"Good news" for the APEC Cross-Border Privacy Rules

FTC settles with Vipvape on CBPR privacy policy deception

The Asia-Pacific Economic Cooperation ('APEC') Cross-Border Privacy Rules ('CBPR') may not yet have reached the 'most stolen privacy seal' status, but a recent case by the US Federal Trade Commission ('FTC') may have revealed that this up-and-coming Asia Pacific-based cross-border data transfer mechanism is gaining recognition and may very well be on that trajectory.

The case

On 4 May 2016, the FTC announced its settlement with the hand-held vaporisers manufacturer Very Incognito Technologies, Inc., also known as Vipvape, relating to a claim of alleged deception in its privacy policy. Apparently, Vipvape had falsely claimed that it was certified under the APEC CBPR system, a regional, multilateral, cross-border data transfer mechanism and enforceable privacy code of conduct for businesses that was developed and finalised in 2011 by the 21 APEC member economies. According to the FTC's complaint, Vipvape included in its privacy policy the following statement: 'Vipvape abides by the APEC CBPR System. The APEC CBPR system provides a framework for organisations to ensure protection of personal information transferred among participating APEC economies.'

The CBPR system does do that, but only for companies that obtain certification from an APEC-recognised third party certifier or 'accountability agent,' like US-based TRUSTe or the Japan-based trustmark JIPDEC, which Vipvape apparently had not done.

The settlement between the FTC and Vipvape prohibits Vipvape from misleading consumers about its participation in any privacy and security certification programme, including the APEC CBPR system, going forward. According to the FTC's Chairwoman Edith Ramirez, the FTC is "committed to vigorously enforcing cross-border privacy commitments" and "[c]onsumers should be able to rely on a company's claim that it is a certified participant in an international programme designed to protect personal information."

Conclusions

The Vipvave action and the Chairwoman's statement bode well for the APEC CBPR. In the past, the CBPR had, at times, been mischaracterised as a self-regulatory system with little substantive rigour or bindingness on participants. Nothing could be further from the truth and the Vipvape case proves it. In fact, governmental oversight and enforceability of the CBPR are mandated by the terms of the system itself. It allows only those APEC countries that can and will enforce the CBPR to participate in it. And each participating APEC country must have at least one privacy cop on the CBPR beat - the FTC in the case of the US. This cop must also participate in the APEC Cross-border Privacy Enforcement Arrangement ('CPEA'), which is a multi-lateral cooperation arrangement for APEC privacy authorities specifically developed to enable CBPR backstop enforcement.

Of course, the CBPR system is still in its infancy - four participating countries, two accountability agents, 15 certified companies – but more of each in the pipeline. But the fact that the FTC has taken an enforcement action so early on the development of this cross-border privacy code of conduct sends two important signals: one, CBPR certification, apparently, is seen to add value and stature to an organisation's privacy policy, and two, the CBPR are on the FTC's radar and will be enforced, which will benefit the credibility of the system as it takes off over the next couple of years as the principal cross-border transfer mechanism in the Asia-Pacific region.

Markus Heyder Vice President and Senior Policy Counselor
The Centre for Information Policy Leadership at Hunton & Williams, Washington D.C.
MHeyder@hunton.com