MARSHALL DENNEHEY
WARNER COLEMAN & GOGGIN

The Impact of EU Rulings on the Cyber Landscape

By Ed Lewis and David Shannon

Global [RE]Insurance
October 13, 2015

European judges handed down two landmark rulings last week, changing not only where and how EU citizens' personal information is handled but also perhaps the internet forever.

The first was the case of Hungarian property website 'Weltimmo'. Its Slovakian owners incurred the wrath of the Hungarian regulator when they breached local privacy laws by passing on customer details to debt collectors. The European Court of Justice (ECJ) was asked to decide if a fine imposed by the regulator was enforceable. The court said yes.

Before Weltimmo, companies trading in multiple EU member states were subject to regulation only in the state where they had their European headquarters. States with softer rules were therefore attractive locations to set up home base.

However, after 'Weltimmo' companies now have to comply with the local data protection rules of every EU state they trade in. That means increased overheads and legal costs just to carry on business as usual. The alternative is to pull back to fewer states or possibly shut down altogether.

With the bit of change firmly between its teeth, the ECJ's second decision targeted Europe's 'safe harbour' agreement with the US.

For 15 years US companies have been allowed to store their European customers' personal information on American soil, but once stateside there was very little in practice to prevent this information being processed or exported elsewhere.

Then came the Snowden files' revelation that US security services have routinely dipped into this data as well. The inability to control when and how this happened would appear to have influenced the ECJ's reasoning, thereby sounding the agreement's death knell.

A growing sense of unease at just how much of the world's Internet infrastructure is housed within US borders has developed around Europe in recent years.

With so much data flowing there from every corner of the planet, it offers not just a substantial commercial advantage for US companies but also a leg up for Washington in the political and national security stakes, too. Europe could not allow that trend to carry on unchecked.

What Europe wants instead are new data warehouses set up within the EU. It's an ambitious play, but with the data storage industry valued at $100bn, it's also hardly surprising.

Of course, the ECJ's decision is not insurmountable. Those in the know will tell you that the export of data to the US can continue subject to agreements founded upon the EU's model clauses.

The smart money though is on these also being tightened up before too long, especially with the General Data Protection Regulation looking like it may come into force by the end of 2017.

However, are restrictions on moving data to the US a good thing and what are the likely repercussions for the insurance industry of the ECJ's changes?

From a European standpoint, the idea of a more protective environment that simultaneously fosters the growth of our own tech companies capable of competing with the best the US has to offer is undoubtedly positive and exciting.

But is it realistic? After all, if Europe wants its citizens' data kept in the EU as a condition of US companies being allowed to trade within its borders, the same is likely for European companies wanting to do business across the pond.

In turn that's likely to impede all but the biggest companies which can afford to implement such measures, effectively stifling innovation, new start-ups and depriving customers of the choice they currently enjoy.

If that happens, the Internet won't be the global phenomena it is currently, but instead a segregated trade zone with fewer opportunities for consumers and vendors beyond their national borders. It's ironic really given the principle of a single market upon which the EU was originally founded.

From the American perspective, US companies in industries such as online advertising, social media site providers and cloud services will now have to more closely monitor and comply with the privacy regulations for each EU country.

While an updated Safe Harbour Agreement is being negotiated between the US and the European Commission, when and how it will be implemented is unknown.

The EU has a much stronger position with the ECJ's decision invalidating the current agreement.
As a result, US companies must begin to ensure they comply with all 28 EU countries' privacy and security regulations.

While most commentators feel the national data protection regulators will not immediately start investigating US companies, the companies cannot afford to be caught flat footed if they are suddenly told to change their procedures or have their international transfers suspended by 28 diverse countries.

Since US companies already must deal with 47 different US state data breach statutes, federal HIPAA regulations, SEC and FTC regulations, companies should understand how to handle a large variety of privacy rules and regulations.

The disruption may not be as significant as initial reports suggest, but the implications are clear, the EU will move to force US companies to provide stronger privacy security for its citizens.

In addition, it's a safe bet that US companies will have to increase their privacy security, and the inevitable costs, to become more in line with the EU.

Global transfer of personal data is only going to increase, and the two recent decisions demonstrate that if US companies want to play in the EU, they will have to play by their rules.

How EU members and their local regulators define an "adequate level of protection" for personal data should become a key focal point for US companies that want to transfer European customers' personal data to the US.

The impact of the ECJ's decisions on insurance must not be overlooked either.

The creation of multi-jurisdictional exposure to regulatory action will have expanded significantly the risk to which many insurers of cyber policies had thought they'd signed up.

Conversely, some policyholders may now find themselves without cover for jurisdictions where previously they had expected none. Modeling for these new exposures will also need to be rapid, with the spectre of many overwhelmingly complex aggregation scenarios looming on the horizon to be factored in.

Ed Lewis is an insurance and reinsurance partner in the EC3 team at Weightmans and David Shannon chairs the Privacy and Data Security and the Technology, Media & IP Practice Groups at US law firm Marshall Dennehey Warner Coleman & Goggin.