A huge tipping point for NZ cloud computing providers and customers?

October 2015

Speed read

Europe's highest court has turned the US into a privacy pariah, and the fallout could have a major impact on New Zealand businesses.

Tech companies and cloud computing providers, big and small alike, are staring down the barrel of increasingly uncertain privacy compliance challenges, as are their customers. Offshore data storage suddenly has an added dimension of risk. This could be a major tipping point in how cloud computing evolves, both internationally and specifically in New Zealand.

According to the European Court of Justice, personal data is not adequately protected in the US because it can be readily acces sed by US government authorities. The court has ruled that the EU's "Safe Harbour" agreement with the US, and which provides the legal basis for EU/US data transfers, is invalid.

Beyond the immediate consternation of global data giants like Facebook, Google and Microsoft, the wider commercial consequences of this judgment will be significant.

In privacy terms, the US is now *persona non grata*.

New Zealand businesses with a US presence – Xero, for instance – may move their non-US data well away from US servers. And if developments snowball further, New Zealand's data protection standards could be subjected to the same scrutiny as the US.

This article first appeared in the *National Business Review* (http://www.nbr.co.nz/article/huge-tipping-point-nz-cloud-computing-providers-and-customers-180488) on 23 October 2015.

The Detail

'Safe Harbour' decision

The right to privacy is heavily protected under EU law, where businesses are only permitted to transfer personal data to third party countries that maintain privacy standards comparable to those in the EU.

Since 2000, the EU/US Safe Harbour pact has enabled data transfers to the US on this basis. However, in light of the Edward Snowden leaks about American government access to US-based information, the ECJ's recent ruling has rendered the agreement invalid.

An updated version of the Safe Harbour pact has been under negotiation for two years or, in other words, since the Snowden leaks. Few expect that the EU/US attitudes to privacy will be reconciled easily. Yves

A huge tipping point for NZ cloud computing providers and customers?

Bot, the Advocate General at the European Court, has stressed that "the surveillance carried out by the US is mass, indiscriminate surveillance ... in those circumstances, a third country cannot in any event be regarded as ensuring an adequate level of protection."

In a post-Safe Harbour world, there remain alternative methods of legally executing EU data transfers to the US. A likely option is to implement model clauses – standard form contractual clauses approved by the European Commission – which outline sufficiently adequate privacy obligations.

But there's a problem with this as well. The European Court has ruled that the EU's national privacy regulators are entitled to make their own investigations into offshore privacy compliance, and suspend data transfers as necessary. The possibility of independent regulatory action, and the fact that privacy doctrines across the EU's member states vary markedly, mean the commission's model clauses will not automatically ensure compliance across Europe.

How does it affect New Zealand?

The net result of this situation is commercial uncertainty for multinationals, data processing companies, cloud service provider, and any organisation using these services in an international context.

New Zealand businesses with US connections, such as US-based cloud solutions, are the most directly affected. Not only will these businesses need to ensure personal data transferred from Europe to US servers is protected in accordance with EU privacy law but the European Court's rejection of Safe Harbour will probably prompt other jurisdictions to reconsider the legality of US data storage. Expect complaints under New Zealand law that, in the absence of adequate contractual commitments, transferring personal data to US servers is inconsistent with New Zealand's privacy principles.

The judgment also intensifies concerns about the adequacy of privacy standards outside the US.

New Zealand is one of a select group of countries whose data protection standards are deemed adequate under EU law but this might be revised because of Edward Snowden's revelations about New Zealand's role in the Five Eyes network. (If not reviewed by the European Commission, then it possibly may be by a national EU regulator utilising their new investigative powers).

I spoke to privacy specialist and former assistant privacy commissioner Katrine Evans, now a senior associate at Hayman Lawyers, who said:

> *The best advice at the moment is probably to follow the mantra of the Hitchhikers' Guide – don't panic. It will take a while for the implications of the decision to play out, and most of the immediate impact will be in Europe and the US.*
>
> *But could it affect our businesses? Absolutely. There have already been calls from Europe to re-examine our "adequacy" [privacy white-list] status because of our membership of Five Eyes. The court's reasoning adds some fuel to the fire. If we lose our white-list status, there would be disincentives for European companies to send personal information here, and it would increase costs of developing contracts. So our discussions with European officials will matter a great deal.*

A huge tipping point

Add it all together, and you have a potentially massive multinational disruption about where and how data on the cloud is hosted, well beyond data with a US and/

A huge tipping point for NZ cloud computing providers and customers?

or EU component. What's it going to do for New Zealand-based cloud providers and their offshore customers? And for offshore providers to New Zealand-based customers? Will this lead to a major change in where data is hosted (for example, largely only in the customer's own country, as the patchwork quilt unravels country by country?).

Can New Zealand emerge as an internationally strong data oasis in a privacy desert, with the economic benefits that entails? Will we be recognised by regulators such as the EU, after the inevitable review of New Zealand's data protection status?

Or will Five Eyes and other intelligence operations consign New Zealand to a US-like international data ghetto?

Given the importance of data flows and cloud services to modern commerce, the ECJ's disruptive decision could turn out to be a game-changing tipping point.

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com