

Global Data & Privacy Update

Clyde & Co's Weekly Update 11.12.14

UK Information Commissioner intervenes in Google hearing

This week, the UK's Information Commissioner took the rare step of intervening in the Court of Appeal case in relation to the ruling that Google exploited security loopholes to track devices for advertising. Google's appeal is based on the argument that consumers did not suffer financial harm as required under section 13 of the Data Protection Act (DPA). The Commissioner submitted that the interpretation of damage under this section is a serious issue to be tried and the outcome will be an important test of the provision.

Microsoft claims bid to seize Irish emails threatens US citizen's privacy

In its ongoing legal battle against the US government, Microsoft filed a brief this week submitting that, if the warrant to seize emails stored on a Microsoft server in Ireland is carried out, it would open the door to such seizures in the US, endangering the privacy of US citizens. The Irish government has asked the European Commission for legal aid in this case and has warned that if the warrant is executed, European data protection laws may effectively be bypassed.

Internet companies push to be excluded from EU cyber security law

Internet firms, including Google and Cisco, have asked to be left out of the new EU cybersecurity law, the so-called Network and Information Security Directive, which would force them to report serious security breaches to national authorities. The directive is due to be finalised in talks between the European Commission, the European Parliament and Member States over the coming weeks and so far covers sectors considered critical, such as energy, transport and finance.

DDOS attack on Sony

Following last month's cyber-attack on Sony Pictures Entertainment, Sony Corp has confirmed that its PlayStation Network and Sony Entertainment Network suffered a distributed denial-of-service (DDOS) attack this week. Sony has said that its systems are back online and, whilst the company is still investigating the disruption, there is no indication of user information being stolen. It is thought that a few hundred addresses were affected.

Bebe confirms cyber-attack

Bebe Stores Inc. confirmed its credit card breach last week and announced the hackers gained access to data from cards used between 8th to 26th November. It is believed that the stolen data included card numbers, cardholder names, verification codes and expiration dates. The retailer said that transactions completed online were not affected.

New US cyber security unit

The US Department of Justice is creating a specialised unit within its criminal division to advise on electronic surveillance in cyber investigations and to help the private sector prevent online crime. Leslie Caldwell, head of the department's criminal division, said the new unit would also help temper what she called growing public distrust of law enforcement surveillance and investigative techniques.

OAIC to remain operational

The Office of the Australian Information Commissioner (OAIC), which was supposed to close at the end of this month, was granted a reprieve as the Bill which proposed its closure was not considered by the Australian Senate in time. The OAIC will remain operational until further notice and is currently liaising with the Australian Government about transitional arrangements.

For further information please contact:

Margaret Tofalides

E: margaret.tofalides@clydeco.com

Clyde & Co LLP is a limited liability partnership registered in England and Wales. Authorised and regulated by the Solicitors Regulation Authority.

© Clyde & Co LLP 2014

www.clydeco.com