SQUIRE PATTON BOGGS

WEEKLY DATA PRIVACY ALERT
24 NOVEMBER 2014

UK

Pharmacist Fined for Spying on the Medical Records of Family and Friends

A pharmacist has been prosecuted under section 55 of the Data Protection Act for unlawfully accessing the medical records of family, work colleagues and other health professionals he knew, without any justifiable reason. Magistrates fined the pharmacist £1,000 and ordered him to pay a £100 victim surcharge and £608.30 in prosecution costs.

Information Commissioner's Office news release – November 2014

Health Board Ordered to Improve Privacy Processes After Data Breaches

The Information Commissioner's Office (ICO) has ordered a Scottish Health Board to take action to improve the protection of patient data. The ICO's warning follows six data breaches over a 13-month period which saw sensitive patient data left in public hospital areas and, on one occasion, at a supermarket.

ICO news release – November 2014

ICO Blog Post – Is Someone Watching You Right Now?

The ICO has published a blog post explaining how webcam users can secure their cameras and protect themselves from snooping. The post comes on the back of revelations about a Russian website which allows people to watch live footage from insecure webcams across the world, exploiting the use of weak password protection by camera owners.

ICO blog post – November 2014

Care Quality Commission Guidance on the Use of Cameras to Monitor Care Standards

The Care Quality Commission (CQC) has announced that it will publish guidance on the use of covert or surveillance cameras by people who want to monitor the care being provided to their relatives. The guidance will not condone or criticise the use of cameras for this purpose but will instead set out the issues the CQC expects relatives to take into account when deciding whether to install hidden or public cameras, such as first consulting with the care setting.

Care Quality Commission announcement – November 2014

ICO Guidance on Enforced Subject Access Requests

The Information Commissioner's Office (ICO) has issued new guidance on enforced subject access requests. The guidance explains the new criminal offence in section 56 of the Data Protection Act and has been published in anticipation of that section coming into force in full (introducing the new offence), which is expected to be on 1 December.

ICO website – Enforced Subject Access Requests

EU

Germany

Draft Law: Greens Want to Protect Whistleblowers

The German political party Bündnis 90/Die Grünen (The Greens) recently submitted a draft law on the protection of whistleblowers to the German Parliament. The legal position of whistleblowers in Germany is currently unclear and the draft law aims to rectify that. It provides that employees must first report issues of concern internally to their employer but if their employer ignores the report or the issues are of wider public interest then the employee may report their concerns to an external body at the outset.

Parliament press announcement – November 2014 and draft law

88th Conference of German Privacy Watchdogs Presents Its Resolutions

Following its most recent twice-yearly conference, the German data privacy watchdogs have presented their resolutions on current privacy topics. Amongst other things, they confirmed the importance of data protection as a basic personal right, called for privacy regulators to be given additional resources and more effective sanctions and welcomed the recent 'right to be forgotten ruling' from the Court of Justice of the European Union, calling for this right to be available to all internet users globally.

Announcement following 88th conference

International

US

Federal Court Orders Data Brokers to Protect Exposed Information and Notify Customers

In two separate cases brought by the Federal Trade Commission (FTC), the DC District Court has issued preliminary injunctions calling for the defendant data brokers to ensure that certain personally identifiable information is protected by reasonable safeguards, to cease disclosing such data without appropriate protection, and to notify affected consumers of the data exposure and how they can protect themselves from identity theft. The FTC alleges in both cases that defendants posted extensive personally identifiable information in spreadsheets on their publicly available websites in an effort to sell debt portfolios to other organisations.

Federal Trade Commission press release

FCC Hits Carriers with Largest Fine for Privacy Violations

The Federal Communications Commission (FCC) has released a Notice of Apparent Liability (NAL) proposing a US$10 million fine against two telecommunications carriers for failing to take reasonable and appropriate security measures to protect the personal information of their subscribers and for exposing their customers to unacceptable risk of identity theft or possible other harm. The NAL is the largest proposed fine the FCC has sought for an alleged privacy violation by a carrier. It is also the first time the FCC has found in its underlying statutory authority a duty of carriers to "employ reasonable data security practices to protect" customers' personal information.

FCC document – Notice of Apparent Liability

FTC Imposes Fine on Leading Privacy Credentialing Provider

The Federal Trade Commission (FTC) has announced a proposed Consent Order with TRUSTe settling allegations that the company had deceived its customers regarding its privacy certification program. Since at least 2006, TRUSTe, based in San Francisco, has offered a privacy credentialing and monitoring service for companies. Participating companies then post TRUSTe's Certified Privacy Seals on their websites. The FTC alleged that, from 2006 to2013, TRUSTe failed to conduct annual re-certifications for all its clients to confirm their compliance with the requirements of TRUSTe's privacy certification program. TRUSTe has agreed to pay a US$200,000 fine and to report annually for ten years to the FTC regarding its privacy certification program.

Agreement containing consent order

Key *Federal Trade Commission v. Wyndham* Data Security Case Goes to Mediation

The New Jersey District Court has stayed and referred to mediation the ongoing action by the Federal Trade Commission (FTC) against Wyndham Hotels. The action relates to alleged improper data security practices as a result of multiple data breaches and lapses in information security that the company and its affiliates suffered from 2008-10. While the mediation could resolve the FTC's specific action against Wyndham, it would leave open some of the broader questions regarding the FTC's authority to regulate data security practices that Wyndham has so vigorously challenged.

FTC v Wyndham case report

Australia

OAIC Publishes Privacy Action Policy

The Office of the Australian Information Commissioner (OAIC) has published its Privacy Regulatory Action Policy. In essence, the policy explains what regulatory powers Australia's Privacy Commissioner has and how he intends to use them. The objective is to ensure transparency on data regulatory matters for organisations handling personal data.

OAIC news – 17 November 2014

OAIC Consults on Regulatory Action Guide

The OAIC has launched a consultation on a proposed Guide to Privacy Regulatory Action. The Guide will support the newly published Privacy Regulatory Action Policy (see above) by providing a more detailed explanation of the Australian Privacy Commissioner's powers and how they will be used, as well as practical guidance for OAIC staff exercising those powers. The consultation seeks the views of stakeholders on whether the Guide is clear in its explanation of the OAIC's approach to the exercise of its regulatory powers.

OAIC consultation information – November 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

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

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

Melodi M. Gates
Denver
T +1 303 894 6111
E melodi.gates@squirepb.com