Is Safe Harbor No Longer Safe?

*Post-*Schrems, *what legal professionals need to know to ensure they abide by the EU's privacy standards*

Until the recent decision, up to 4,500 companies, including many e-discovery companies, depended on Safe Harbor for transatlantic data transfers. ***Inventus' Nicola Avery-Gee****, General and Discovery Counsel at Inventus UK, reviews the immediate effects the Schrems decision has for corporate counsel and legal professionals whose companies have relied on Safe Harbor.*

MCC: What was the precise question that was posed to the ECJ and what did they decide

Avery-Gee: The question was whether the Safe Harbor scheme offers an adequate level of protection to data originating in the EU. In recent years, the large-scale collection of EU citizens' personal data has been facilitated by U.S. law and practice, without effective EU judicial protection. The ECJ, coming off a recent and controversial recommendation from the Advocate General, recognized that the mass, indiscriminate and broadly unmonitored access to personal data enjoyed by the U.S. intelligence services during surveillance activities constitutes a disproportionate interference with EU citizens' right to respect for their private life and of protection of their personal data under the EU Data Protection Directive and EU Charter of Fundamental Rights.

MCC: What does this development mean for e-discovery companies transferring data between the U.S. and EU? Is this decision final?

Avery-Gee: There are ongoing negotiations between the U.S. Department of Commerce and the European Commission, and changes to the Safe Harbor scheme are already in the pipeline: We expect these to include measures to enforce boundaries on U.S. government access to the data of EU citizens. Therefore, the approval of a new Safe Harbor agreement is likely to address at least some of the reasons given as justification for invalidating it at this time. U.S. companies and European e-discovery companies doing business in the U.S. should start thinking about alternative processes for treating European data. Customers may turn to alternative methods of legitimizing data transfers, such as the European Commission's standard contractual clauses (commonly referred to as model clauses), or wherever possible to seek to avoid transfer to the U.S. altogether.

MCC: How will this affect corporate counsel and legal professionals?

Avery-Gee: Tech companies and legal professionals working in and around Silicon Valley should be particularly concerned. The biggest players – including Twitter, Google, Facebook, Netflix and Uber – are said to have been ahead of the game with backup agreements in place to enable the continuing movement of data between the EU and U.S. Therefore, it is smaller U.S. companies who relied upon Safe Harbor that may be struggling to get a grasp on the effect of the ruling.

MCC: Now that Safe Harbor is off the table, what do legal professionals and e-discovery companies need to know about changes to their discovery processes and third-party relationships to ensure they abide by EU privacy standards?

Avery-Gee: If discovery exercises are being undertaken in relation to data originating in the EU, it would be advisable for the collection of the data to take place on-site or remotely within the EU. Similarly, processing, hosting and review of any such data should be undertaken in the EU wherever possible. The easiest and surest way of doing this is to engage an e-discovery provider with presence and experience in the EU, keeping data in the jurisdiction in which it resides.

MCC: More importantly, what do they need to do to be compliant?

Avery-Gee: If data has to be transferred from the EU to the U.S., the same seven principles set out in Safe Harbor should continue to be adhered to and additional precautions taken, particularly in respect of the security of the data. Legal advice should be taken from international law firms with a deep understanding of European and international law. It is clear that companies will need to put revised processes in place to ensure compliance with the existing European law.

MCC: What future ramifications might this have for both the U.S. and the EU?

Avery-Gee: The White House has expressed disappointment that a "critical" agreement has been struck down because of "incorrect assumptions about data privacy protections in the United States." There are ongoing discussions, which were running in parallel to the ECJ decision, with regard to the forthcoming European General Data Protection Regulation. This is a new European law under consultation that will revise and strengthen data protection measures in Europe and worldwide. It will be a single law binding on all EU member states, as well as international companies with offices in member states. Therefore, we should expect further requirements regarding transatlantic data transfer in coming years when the regulation is implemented.

MCC: How will this impact future litigation and e-discovery process?

Avery-Gee: If the U.S. is open to compliance with the new EU laws, then transatlantic data transfers may become more straightforward. However, if the laws are too stringent for the U.S. palate, then it may become increasingly difficult to handle EU data in the U.S. There are likely to be significant cost implications associated with compliance with the EU regulation, including, inter alia, appointing a dedicated and independent data protection officer – this may prevent its adoption on a wider basis, leaving only limited companies who can afford to make that commitment.

MCC: How can Inventus help?

Avery-Gee: Inventus already offers data collection, processing, hosting and document review services in EU and elsewhere from our centralized London office and data center. Inventus is ListX certified, meaning we have the highest levels of local EU-based security standards in place. In addition, our London data center is the only Relativity-certified Best in Service Orange data center outside of the U.S. Furthermore, our "discovery in a box" capabilities allow us to work directly in local jurisdictions, so we can fully operate in compliance of all international data laws. We ensure data abides by the best security, quality and customer service standards. With an international presence, we easily remain compliant of EU law and abide by ECJ opinions.

Nicola Avery-Gee
General and Discovery Counsel at Inventus UK
nag@unif-id.com

7 Turning Points for Safe Harbor

1995: *The European Commission issues EU Directive 95/46/EC, governing the protection of the personal data of EU citizens.*

2000: *Consultations between the U.S. Department of Commerce and the European Commission produce the Safe Harbor program, which allows U.S. companies to self-certify compliance with the seven data protection principles established by the EC's directive.*

2013: *Via a group named Europe v Facebook, Maximilian Schrems, an Austrian law student, complains to the Irish data protection commissioner that U.S. law and practice offers insufficient protection for the personal data of EU citizens.*

June 2014: *A case brought by the group in the Irish High Court is referred to the European Court of Justice.*

March 24, 2015: *The first hearing relating to the case brought by Schrems is held in the ECJ before Advocate General Yves Bot.*

September 23, 2015: *Bot issues an opinion that the U.S. Safe Harbor does not satisfy the EC's directive.*

October 6, 2015: *ECJ declares Safe Harbor to be invalid.*