SQUIRE PATTON BOGGS

WEEKLY DATA PRIVACY ALERT
20 JULY 2015

The Squire Patton Boggs Data Protection & Cybersecurity team is pleased to share with you a weekly alert on data privacy issues. This week's alert covers news from Australia, the EU, UK and the US.

Australia

Office of the Australian Information Commissioner Releases Guide to Privacy Regulatory Action

The Office of the Australian Information Commissioner has released a guide titled "Guide to Privacy Regulatory Action". The guide provides guidance in relation to regulatory powers provided under Australian legislation. Each chapter includes information about the legislative framework, purpose and procedural steps for exercising the regulatory power.

The purpose of the guide is to provide a source of information for entities about the Office of the Australian Information Commissioner's exercise of particular regulatory powers and to facilitate efficient and effective regulatory action.

OAIC Guide to Privacy Regulatory Action (PDF)

EU

Article 29 Working Party Opinion on the Draft Data Protection Regulation

On 19 June 2015, the Article 29 Data Protection Working Party published an opinion on the draft Regulation in view of the "trilogue" discussions which have recently commenced between the European Parliament, the European Commission and the European Council. If agreed, the Regulation would introduce a new single data protection law for the whole of the EU.

In their published opinion, the Working Party expressed the need for the Regulation to maintain the same level of protections currently provided by the Data Protection Directive and to ensure that its core principles and rights are not undermined. The Working Party cautioned against the dilution of the purpose limitation principle and called for a reassessment of the powers and resources of data protection authorities.

The Working Party suggests that personal data should be defined in a broad manner in line with technological evolution in order to ensure that the general objective of maintaining a high-level of protection of personal data is upheld. The Working Party also suggests that the definition of personal data should therefore take into account the situation in which people can be "singled out" on the basis of identifiers or other information.

Article 29 Working Party Opinion (PDF)

Draft EU Rules Approved Concerning the Passenger Name Record Data of People Flying to or From the EU

On 17 July, draft EU rules in relation to the sharing and protecting of the Passenger Name Record (PNR) data of people flying to or from the EU, and its use by member states and Europol to fight terrorism, were approved by the Civil Liberties Committee.

The PNR rules would only apply to air carriers and non-carriers such as travel agencies and tour operators operating international flights, intra-EU flights would not be included under the rules. The data will only be used to prevent, detect, investigate and prosecute terrorism and serious transnational crimes and a number of safeguards will be inserted in order to ensure that the data is dealt with lawfully.

Trilogue talks are anticipated to commence soon.

Passenger Name Records Press Release

Russia

Russian Parliament Approves "Right To Be Forgotten" in Search Engines

On 13 July 2015 the President of the Russian Federation signed Federal Law No. 264–FZ "On Amendments to Federal Law on Information, Information Technology and Protection of Information" and to Articles 29 and 402 of the Russian Civil Procedure Code" ("the Law"), which will enable individuals to request that Internet search engines delete links to websites containing certain information about such individuals. The Law will come into force on 1 January 2016.

The Law uses the term "search engine operator", which distributes advertisements via the Internet addressed to the consumers located in the territory of the Russian Federation (the "Search Engine Operator"). Thus the Law can be interpreted as applying to such search engines as Google, Yandex, Rambler, etc.

Upon an individual's request the Search Engine Operator must remove web links, enabling access to information pertaining to such individual, from search results. More specifically, the Law refers to information which is:

- disseminated in contravention of the Russian law, incorrect; or
- obsolete and no longer relevant for that individual due to subsequent events or his actions.

The Law does not elaborate on what qualifies as, or what are the criteria for, obsolete and irrelevant information. This may be subject to judicial interpretation. The Law will not apply to information concerning allegations of crime in respect of or criminal records of such individual, subject to certain time limitations.

To exercise the "right to be forgotten" an individual must file a request with the Search Engine Operator along with his identity details, web links in question and grounds to remove such web links from search results..

Within 10 working days from receipt of such request the Search Engine Operator must either satisfy or reject the request. If an individual disagrees with the rejection he may appeal to the court. Such a claim will be considered in accordance with the Russian civil procedure legislation.

Currently there is no specific liability provided to be imposed on the Search Engine Operator for ignoring or rejecting an individual's request. However, the recent draft law under No. 804140-6 "On Amendments to the Code of Administrative Offenses of the Russian Federation (with regard to the introduction of administrative liability of search system operators)" proposes to introduce such liability for:

- failure to satisfy an individual's request – 100,000 Rubles (approx. US$ 1,700); and
- failure to comply with the court's ruling on the individual's claim for removing web-links enabling access to information on that individual within five days – 3 million Rubles (approx. US$ 53,000).

This draft law is still under the consideration in the State Duma.

UK

Internet of Things Launches a £10 million Competition for UK Cities

UK cities and businesses can bid for a £10 million government fund to revolutionise the way the Internet of Things (IoT) benefits citizens. The Department for Culture, Media and Sport and Innovate UK are offering the money to a single collaborative research and development project which offers either environmental improvements, economic opportunities or more efficient and effective delivery of services such a transport, healthcare and energy.

All competition entries must involve IoT, and additional requirements include:

- A specific benefit for citizens, the city region and the environment;
- Economic benefits for businesses and local authorities, both during and after the initial trial;
- Appropriate security and privacy features; and
- Entries must be able to work across a variety of sectors, for example social care, transport and housing.

Information on the Internet of Things Competition

Independent Surveillance Review Publishes "A Democratic Licence to Operate"

Following a year of consultation, the Independent Surveillance Review has presented its report, "A Democratic Licence to Operate". The Review highlights how democracy should combine a respect for privacy and freedom of speech whilst maintaining high levels of security.

The review panel recommends that the intrusive investigative techniques used on the Internet and in relation to digital data are brought into full compliance with the human rights framework. The Review also sets out 10 tests that any new legislation should pass before it can be regarded as giving the police and intelligence agencies a democratic licence to operate.

A Democratic Licence to Operate (PDF)

MPs Win Surveillance Powers Legal Challenge

On 17 July 2015, two conservative MPs, David Davis and Tom Watson, won a High Court battle in relation to the Data Retention and Investigatory Powers Act's incompatibility with articles 7 and 8 of the EU Charter of Fundamental Rights. The Act permits Britain's security agencies and other public bodies to gather information about the UK citizens who suspects have contacted by telephone or email. The two High Court Judges in the case ruled that the Act is inconsistent with EU law thus effectively nullifying parts of the legislation.

The order has been suspended until March 2016.

David Davis and others v Secretary of State for the Home Department [2015] EWHC 2092 (PDF)

US

The Federal Trade Commission release "Start with Security: A Guide for Business"

The Federal Trade Commission has released a guide titled "Start with Security: a Guide to Business". The guide draws from the lessons learnt from more than 50 law enforcement actions and provides practical guidance on how to reduce the risks posed by vulnerabilities that could affect companies. The guidance discusses subjects such as access to data, authentication processes, storage of data and physical security of businesses.

Start with Security: A Guide for Business (PDF)

Squire Patton Boggs News

Opinion Piece by Andreas Fillmann: The Digital Single Market: Privacy and Security to be observed

The adoption of the envisaged Digital Single Market on 6 May 2015 highlighted the important role that banks and financial institutions will play in the EU Commission's strategy going forward. Together the banks and financial institutions will be expected to deliver over 16 initiatives by the end of 2016, including providing a framework for future digital banking activities. Privacy and security continue to remain key priorities in the area of digital banking, particularly in relation to online payments, mobile banking, security systems, data analytics and protection.

In light of the planned changes for the digital banking services in Europe, any reform in relation to data protection will need to be monitored due to its potential impact on mobile banking. On 15 June 2015, the Council of the EU approved its version of the Regulation which aims to give EU citizens control over of their personal data and to simplify the regulatory environment for businesses in the EU. Equally, the new EU Data protection rules provide the basis for a review of Directive 2002/58/EC which concerns the processing of personal data and the protection of privacy in the electronic communications sector.

The EU Commission aims to further promote the unrestricted movement of big data in Europe. This initiative will focus on the restrictions on data location and also hopes to encourage innovation through access to public data. In addition, the EU Commission will launch a European Cloud initiative which will include cloud services certification, switching of cloud service providers and a research cloud.

Data Privacy & Cybersecurity Conference – Data in a Global Marketplace – Minimising Risks, Maximising Opportunities

We are pleased to be hosting a Data Privacy & Cybersecurity Conference at our London office. The conference will include speakers from the UK's Information Commissioner's Office, leading industry figures and experts from our Data Privacy & Cybersecurity team. Attendees will gain insight into a range of current privacy issues impacting businesses throughout Europe including:

- The draft General Data Protection Regulation
- The opportunities and challenges from Big Data
- Managing multi-country privacy compliance
- Technology takeover
- Cybersecurity

Please visit our website for additional details.

Contacts

Mark Gleeson
Partner, London
T +44 20 7655 1465
E mark.gleeson@squirepb.com

Andreas Fillmann
Partner, Frankfurt
T +49 69 17392 423
E andreas.fillmann@squirepb.com

Irina P. Golovanova
Senior Associate, Moscow
T +7 495 258 5250
E irina.golovanova@squirepb.com

Alexey Pashinskiy
Associate, Moscow
T +7 495 258 5250
E alexey.pashinskiy@squirepb.com

20178/07/15