Edward Snowden marked Max Schrems’ victory in the European Court of Justice with a tweet - “You’ve changed the world for the better”.

The judgment is significant; the US Safe Harbor no longer justifies the transfer of personal data to the US (Schrems C-362-14). This is not due to misuse of the scheme by commercial organisations that are part of Safe Harbor but instead because it does not address access by the US government, particularly its intelligence agencies.

European businesses have relied on this enormously popular scheme to transfer personal data to thousands of US companies offering cloud computing, whistleblowing hotlines, social media and other services. The judgment means those businesses will now need to review those transfers and consider other ways to justify them.

The Article 29 Working Party, the representative body of national regulators in the European Union, is still considering the impact of the judgment on other transfer mechanisms, such as Model Contracts or binding corporate rules. It has said those other mechanisms will remain valid until the analysis is complete. However, the Article 29 Working Party has stated that transfers under Safe Harbor are unlawful.

The Article 29 Working Party has also set a deadline at the end of January 2016 for the EU and the US to come to a solution that respects the fundamental rights of data subjects. Once this deadline passes, the regulators intend to take co-ordinated action against unlawful transfers.

In the short-term organisations making transfers based on Safe Harbor should put alternatives in place, such as Model Contracts. The medium to long-term position is much less clear. If the regulators decide Model Contracts no longer provide a valid means to transfer personal data to the US then much more radical solutions will be required, such as the use of segregated EU data centres.

In this note we set out the background to the decision, the key findings by the Court of Justice and options for future transfers of personal data to the US.
Background

The Safe Harbor

European data protection laws are intended to protect personal data not only when it is processed within the European Union, but also when it is transferred to a third country. This continued protection flows from the right to data protection in the Charter of Fundamental Rights.

It is therefore only possible to transfer personal data outside of the European Union if the third country provides “adequate protection” or there is a specific justification for the transfer.

One justification for transfers to the US was where the recipient is a member of Safe Harbor. This is a voluntary scheme set up by the European Commission and the US Department of Commerce. The Federal Trade Commission oversees Safe Harbor and over 4000 entities have signed up to the scheme, including most large US tech companies. It has been in place for 15 years and predates the creation of many of these companies.

Formal recognition came from European Commission Decision 2000/520. This states that transfers under Safe Harbor automatically ensure an adequate level of protection. National data protection regulators can only suspend data flows based on Safe Harbor in very limited circumstances.

Europe v Facebook

Max Schrems is an Austrian law student and part of the group Europe v Facebook. He is responsible for numerous campaigns against Facebook, and made 23 complaints about its practices to the Irish Data Protection Commissioner. One of those complaints was that Facebook Ireland Limited was transferring his personal data to Facebook Inc. in the US.

The Irish Data Protection Commissioner rejected the complaint because Facebook Inc. is part of the US Safe Harbor. The Commissioner was bound by Decision 2000/520 to find that Safe Harbor provided an adequate level of protection.

Max Schrems appealed that decision to the Irish High Court which, in turn, referred the matter to the European Court of Justice.

Key findings

Safe Harbor invalid

The key finding by the Court of Justice is that European Commission Decision 2000/520 is invalid. This means Safe Harbor no longer provides a justification for the transfer of personal data from the EU to the US.

This is not the result of potential misuse by commercial organisations receiving that personal data. Instead, it is because of structural faults in Decision 2000/520. In particular:

> the Decision allows information transferred on the basis of Safe Harbor to be accessed by the US government, including intelligence agencies;
once that personal data is in the hands of the US government it falls outside the scope of Safe Harbor. Access for national security or law enforcement purposes is not necessarily incompatible with data protection laws, but that access must be strictly necessary and proportionate. The European Commission failed to confirm this is the case both at the time it made the Decision and afterwards. In fact, the European Commission’s review of Safe Harbor in 2013 strongly suggested the opposite; and

the right of data protection regulators to suspend transfers under the Decision is too constrained.

Importantly, the judgment is much more moderate than the Advocate General’s opinion. The judgment focuses on the formal provisions of Decision 2000/520 and avoids an analysis of the legal framework for surveillance in the US. It does not repeat the much criticised assertion by the Advocate General that the US engages in “mass and indiscriminate” surveillance, though does state this was the finding of the Irish High Court.

The judgment draws heavily from the European Charter of Fundamental Rights. This also makes the problems raised by the judgment very difficult to fix. Issues such as the high standards for adequacy or independence of regulators reflect the fundamental human rights to privacy (Article 7) and data protection (Article 8). They cannot be overridden by new legislation.

**Independence for national regulators**

The judgment also considers the powers of national data protection regulators to review Commission Decisions, such as Safe Harbor. In doing so, the Court had to balance:

the need for national data protection regulators to have “complete independence” in fulfilling their functions - a right guaranteed under Article 8(3) of the Charter of Fundamental Rights; and

the fact that Commission Decisions are binding on Member States, including national data protection regulators, until declared invalid by the Court of Justice.

This tension is resolved by allowing national data protection regulators freedom to review the Commission Decisions and, where necessary, refer the issue to their national courts which in turn can refer it to the Court of Justice. In other words, national data protection regulators have the right to review those decisions and raise concerns, but only the Court of Justice can declare them invalid.

Not only can regulators review transborder dataflow, the judgment suggests that they must do in response to complaints. It is “incumbent” on them to “examine [such] claims with all due diligence”.

>
Options for transfers to the US

Reactions to the judgment

The Court of Justice’s judgment sparked rapid responses from both the European Commission and US Department of Commerce who confirmed they will continue to work on enhancements to Safe Harbor.

The Article 29 Working Party arranged an urgent meeting shortly after the judgment and has had an extraordinary plenary meeting on 16 October 2015. It has published a statement following that meeting in which it calls on the EU and the US to find a solution that will allow transfers of personal data to the US in a manner compatible with citizen’s fundamental rights.

The Working Party is still considering the impact of the judgment on other transfer mechanisms, such as Model Contracts or binding corporate rules. These mechanisms will remain valid until the analysis is complete. However, this will not prevent data protection regulators investigating individual cases and some, such as the regulator for Schleswig-Holstein, have already stated Model Contracts and binding corporate rules cannot be used for transfers to the US.

Finally, the Working Party has set a deadline at the end of January 2016 for the EU and US to reach a solution on the protection of citizens’ rights. If no solution has been reached by then, the regulators intend to take co-ordinated action against unlawful transfers.

So what are the remaining options for transfers to the US? We consider the alternatives below.

Option 1 - Safe Harbor version 2.0

The European Commission has been negotiating with the US to try to improve the protection afforded by Safe Harbor for more than two years.

The Commission proposed a number of recommendations to improve Safe Harbor including two specifically aimed at access by US authorities, namely that access for national security should only take place where strictly necessary or proportionate, and that data subjects should be granted a right of redress which is enforceable in the US. As part of that process, the US has proposed a number of reforms, including the Judicial Redress Bill, which if passed would provide some rights to European citizens in case of misuse of their data by US government agencies.

It is not clear if these proposals will be sufficient. While the Court avoided any substantive findings about the current US legal system, it has stated that:

> the requirement for “adequate protection” in a third country means the protection afforded by national law must be “essentially equivalent” to that afforded by the Data Protection Directive, even though it can be implemented in a different manner;

> there must be an effective detection and supervision mechanism enabling infringements to be identified and punished. The FTC, which...
currently oversees Safe Harbor, cannot fulfil this role as it has no jurisdiction over the US intelligence agencies. Whether another US body can regulate the agencies remains to be seen;

> the law must only allow access to US intelligence agencies where strictly necessary and proportionate for the protection of national security. This cannot allow generalised storage of all personal data transferred from Europe to the US. Objective criteria must be used to limit access to and use of that data. US officials advocate this is already the case; and

> individuals must have legal remedies to allow them access to their personal data and rights to have it corrected or deleted.

There is likely to be significant debate about whether the current reforms to Safe Harbor are sufficient to satisfy these criteria. The view of the civil liberty advocacy group, Europe v Facebook, is that “a solution will very likely require severe changes in US law and more than just an update to the current ‘safe harbor’ system”. The data protection regulator for Schleswig-Holstein has voiced a similar view. In contrast, both the European Commission and US Department of Commerce think a solution is possible.

The more difficult problem is timing. The reforms may require changes to US law, such as the passing of the Judicial Redress Bill. This will take time, especially given the upcoming US Presidential election.

European privacy regulators could have decided to keep Safe Harbor going on “life support” until then. However, the statement from the Article 29 Working Party is very clear; “transfers that are still taking place under the Safe Harbor decision … are unlawful”. They also intend to launch a public information campaign directed at companies using Safe Harbor. In practice, companies relying on Safe Harbor now need to put alternatives in place such as Model Contracts.

Finally, the judgment only invalidates Commission Decision 2000/520. It does not invalidate the US side of Safe Harbor so existing Safe Harborites will need to continue to comply with the Safe Harbor principles so long as they remain part of the scheme, notwithstanding the fact it no longer helps with transfers to the US.

**Option 2 - Use of Model Contracts**

One of the main advantages of Safe Harbor is that it provides a “structural” solution covering all dataflows to the recipient in the US. However, other structural solutions are available. This includes the so-called Model Contracts, which are the standard contractual clauses approved by the European Commission.

For example, Facebook Ireland Limited could put Model Contracts in place with Facebook Inc. and justify transfers between the two on that basis. Other organisations that currently just rely on Safe Harbor could do the same. Some US tech companies, such as Salesforce, have now made an open offer to enter into Model Contracts with their customers.
A switch to Model Contracts will involve:

> deciding which version of the Model Contracts to use. In particular, is the US entity a controller (requiring the use of controller-controller Model Contracts) or a processor (requiring the use of controller-processor Model Contracts) or both? To add to the complexity there are two different types of controller-controller Model Contracts to choose from. The older version is less business friendly but provides more flexibility over mandatory disclosures under local law;

> agreeing to the relatively burdensome nature of the obligations under the Model Contracts (though arguably they are not much more burdensome than Safe Harbor). One major change will be for controller to processor transfers as the US processor may have to enter into new arrangements with its sub-processors;

> the EU entity complying with additional formalities and in some cases filing the Model Contracts with national data protection regulators. The Article 29 Working Party has taken some steps to reduce these formalities through its proposed “co-ordinated procedures” (see working paper 226); and

> updating privacy policies and other collateral referring to Safe Harbor.

Perhaps the bigger question is why are Model Contracts different to Safe Harbor? If the Safe Harbor Decision is invalid because it does not address access by the US government, why are Model Contracts any better?

Part of the answer comes from the terms of the Model Contracts themselves. They require the importing US entity to confirm that national law does not prevent them fulfilling their obligations under the Model Contracts. US entities signing up to Model Contracts will need to consider this undertaking carefully (though under some versions of the Model Contracts allow disclosure for national security or law enforcement purposes in any event).

More important is the regulators’ express right to prohibit or suspend dataflows based on the Model Contracts. This right arises in a range of situations including where the importer is subject to national security or law enforcement laws are excessive or disproportionate. Whilst the Court of Justice carefully avoided making any findings about US national security law, European regulators might rely on other material, such as the European Commission’s own review of Safe Harbor in 2013, to prohibit or suspend transfers under the Model Contracts to the US.

Until the Article 29 Working Party has completed its review of Model Contracts it is very difficult to know if they will continue to provide a safe means for transfers of personal data to the US.

Model Clauses are unlikely be the “bullet proof” solution they once were. They may need a much more careful case-by-case assessment in light of the actual personal data being transferred and the risks around access for national security or law enforcement purposes. For example, this might mean
that limited intragroup transfers are possible but bulk transfers to cloud providers or similar are not.

**Option 3 - Binding corporate rules**

The final “structural” solution is binding corporate rules; a set of group-wide binding privacy commitments. Whilst binding corporate rules provide a number of benefits over other transfer solutions, there are some obvious drawbacks:

> regulators must approve them. This normally takes at least 12 months, though approval times could lengthen if the Schrems judgment leads to a flurry of new applications;

> it is unclear how regulators will respond to future applications following the Schrems judgment. They may well look for additional comfort regarding access for national security or law enforcement purposes; and

> they generally only apply intra-group, though processor binding corporate rules are also available to legitimise transfers to non-EU processors.

This means that binding corporate rules are only likely to be a medium to long-term solution and will not cover all transfers. They are also under review by the Article 29 Working Party and it is possible they too will not automatically permit transfers of personal data to the US.

**Option 4 - Consent and other individual derogations**

In the absence of a “structural” solution, it might be possible to rely on one of the individual derogations set out within the Data Protection Directive.

Most of these are very fact specific. For example, it is possible to transfer personal data to the US if it is necessary for the performance of that contract. The key here is the word “necessary”. This means if I book a hotel in New York, my details can be sent to that hotel because they have to know who has actually booked the room. In contrast, it does not justify transfers just because it is more “efficient” or “convenient” to do so.

The other derogations include transfers that are on important public interest grounds, made in relation to legal claims, are to protect the vital interests of the data subject (e.g. medical emergencies) or are made from a public register. All of them have narrow application.

One derogation of wider application is consent. However, the Article 29 Working Party has previously deprecated its use describing it as a “false good solution; simple at first glance but in reality complex and cumbersome”. Problems with consent include the fact it must be freely given so is unsuitable in some situations (e.g. it can be difficult to obtain consent from employees) and must be informed. Some commentators suggest this means expressly referring to access by law enforcement and intelligence agencies. Finally, while consent may legitimise the transfer of new personal data, it will not help
with the transfer of existing pools of personal data unless fresh consents are sought from the relevant individuals.

**Option of last resort - European data centres**

The final option is to keep the personal data within the EU. The group *Europe v Facebook* certainly considers that some of the big US tech companies; “may need to fundamentally restructure their data storage architecture and maybe even their corporate structure”. There is also a precedent for this approach following SWIFT’s decision to relocate all of its European payment messages from the US to a data centre in Switzerland. The US tech company Box has already announced it will establish EU only data centres, and other US tech companies have already established EU data centres.

However, simply placing the data centre in the EU does not, by itself, solve the problem. It is also necessary to consider where that data centre can be accessed from. For example, it might be accessed from the US or elsewhere in order to provide technical support. If so, what is the justification for transfers associated with that access?

The need for EU data centres will depend greatly on the final position taken by the Article 29 Working Party. If it removes the use of other structural transfer mechanisms, such as Model Contracts, EU based data may be the only solution in some cases.

**Back to the Irish regulator**

The case will now be brought back before the Irish High Court, which is likely to refer the case back to the Irish Data Protection Commissioner. That review may well be a flashpoint for the issues discussed above.

Facebook has responded to the judgment in bullish terms on the basis it “has had other ways to legitimately transfer data from Facebook Ireland to Facebook Inc for many years, and it also has a registration process that allows it to obtain consent from people who choose to use Facebook. Facebook will be able to operate our business as usual”.

This may face an equally bullish response from Max Schrems who will, no doubt, challenge Facebook’s “other ways” to transfer (presumably Model Contracts) and its reliance on consent. The Schrems judgment imposes a clear obligation on the Irish Data Protection Commissioner to investigate those complaints. The outcome of that investigation will be watched carefully and might again wind up in front of the Court of Justice.

**International issues and other thoughts**

**The rest of the world**

On the face of it, it is difficult to see why the judgment is so significant for the US. The loss of Safe Harbor leaves it in the same position as most other countries that are “inadequate” under European data protection law. This includes most other major G-20 economies such as Australia, India, Russia, Brazil and Japan.
One school of thought is that the US is being marked out for special treatment. Concerns over the massive volumes of personal data transferred to the US, coupled with what was an aggressive surveillance regime, might lead regulators to take a harder line on transfers to the US.

The other school of thought is that this is part of wider clamp down on international transfers. The judgment certainly has implications for transfers to other countries around the world. For example, it imposes a firm obligation on the European Commission to review periodically its adequacy findings for Canada, New Zealand, Israel, and Argentina (among others) in light of the new stringent adequacy criteria set out in the judgment.

There might also be more scrutiny for transfers to other jurisdictions with broad surveillance regimes. Are transfers of personal data to these jurisdiction also now in doubt?

**Has the world changed for the better?**

This action was brought to provide better protection for European citizens. Whether this will be the outcome is not entirely clear.

The most likely short-term outcome is a switch to alternative compliance solutions, such as Model Contracts. This may undermine the work of the US Federal Trade Commission to improve privacy compliance under the auspices of Safe Harbor.

In the medium term, the judgment may lead to further changes to the US surveillance regime to ensure a more proportionate surveillance regime and better rights for European citizens in the US. Whilst there is greater pressure for these changes, the US may well be reticent about making them as a result of European courts’ action. This may also become politically difficult in the context of the US Presidential election next year.

The judgment could also lead to greater use of European data centres. Even then it is not clear how much safer the information will be within the European Union. Most Member States grant their own intelligence and law enforcement agencies rights to access this type of data. In addition, the Snowden revelations indicate that some European intelligence agencies, such as GCHQ, also operate bulk surveillance programmes. This is not just an Anglo-American problem. France is also pushing for its own broad surveillance powers. Finally, there is still a possibility that the US government tries to obtain information stored in EU data centres, as illustrated by the current attempt to force Microsoft to provide access to information stored in Ireland.

What is certain is that this will frustrate many businesses. The judgment is not the “fault” of companies using Safe Harbor. Compliance with US national security laws is not voluntary and many US tech companies have taken positive steps to protect their customers from government access by publishing transparency reports, fighting for customer’s rights in court and lobbying for more proportionate surveillance laws.
Many will feel like pawns in a wider constitutional showdown between the EU and the US and will continue to struggle to reconcile the strict rules on transborder dataflow with the borderless nature of the internet.

The final guidance from the Article 29 Working Party on other transfer mechanisms, such as Model Contracts and binding corporate rules, will be crucial for business trying to grapple with the implications of this judgment.