

## WHAT IF A “SAFE HARBOR” IS UNSAFE? THE GLOBAL IMPACT OF POOR U.S. DATA SECURITY

By Clint Fillipou, Principal

7 December 2015

As marketers reach customers and collect data about those customers in an increasingly global way, it is hard to fathom that we still toil in a system of separate, largely domestic privacy laws. After all, what happens when you can't fully trust the laws and enforcement procedures of one of the largest markets of them all? Does the whole system fall down? A major recent EU case has placed USA privacy regulations in the spotlight and we should all sit up and take note.

### The EU “Schrems case” and its impact on the “Safe Harbor” framework

As you may already be aware, privacy law is generally dealt with on a country-by-country basis, while the EU has a large and interconnected framework that governs the entire European Economic Area. Until now, it was only acceptable for entities in the EEA to send personal information to countries outside the EEA if those entities resided in one of a small number of countries declared to have “adequate” privacy laws, or if the recipient was bound to a contract or some other rules that were satisfactory.

Australia's privacy framework was not deemed “adequate” for instance, and neither was that of the USA. Unlike here in Australia however, the USA established the “Safe Harbor” provisions which entities could agree to comply with – the provisions were essentially a scheme to impose more detailed privacy obligations on those entities so as to satisfy the European Commission that they were “safe enough” to be allowed to receive personal information from EU businesses. The Schrems case effectively pulled back the curtain a little and the Safe Harbor rules were clearly shown to be inadequate to protect the personal information according to EU standards. This landmark case has effectively killed the “Safe Harbor” in the USA, which means that the USA is no longer an exception to the general EU rules on personal information transfers. In essence, the USA is now no different to Australia or many other developed nations, in terms of receipt of personal information from entities in the EU.

### So what does it mean here in Australia, for us?

Well, in short, we must take particular care any time we send any personal information to the USA. The Schrems case has not necessarily changed this for us – such care has always been prudent for Australian entities and this has not changed. To explain how Anisimoff Legal expects Schrems to impact us here in Australia, we need to backtrack a little and clarify that the Australian privacy law acts in much the same way as Europe when it comes to sending personal information overseas. In short, in Australia:

- a) an Australian entity disclosing personal information to an overseas recipient must take reasonable steps to ensure the recipient does not breach the *Australian Privacy Principles* (APPs), and the Australian entity will be accountable for any such breach by the recipient;
- b) The above point a) won't apply if the Australian entity reasonably believes the recipient is subject to a law or binding scheme imposing privacy protections that are substantially similar to the APPs;
- c) Point a) also doesn't apply where the individual consents to the disclosure and to the Australian organisation not being accountable for the acts of the overseas recipient.

While Schrems doesn't change the Australian law it does shine a spotlight on points a) and b) above. It is obviously a difficult if not impossible challenge for an Australian business to properly analyse an overseas third party's privacy practices and procedures, or to assess their regulatory obligations, outside of perhaps briefly reading their privacy policy. The simplest and most effective way for an Australian business to satisfy itself that it is compliant with Australian law when sending personal information overseas is still a very effective, properly worded contract forcing the overseas recipient to comply with Australian law, including the APPs, and provide indemnification in respect of any loss or damage caused by breach.

Specifically now, in light of Schrems, Australian businesses need to be particularly careful when dealing with businesses in the USA. Schrems highlights for us that we can no longer satisfy ourselves or be comforted by a USA company claiming EU "Safe Harbor" compliance as indicative of satisfying Australian privacy concerns. We should also watch this space closely, to see if there is any regulatory or policy shift in either the US or EU – as mentioned above, it's a very small world nowadays.

## Contact us

If you would like further information on cross-border information flows, international privacy issues or you have any kind of privacy questions, please contact us.

### Clint Fillipou

+61 3 9907 4302

[clint.fillipou@anisimoff.com.au](mailto:clint.fillipou@anisimoff.com.au)

### Heidi Bruce

+61 2 8935 8806

[heidi.bruce@anisimoff.com.au](mailto:heidi.bruce@anisimoff.com.au)



[www.anisimoff.com.au](http://www.anisimoff.com.au)



<https://www.facebook.com/AnisimoffLegal>



<https://twitter.com/AnisimoffLegal>



<http://www.linkedin.com/company/anisimoff-legal>