Data Protection and Privacy Group

CLYDE&CO

Global Data & Privacy Update

Clyde & Co's Weekly Update 29.01.15

EU air passenger data to be handed to police

Under a new European Commission proposal which was just announced, every airline passenger flying in or out of the EU will have their personal data, including bank card details, stored on a police database for up to five years and shared between the member states. This proposal contains tighter data protection rules than its predecessor. Although supported by the majority of the European interior ministers in the fight against counter terrorism, civil liberties campaigners are concerned that the move would still invade the privacy of passengers.

WikiLeaks accuses Google and US Government of privacy violations

This week, WikiLeaks' lawyers sent a letter to both Google and the US Department of Justice (DOJ) alleging "a serious violation of the privacy and journalist rights of WikiLeaks' staff". The allegations follow evidence that Google handed the DOJ emails and metadata, apparently in response to warrants, without providing notification to WikiLeaks until almost three years later.

Social media denies cyber-attacks

Both the website and mobile versions of social media giants Facebook and Instagram were temporarily brought down this week. Although Lizard Squad claimed responsibility for the attacks via Twitter, a spokesperson for Facebook, which owns Instagram, denied that the sites were hacked. They blamed a technical hitch after they "introduced a change that affected our configuration systems".

US FTC recommends self-regulation for IoT

The US Federal Trade Commission issued a report this week on the Internet of Things (IoT), with steps for businesses to 'enhance and protect consumers' privacy and security'. The report recommends technology-neutral (not IoT specific) legislation coupled with self-regulation and suggests that security is built into the devices at the outset, "security by design". The report has been largely commended for its stance which remains vigilant about privacy, but allows for innovation.

Criticism over China's new cyber-security rules

At the end of last year, the Chinese government adopted new regulations requiring companies that sell IT equipment to Chinese banks to build "back doors" into hardware and software, reveal secret source code and submit to invasive audits. This week, foreign business groups, including the US Chamber of Commerce, sent a letter to the government committee on cyber-security, objecting to the new policies and calling for "urgent discussion and dialogue".

Banks ask for more data sharing

Some of world's biggest banks are in discussions with regulators urging them to relax privacy laws to allow increased sharing of client data. This follows fears about the impact of "financial abandonment" as banks withdraw from riskier emerging markets. In particular, US dollar clearing banks have been severing ties with lenders in developing nations in light of regulators cracking down on sanctions breaches, money laundering and terrorism financing.

New Cyber Security Agency in Singapore

The Singapore government has established a new Cyber Security Agency (CSA), which is tasked with overseeing the country's cyber-security operation and leading future developments in this area. The CSA is scheduled to commence operations on 1 April of this year with the aim to consolidate the government's cybersecurity capabilities. It will also work with the private sector to bolster the local IT security ecosystem.

For further information please contact:
Margaret Tofalides
E: margaret.tofalides@clydeco.com

www.clydeco.com

CC006781 - January 2015