SQUIRE PATTON BOGGS

Weekly Data Privacy Alert

17 May 2016

EU

New Rules Give Europol More Power to Fight Cybercrime

On 11 May 2016, the EU Commission approved new powers for Europol – the EU's law enforcement agency – to fight international crimes such as terrorism and cybercrime. The organisation will now be able to liaise with private entities directly in order to exchange information, and also imposes a strict duty on Member States to provide Europol with the data it needs. The regulation, which will take effect from 1 May 2017, comes with robust data protection safeguards. The European Data Protection Supervisor will monitor Europol and provide a clear avenue for complaints from citizens throughout the European territory.

Press release

France

The CNIL Prioritises Its Topics of Investigation

The Commission Nationale de l'Informatique et des Libertés (CNIL) has estimated that it will carry out between 400-450 investigations in 2016 alone. The inquiries will vary between onsite investigations, hearings and document or online reviews, and will focus on the following main themes which the CNIL estimates will represent 25% of the agency's total investigations:

- The SNIIRAM: The national system of inter-systems of health insurance information
- The API-PNR file: The API-PNR system (Advance Passenger Information Passenger-Name Record)
- The Data brokers: the CNIL's intention in this instance is to ensure compliance with the principles of proportionality, relevance of data and information, consent, the rights of the data subject and security

Aside from these main topics, investigations will be made in relation to: complaints received by the CNIL (20%); following up on verification or issues revealed by the press (approximately 35%), and CCTV (approximately 20%).

Press release (in French)

UK

Nuisance Callers Face Tighter Controls

From 16 May 2016, marketing companies registered in the UK, even those with call centres located abroad, will no longer be able to withhold their telephone numbers when making unsolicited telephone calls. The move comes as part of a package of reforms aimed at shaking up existing laws in order to improve consumer protection and ensure that the Information Commissioner's Office (ICO) can investigate and penalise persistent offenders efficiently. The change under the Privacy and Electronic Communications (EC Directive) Regulation will mean that these companies will now be forced to display their telephone numbers when making unsolicited calls, making it easier for consumers to report unwanted callers to the ICO.

Press release (PDF)

Judicial Review into the Legality of UK Government's "Thematic Warrants"

Digital rights group, Privacy International, has filed a Judicial Review in the UK High Court over the government's use of general hacking warrants, challenging the Investigatory Powers Tribunal's decision to sanction the use of these so called "thematic warrants". These warrants allow British intelligence agencies to hack into devices, such as computers and telephones, of a wide class of people with a single warrant. The Investigatory Powers Bill, which is still going through the process of parliamentary debate, hopes to cement these powers in to law, with Privacy International arguing against the ability of the government to "log keystrokes, track locations, take covert photographs and videos, and access stored information".

Press release (PDF)

US

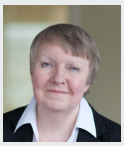
FTC and FCC Investigate the Mobile Device Industry's Security Updates Protocols

On 9 May 2016, the US Federal Trade Commission (FTC) and US Federal Communications Commission (FCC) commenced an investigation into mobile device security updates. The investigation stems from growing concerns over security vulnerabilities in mobile devices, such as smart-phones and tablets, and the effect of such vulnerabilities on the safety of personal communications and personal information. As part of the investigation the agencies are examining the practices of a number of carrier and device-manufacturing companies, including Apple, Verizon, Google and AT&T, regarding security updates and associated issues, such as the distribution of patches and patching vulnerabilities. These companies have been issued with an order to provide information on a number of related issues, such as the factors they consider in deciding whether to patch vulnerabilities on a particular mobile device, the vulnerabilities that have affected their devices, and whether or not they have successfully patched such vulnerabilities. The companies must respond to the agencies' inquiries within 45 days.

The Order (PDF)

Contacts

Annette Demmel
Partner, Berlin
T +49 30 7261 68 108
E annette.demmel@squirepb.com



Caroline Egan
Consultant
T +44 121 222 3386
E caroline.egan@squirepb.com

Francesca Fellowes
Senior Associate
T +44 113 284 7459
E franscesca.fellowes@squirepb.com

Stéphanie Faber
Of Counsel, avocat à la cour
T +33 1 5383 7400
E stephanie.faber@squirepb.com

Ivan Rothman
Of Counsel
T +1 415 954 0241
E ivan.rothman@squirepb.com