THE LAWYER BRIEFING E-DISCOVERY

DATA TRANSFER

Life after Safe Harbour

What the ECJ's decision means for cross-border investigations, and the wider implications for companies

By (from the top) Toby Duthie, founder and partner, and Greg Mason, partner, Forensic Risk Alliance

Today's global economy is shaped by rapid technological advancements. Information is moved more easily across international borders than ever. And data volumes are growing at a staggering rate, with many multinationals producing more than a million emails a day.

In this context some 4,000 companies have, for up to 15 years, relied on the Safe Harbour arrangement in moving data between the US and the EU.

The October 6 decision by the European Court of Justice (ECJ) to scrap the Safe Harbour treaty is a game-changer, and appears to have caught a number of companies off-guard. It is attributable to the Edward Snowden disclosure a couple of years ago regarding the US National Security Agency's snooping. The Snowden affair and the ensuing ECJ decision highlight fundamental differences between the EU and the US on data privacy. In fact, these go well beyond the EU – Brazil, China and Russia have all recently passed legislation restricting the movement of data, in part as a result of Snowden.

At worst, this could be the start of the Balkanisation of the internet.

However, none of this should come as a surprise. Long before Snowden there were grumblings from national Data Protection Agencies about the inadequacy of the Safe Harbour treaty. Until now, these went largely ignored. Ideally, a new treaty will be negotiated to address perceived shortfalls, but in the interim –what should companies and lawyers do, especially when it comes to contentious situations such as litigation and criminal investigations?

The stakes are high

When a multinational organisation responds to eDiscovery requests as a result of litigation, government inquiries, or performing internal compliance audits, there is a substantial and very real risk of violating EU and other data protection laws if data is moved across borders – especially when it is moved into the US.

Personal employee data, in some shape or form, almost always lies at the heart of a contentious matter. In the criminal context the stakes have been raised further as, in September, US Assistant Attorney General Sally Quillian Yates emphasised the US Department of Justice's focus on individual prosecutions in matters of corporate wrongdoing.

Understanding data protection in the context of a cross-border investigation –and, in particular, the process of eDiscovery – can help an organisation contain an investigation and prevent potential derivative criminal violations.

Further, the General Data Protection Regulation (GDPR) is likely to be approved in 2015 or 2016. This will cover all EU states and sets out a draconian fines regime (up to 5% of global annual turnover).

In-country response

FRA has been dealing with, and addressing, complex international data transfer issues for more than 10 years in the context of major litigation and enforcement actions, and we have long argued that the Safe Harbour treaty – basically a self-certification process – in the context of litigation and investigation was dangerously lightweight and did not take into consideration major legal issues such as blocking statutes (for example in France and Switzerland). We have always advised that, in the case of mainland Europe, an in-country eDiscovery response is more appropriate. Frequently, this has been ignored – though less so recently

Following the ECJ decision it is clear that data collection, hosting, review and analysis needs to take place in the country of origin. Counsel should therefore use eDiscovery tools to review and segregate data locally. Once the data has been segregated there are several options available to accommodate any cross-border discovery request, such as going down MLAT route or even engaging with the country's local data protection authority. Removing and/or redacting any sensitive information (some of which can be done automatically), and providing restricted access via the internet (but ensuring the physical location of the data remains in the country) are options we have frequently deployed. The company and its legal team is then able to maintain far greater control of the data and eDiscovery response, and ensure compliance with relevant data protection legislation. It might even be appropriate to deploy a mobile eDiscovery solution at the physical location of the company.

There are also practical advantages to holding the data in-country (or on-premises), such as mitigating the risk of follow-on civil litigation.

Assuming eDiscovery is outsourced, vendor due diligence is more important than ever. Only a handful of vendors can deploy robust in-country solutions. Historically, most have shipped data to larger processing centres in the UK and the US. This may not always be made apparent to the corporate and the lawyers who, in the post-Safe Harbour environment, are even more ill-advised. An experienced vendor who can work with the legal team to develop an appropriate strategy and manage data transfer risks from the outset is vital.

At FRA we have been deploying fully mobile, compliant, end-to-end eDiscovery solutions since 2006 throughout the EU, Switzerland, Canada and in many emerging market locations.

Forensic Risk Alliance
Audrey House
16-20 Ely Place
London EC1N 6SN
Tel: +44 (0) 207 831 9110
Email: tduthie@forensicrisk.com
Web: www.forensicrisk.com