cannot simply ignore our fundamental right to privacy, but must abide by the law and enforce it.

This decision is a major blow for US global surveillance that heavily relies on private partners. The judgement makes it clear that US businesses cannot simply aid US espionage efforts in violation of European fundamental rights.

At the same time this case law will be a milestone for constitutional challenges against similar surveillance conducted by EU member states.

There are still a number of alternative options to transfer data from the EU to the US. The judgement makes it clear, that now national data protection authorities can review data transfers to the US in each individual case – while 'safe harbor' allowed for a blanket allowance. Despite some alarmist comments I don't think that we will see mayor disruptions in practice."

Irish DPC

The judgment is also a victory against the Irish Data Protection Commissioner (DPC), who has maintained until the end of the procedure, that this case should not be dealt with because it was 'frivolous'. The Irish DPC has a clear duty to do its job and protect our privacy under EU and Irish law."

Political Solution

The European Commission and the US government may be able to remedy the situation. It's clear from the judgement, that a solution will very likely require severe changes in US law and more than just an update to the current 'safe harbor' system. Otherwise full compliance with EU fundamental rights and the judgement will be very hard to achieve.

Consequences in Practice

There were a lot of alarmist responses to this case. But it is clear from the judgement applies to a limited set of situations, such as outsourcing of EU data processing operations to US providers. The court could have allowed for a transitionary period, to allow a smoother implementation even in these limited cases, but did not chose this option.

The average consumer will not see any restrictions in daily use, but will hopefully soon be able to use online services without potentially being subject to mass surveillance.

However, US companies that obviously aided US mass surveillance (e.g. Apple, Google, Facebook, Microsoft and Yahoo) may face serious legal consequences from this ruling when data protection authorities of 28 member states review their cooperation with US spy agencies.

Thanks

Finally I want to highlight that this result was only possible because of the revelations by Edward Snowden, donations by many concerned citizens and the work of a great legal team.

Further Background Information

Based on previous questions by journalists and the public, we have drafted the following fact sheet before the delivery of the CJEU's judgement, aimed at persons not familiar with the procedure.

I. Facts: Procedure, Parties, Roles and Timeline

Parties to the Procedure.

Parties: The plaintiff is Max Schrems (28), an Austrian law graduate, PhD student at the University of Vienna and Facebook user.
The defendant in the case is the Irish Data Protection Commissioner (DPC), Helen Dixon.

Interventions: As the "European Commission" has issued the relevant "Safe Harbor" decision (2000/520/EC) the Commission had the role of in fact defending the decision during the ECJ hearing. The European Parliament, the European Data Protection Supervisor (EDPS) and eight member states (Austria, Belgium, Czech Republic, Ireland, Italy, Poland, Slovenia and the UK) have also intervened in the procedure. DRI was joined as an "amicus" in the Irish procedure.

Facebook: While the case is about Facebook's interaction with the NSA and other US agencies, Facebook has (for unclear reasons) decided to not formally join the procedure. While the case will have direct effect on Facebook's data transfers to the US, it is not party of the procedure.

Judges and AG: The advocate general (AG) that delivered his opinion is "Yves Bot" of France.
The reporting judge at the ECJ (preparing the judgement) is "Thomas von Danwitz" of Germany. The final decision will be delivered by the "Grand Chamber", consisting of 15 of the 28 ECJ judges.
The procedure is a reference by the Irish High Court for a preliminary ruling by the CJEU.
The Irish procedure was held before High Court judge "Gerard Hogan".

Irish Procedure

The case is based on a "judicial review" application at the "High Court" in Dublin, Ireland. The "High Court" procedure was paused to refer a number of legal questions to the European Court of Justice (ECJ). The case will be decided by the High Court, but the Irish court is bound by ECJ's opinion.
Common Error: The "High Court" is not the "highest court" in Ireland – there is also a "Supreme Court".

Irish "PRISM" Case ≠ Austrian "Class Action"

The Irish procedure is independent from a recent consumer "class action" against "Facebook Ireland Ltd" filed at an Austrian court with more than 25.000 participants. There are three "lines" of procedures that are factually connected and often confused in the public:
1. The Juridical Review before the Irish High Court (only this procedure is subject to today´s opinion);
2. A "class action" before the Austrian courts (filed 2014 and right now at the appeals level) and
3. Administrative "complaints" filed at the Irish DPC in 2011. These "complaints" were withdrawn in 2014 as the DPC refused a "fair trail" and a "formal decision" for three years. These complaints are therefore not existent anymore.

Often mistaken: The opinion of the AG is only concerned with the "Judicial Review" in the "PRISM / Safe Harbor / Facebook" case – not the Austrian "class action" procedure.

Dates / Timeline

26. 6. 2013	Complaint against "Facebook Ireland" filed with Irish DPC
25. 7. 2013	Irish DPC finds that he has "*no duty to investigate*" the complaints
	Later the DPC argues that the complaint was "*frivolous and vexatious*"
24. 10. 2013	Judicial Review against Irish DPC filed at the Irish High Court
29. 3. 2014	Hearing at the Irish High Court
18. 6. 2014	Interlocutory Judgment, Reference to the ECJ for a preliminary ruling
24. 3. 2015	Hearing before the Grand Chamber of the ECJ
24. 6. 2015	Initial date for the delivery of the AG's Opinion *(postponed for unknown reasons)*
23. 9. 2015	Delivery of the AG's Opinion.
6. 10. 2015	**Delivery of the Court's Judgement at 9:30.**
unknown	Delivery of the High Court's Judgement *(typically soon after the ECJ's judgement)*

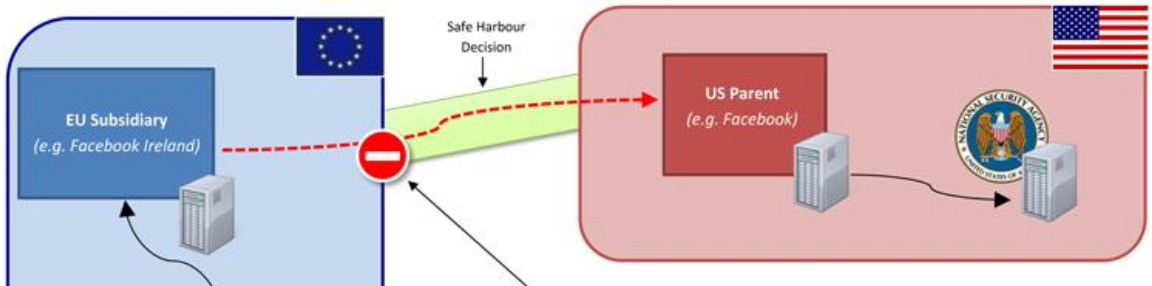
II. Key Facts of the Case

The case is based on the facts revealed by Edward Snowden, who uncovered the mass surveillance programs by the US government (e.g. the "PRISM" program).

Facts: Facebook's EU-US data flows

Facebook Ireland. Most US tech companies involved in US mass surveillance have their international or European headquarter in Luxemburg or Ireland. "*Facebook Inc*" has outsourced the operations outside of the US and Canada to "*Facebook Ireland Ltd*", based in Dublin. "*Facebook Ireland Ltd*" is responsible for more than 83.1% of all worldwide Facebook users, according to Facebook (Link).

Data not processed in Dublin – but forwarded to the US. The data is however not processed in Dublin, but forwarded by "Facebook Ireland" to "*Facebook Inc*" in the United States. Facebook only operates an office in Dublin. This sharing of data with "*Facebook Inc*" constitutes a "*transfer to a third county*" (or simply put a „*data export*" to the US). Such an export of data is only allowed under Article 25 of the EU data protection directive (95/46/EC) if the receiving country can provide an "*adequate protection*" of this personal data or if the other conditions of Article 26 of the data protection directive (95/46/EC) are fulfilled.



Data further shared with US authorities. Because the data is forwarded from "Facebook Inc." to the NSA and other US authorities for mass surveillance programs, the core claim was that personal data transferred to the US is *not* adequately protected once it reaches the United States.

Core Question: "Adequate Protection" in the United States?

The core claim in this case is that the US does not provide "*adequate protection*" as required by EU law, if data on facebook.com is subject to "mass surveillance" under US laws.

Multiple Legal Layers

The legal details of the case are a bit more complicated than the mere question if the US provides for an "adequate protection", as there is a complex interplay between different layers of EU law.

EU Data Protection Directive: Data Protection issues are regulated in Directive 95/46/EC. It says that data may only be transferred in a non-EU country if "adequate protection" is provided.

Safe Harbor: In 2000 the European Commission has issued the so-called 'safe harbor' decision (an executive decision, 2000/520/EC), which says that companies in the US that have "self-certified" under the so-called 'safe harbor program' provide "adequate protection" within the meaning of EU law. "Facebook Inc." has self-certified 'safe harbor', just like more than 4.000 other US companies.
The question before the court arose, if the 'safe harbor' decision (2000/520/EC) by the European Commission from 2000 can be interpreted to be in line with EU law – if not, the decision would be invalid as it would be incompliant with the law.
Common Error: 'Safe harbor' is an executive decision by the European Commission – not an international agreement/treaty.

Charter of Fundamental Rights: Another issue arose, as the ECJ had held in his 2014 "data retention" decision (C-293/12 und C-594/12) that mass collection of "meta data" is a violation of the EU's Charta of Fundamental Rights (the EU's "constitutional rights document").
US programs like PRISM go far beyond such "meta data" collection, which was found to be a human rights violation by the ECJ. The additional question arose, if a transfer of data to a country that conducts "mass surveillance" can be allowed under the EU's fundamental rights.
The Charter of Fundamental Rights (CFR) is part of the EU treaties. It is the EU's equivalent of national constitutional protections (like the "Bill of Rights" in the United States).

Duties of the Irish DPC

The question referred by the High Court also aims at the role of the Irish Data Protection Commission (DPC) and if it is able to simply "not investigate" a complaint – or if national data protection authorities have a duty to protect users against privacy violations. The Irish DPC is of the view, that she has no duty to act, the plaintiff claims that she has a duty to take action.

III. FAQs

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

Under EU law the finding of facts done by the national courts, not the CJEU. The Irish High Court has accordingly 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 disputed in the procedure, but confirmed by most parties to 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. The US says the CJEU got the facts wrong.

The statement by the US mission to the EU: http://useu.usmission.gov/st-09282015.html
A response by the US non-profit EPIC: https://epic.org/privacy/intl/schrems/statement/
Op-Ed by Robert Litt (US DNI) in the FT: http://www.ft.com/intl/cms/s/0/90be63f4-6863-11e5-a57f-21b88f7d973f.html

First there seems to be a severe misunderstanding on the US side about the functioning of a preliminary reference: The under the EU legal system the facts of a case are established by the national courts – in this case the Irish High Court. The Irish court found, that there is indiscriminate mass surveillance, based on the Snowden documents and current US law. Only the legal questions that follow these facts were before the CJEU. Typically the CJEU does not engage in fact finding.

No party in the procedure (neither before the Irish High Court, not before the CJEU) have really disputed these facts (with the exception of the Irish DPC in the oral hearings), instead all investigations on EU level have found that the US does conduct such forms of mass surveillance. Even the documents of the United States (e.g. by the PCLOB) confirm these facts.

Facebook as well as the US government were aware of this procedure and had every right to intervene before the Irish court e.g. as a notice party or amicus but chose not to. The notion that they had no chance to submit other facts is therefore inaccurate. Instead they chose not to engage in the initial procedure, but the US government has e.g. tried to intervene on a political level.

The claim by the US government the CJEU would have had to further investigate the facts on US spy programs seems strange, given the fact the US government did not appear before courts, the programs are secret and Edward Snowden, who uncovering details of these programs, had to flee to Russia after disclosing the facts the CJEU is now asked to investigate by the US mission. It is also not the function of any court to investigate facts that are undisputed.

The case is also very much based on US laws and orders that are public and clearly allow 'mass surveillance' that is not compliant with EU fundamental right case law. Contrary to some claims the case was not solely based on the "PRISM" program and 50 USC § 1881a, but took these programs as an example of the overall surveillance situation in the US that e.g. include also executive orders.

In addition some US representatives seem to misunderstand EU law's definitions of 'privacy' and 'data protection'. As there there is a much broader definition of privacy under EU law than e.g. under the 4th Amendment, certain acts that do not even constitute an interference with US constitutional guarantees are clearly violating EU law. A typical example would be the "making available" or the mere "storage" of personal data (so just the fact that information can be "pulled", no matter if it is factually used), which triggers EU law protection, but hardly constitutes a "search" under US law.

In other words: "Surveillance" in under EU law may not be regarded as "surveillance" under the US law. If US representatives claim (citing the same facts considered by the Irish court and the CJEU) that they do not conduct 'mass surveillance', this may be true under a US definition, but is at the same time not be correct under the (in this case relevant) EU law definition.

3. 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 the planed 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 (Review by Prof. Boehm, 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 invalidation or a severe limitation of the 'safe harbor' by the Court will bring the ongoing discussions with the US to a new level and finally lead to an updates 'safe harbor' that is – unlike the current system – not a cause for severe criticism and under the continuous threat of being invalidated on grounds of severe shortcomings.

4. 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 (as under e.g. under the "PRISM" program) are 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 the current case before the CJEU.

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 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).

5. What are the practical consequences, if 'safe harbor' is invalidated?

The exact consequences very much depend on the arguments of a decision by the Court.

There are also a number of relevant facts in each individual case of data transfers (e.g. the exact flow of personal data in each case - direct transfer from a data subject, or via a EU business, if a business is established in the EU - or only operating from the US, the purpose of a EU-US personal data transfer - there are many exceptions, or if a US business is factually aiding US spy agencies).

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) if the US entity is aiding US spy agencies. An invalidation or severe limitation of 'safe harbor' could therefor benefit EU cloud providers, that are able to ensure compliance with EU law.

A decsion does not concern other forms of data flows (e.g. emails sent to the US, orders made on a US webpage, data flows from non-EU based US-companies, data processed by consumers, or all data

flows that do not constitute "personal data"). So the vast majority of EU-US data flows are not even subject of this case, despite alarmist comments that claim otherwise.

EU law (Directive 95/46/EC) 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 types of international data flows:

- Article 25 of Directive 95/46/EC provides for a privileged free flow of personal data to all countries that provide 'adequate protection'.
- Article 26 provides for a more limited flow of personal data to the rest of the world.

If the 'safe harbor system' for the US would be invalidated the roughly 4.400 US companies that are 'safe harbor certified' will only lose their privileges 'special status' under Article 25 that allows a free flow of data from the EU, but will still be able to use more limited forms of data transfers under Article 26, just like all other non-EU businesses throughout the world.

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 – see full list at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm) were so far granted this status. All of these countries have - unlike the US - special data privacy laws.

In addition it is necessary to mention that the validity of 'safe harbor' was long debated and most lawyers have advised clients to back up a 'safe harbor' certification under Article 25 with other forms of transfers under Article 26 of Directive 95/46/EC. A decision by the CJEU does hardly come as a surprise and there was little reason to belief that 'safe harbor' is a legally stable system.

In some situations there may be more severe consequences. 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 this case.

IV. Contact, Questions and Documents

- All previous documents can be found at europe-v-facebook.org > Procedures > PRISM
- Plaintiff (Max Schrems): E-Mail: media@europe-v-facebook.org / +43 660 1616 327