SQUIRE PATTON BOGGS

WEEKLY DATA PRIVACY ALERT
27 OCTOBER 2014

UK

ICO Active in Establishing New Commonwealth Network of Privacy Regulators

The Information Commissioner's Office (ICO) has played a part in establishing a new network of privacy regulators from across the Commonwealth. The network will be known as the Common Thread Network and its objective will be to enable the sharing of experience, knowledge and expertise on data protection matters between Commonwealth countries. The intention is that this will facilitate co-ordinated cross-border responses to key data protection issues, currently seen as the growth of the Internet, international data transfers and increased use of cloud technology.

ICO news release – 17 October 2014

ICO Discusses New Co-Operation Framework in Blog Post

In a new blog post, the ICO has explained the benefits it sees as coming out of the recently agreed framework for international data protection enforcement. The new framework, agreed at the International Conference of Data Protection and Privacy Commissioners, sets out how national regulatory authorities will work co-operatively on cross-border investigations, making them more effective and efficient. The ICO identifies the key benefits of the framework as avoiding frustrations and delays which currently result from each data protection authority wanting to handle a cross-border matter "their way", emerging economics benefitting from the data expertise of larger countries and the wider political benefits of helping to make a case for a proportionate, risk-based approach to data regulation.

ICO blog post – 21 October 2014

Call for Journalists to Have New Public Interest Defence to Allegations of Data Breaches

Deputy Prime Minister Nick Clegg has called for a new public interest defence to be introduced to protect journalists accused of data protection breaches. He said that journalists should be able to "go after information in the public interest without fear of being prosecuted". This proposal has yet to receive wider backing from the coalition but it is thought that a new defence would be added to the Data Protection Act for journalists who unlawfully obtain personal data (contrary to section 55) where they do so as part of reporting a wider story in the public interest.

Guardian news report – 20 October 2014

IFB Expansion to Combat Insurance Fraud Industry Wide

The Insurance Fraud Bureau (IFB) has announced plans to expand its focus beyond motor claims. From 2015, the IFB will become the central hub for all fraud data intelligence across the insurance industry as a whole in an effort to combat organised insurance fraud.

IFB news release – October 2014

EU

Process Begins to Appoint New EU Data Protection Supervisor

The process of appointing the next European Data Protection Supervisor (and Assistant Supervisor) begins the week of 27 October. The European Parliament will question the five shortlisted candidates for these posts before consulting with the European Council to agree on who should be appointed to each role. The European Data Protection Supervisor is in post for five years and has responsibility for EU data protection legislation and policies, ensuring data compliance by EU institutions and encouraging cross-border co-operation on privacy issues.

European Parliament news – 20 October 2014

US

Obama Administration Addresses Financial Cybersecurity

On October 17, President Obama signed an Executive Order designed to improve the financial cybersecurity of consumer financial transactions. The Executive Order requires the federal government to take steps to implement greater security protections for governmental payments, including government-issued payment cards, and to protect sensitive data about individuals that is collected and made available online by implementing, for example, multiple factors of authentication. In addition, federal agencies are required to assist and co-ordinate efforts to combat identity theft in conjunction with the Federal Trade Commission (FTC) and its www.identitytheft.gov website.

White House Press Office – October 2014

US District Court Rejects Claims that Mobile Phone IDs Constitute Personal Information

A US district court in Georgia has dismissed a claim of a violation of the Video Privacy Protection Act against Cartoon Network, a cable TV channel provider, because a randomly generated mobile phone ID did not constitute personally identifiable information (PII). A class action lawsuit claimed that the Cartoon Network's mobile app collected a third party user's video history and Android smartphone ID and provided it to a third party data analytics company, which was able to reverse-engineer this information to identify the users. The court dismissed the lawsuit as the randomly generated Android smartphone ID did not constitute PII under the statute because it was randomly generated and, by itself, did not identify the user without being combined with other sources.

Ellis v The Cartoon Network Inc – October 2014

FTC Stresses Privacy and Data Security Obligations of Broadband Providers

In comments to the Federal Communications Commission (FCC), the FTC has outlined the several key privacy and data security obligations of providers of broadband services in an FCC proceeding examining barriers to consumer adoption of these services. Where an entity makes promises or commitments, whether expressly or implicitly, regarding its privacy and data security practices, but then fails to live up to these commitments, the entity may be liable for a violation of the FTC Act's prohibition against "deceptive or unfair business practices." In addition, broadband providers may be subject to the Children's Online Privacy Protection Act's (COPPA) protections for online services and child-directed websites. Finally, broadband service providers may need to comply with the privacy and data security requirements found in the Fair Credit Report Act (FCRA) to the extent they may provide covered information regarding their subscribers to credit bureaus or use credit reports.

Federal Trade Commission comments

California Toughens its Data Breach Law

Governor Jerry Brown of California has signed into law AB 1710, which strengthens the state's existing data breach notification law. Three major changes are made by AB 1710: (1) that any offer to provide identity prevention and mitigation services to an individual receiving a breach notification must be for a period of not less than 12 months and at no cost to the individual; (2) expansion of the requirement of businesses that "own or license" personal information of California residents to implement appropriate and reasonable security procedures and practices to apply also to businesses that "maintain" personal information, such as service providers ; and (3) a prohibition on the sale, offer for sale or advertising for sale of Social Security numbers of California residents.

Assembly Bill No. 1710

SIFMA Publishes New Cybersecurity Principles

The Securities Industry and Financial Markets Association (SIFMA) has published its Principles for Effective Cybersecurity Regulatory Guidance. Its objective is to help regulators develop cybersecurity regulatory guidance that is specifically appropriate for the financial services industry. The guidance sets out 10 key principles, based on the observations of SIFMA members, which SIFMA hopes will form the basis of robust and efficient cybersecurity guidance from regulators for the industry.

SIFMA – 20 October 2014

GLOBAL

Data from the "Internet of Things" is Personal Data

Data protection regulators from around the world have agreed that data generated by devices in the "Internet of Things" (IoT) should be treated as personal data. Agreement was reached at an International Privacy Conference held in Mauritius the week of 20 October and a declaration published. Although the declaration is non-binding it is likely to be followed by those data protection regulators signing up to it, meaning that businesses with involvement in the IoT should be prepared to process data generated in line with their own national data protection laws.

Mauritius declaration – October 2014

For further information on any of the items in this week's alert, please contact:

Mark Gleeson (London)
T: +44 20 7655 1465
E: mark.gleeson@squirepb.com

Mark Johnson (Washington DC)
T: +1 202 626 6265
E: mark.johnson@squirepb.com