SQUIRE PATTON BOGGS

Weekly Data Privacy Alert
17 October 2016

UK

ICO Issue Record Fine to TalkTalk

Following the cyber attack on TalkTalk in October 2015, the ICO has issued the telecoms company with a £400,000 fine. The commissioner, under paragraph 44 of the penalty notice, explained that a monetary penalty was appropriate since the breach constituted a serious contravention of the seventh data protection principle and that:

> "The contravention was of a kind likely to cause substantial damage and substantial distress. The Group knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention."

ICO's in-depth investigation

ICO Commissioner's First Speech in Office

The UK ICO Commissioner, Elizabeth Denham, has given her first speech in the role. She stressed the importance of "privacy and innovation" and was careful to assert that the two were not mutually exclusive, while also reminding businesses that ICO would ensure that investigations were "relevant to the public." She also spoke about the GDPR in terms of opportunity and incentive, urging businesses to take the opportunity to "look at things afresh."

Germany

Baden-Württemberg Commissioner Presents Assessments of IoT Products

The Data Protection Authority of Baden-Württemberg has presented the results of an assessment conducted in April 2016 of the privacy policies of more than 300 products relating to the internet of things (IoT). The assessment was part of the initiative GPEN Privacy Sweep 2016 by the Global Privacy Enforcement Network.

The Authority found that the results of its assessment were not dissimilar to those of other assessors. The main issues were cited to be lack of transparency, insufficient user information (in more than 60% of the cases) and insufficiencies in how personal consumer data is stored and deleted. Moreover, many privacy policies did not refer to individual IoT products, but only to the related product line. The Authority announced that it will continue to assess IoT products in Baden-Württemberg and encouraged consumers to make inquiries into the use of their personal data.

The Data Protection Authority of Baden-Württemberg Report (PDF) (in German)

International Company Sues Germany for Remote Signal Monitoring

DE-CIX, an international operator of internet exchanges, has announced that it has filed a lawsuit against the German Federal Ministry of the Interior before the Federal Administrative Court in Leipzig for the practice of "strategic remote signal monitoring" ("*strategische Fernmeldeüberwachung*") by the German Federal Intelligence Service (*Bundesnachrichtendienst*). A legal assessment by a renowned constitutional lawyer has called into question the legality of this practice. The company declared that it considers itself responsible for protecting its clients and ensuring legal security.

DE-CIX questions legality of government tapping its system

US

Yahoo Discloses Data Breach – Questions Follow

On September 22, 2016, Yahoo publicly announced that account information for at least 500 million users was stolen from its network in late 2014. The compromised information included names, email addresses, telephone numbers, birth dates, hashed passwords and security questions and answers. Yahoo believes the attack was perpetrated by a state-sponsored actor, but did not provide further detail as to who that might be. In its announcement, Yahoo assured users that the "stolen information did not include unprotected passwords, payment card data, or bank account information," and that the company is "working closely with law enforcement" to address the matter.

Yahoo has been criticized for the two-year delay in disclosing the breach. On September 27, 2016, six Democratic Senators sent a joint letter to Yahoo CEO Marissa Mayer, demanding more details about the breach and Yahoo's response, including a timeline and an explanation for how "such a large intrusion of Yahoo's systems [could] have gone undetected."

States Take DHS Up on Offer to Provide Election Cybersecurity Help

In light of impending elections and recent politically-focused data breaches blamed on Russian hackers, the US Department of Homeland Security (DHS) has offered to assist state and local election officials in protecting against cyber intrusions implicating voter and election information. In a September 16, 2016 statement, the DHS emphasized that this assistance is "strictly voluntary and does not entail regulation, binding directives, and is not offered to supersede state and local control over the process. The DHS role is limited to support only." Services offered include risk and vulnerability assessments, cyber hygiene scans on internet-facing systems and sharing of best practices. Testifying before the Senate Committee on Homeland Security and Governmental Affairs, DHS Secretary Jeh Johnson testified that as of September 27, 2016, 18 US states had requested election cybersecurity assistance offered by DHS.

Contacts

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

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

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

Philip R. Zender
Partner, San Francisco
T +1 415 393 9827
E philip.zender@squirepb.com