cybersecuritylaw&practice

STRATEGIC ANALYSIS BY DATAGUIDANCE
VOLUME 02 ISSUE 02 FEBRUARY 2016 WWW.E-COMLAW.COM

Cyber plan sees White House appoint a CISO

US President Barack Obama announced on 9 February a Cybersecurity National Action Plan ('CNAP'), which contains actions to *inter alia* empower citizens to improve their cyber security, to foster cooperation between organisations, and to establish a number of bodies and new roles, including a Commission on Enhancing National Cybersecurity to advise on strengthening cyber security and protecting privacy.

"The Commission is designed to increase the number of cyber security personnel in the federal workforce," explains Dr. Jane LeClair, COO of the National Cybersecurity Institute at Excelsior College. "This is necessary as the trend is for individuals to be saddled with too many responsibilities."

A widely-discussed part of the CNAP is the establishment of a Chief Information Security Officer ('CISO') to coordinate federal agencies' work on cyber security. However, Alex Lakatos, Partner at Mayer Brown, notes that "it does not appear there is a budget for the CISO to hire new employees; the CISO will compete with 13 other Office of Management and Budget ('OMB') units for the attention of 170 employees."

IN THIS ISSUE

Report calls for overhaul of draft Investigatory Powers Bill

The Joint Committee released its report on the UK's draft Investigatory Powers Bill on 3 February, which calls for a significant overhaul of the draft Bill and reiterates the call for clarity expressed in the two previous Committee reports.

"Taken together with the Intelligence and Security Committee report and that of the Science and Technology Committee the draft Bill requires a very significant overhaul," said Graham Smith, Partner at Bird & Bird LLP, who provided evidence to the Joint Committee. "In some areas - particularly compelled retention of ICRs [Internet Connection Records] and bulk powers - the Joint Committee has asked the Home Office to provide significantly more evidence to support its case and address concerns of witnesses. The witnesses' concerns on ICRs go to intrusiveness, technical feasibility and clarity. The Home Office faces a formidable, in some respects perhaps impossible, task to address these - at least in the time available before the Bill is due to be introduced in March."

The Joint Committee presented specific concerns on the issue of encryption and the obligation within the draft Bill that telecommunication service providers could be required to remove electronic protection applied to communications or data. The Joint Committee states that it agrees with the intention of the Government's policy to seek access to communications and data when required by a warrant, while not requiring encryption keys to be compromised or backdoors installed, but that the drafting of the Bill should be amended to make this clear. The Joint Committee further stresses that 'The Government still needs to make explicit on the face of the Bill that CSPs offering end-to-end encrypted communication on other un-decryptable communications will not be expected to provide decrypted copies of these communications if it is not practicable [...].'

"The biggest issue for me is ICRs - the criticism from witnesses on the subject was extreme, and well noted in the report, but the report still ended up broadly in favour of them," adds Dr Paul Bernal, Lecturer at the University of East Anglia. "It seems likely that the Bill will continue to include ICRs - which will mean an immense amount of money, effort and expertise will be wasted on something that will not work, will create unnecessary risks and will be a distraction from the kind of work that might actually help do the things that the Investigatory Powers Bill purports to do."

VTech T&C amendments will 'not override DPA obligations'

Blogger Troy Hunt posted on 9 February that VTech Holdings Ltd has updated its T&Cs to extend its limitation of liability; the T&Cs state, 'You acknowledge and agree that any information you send or receive during your use of the site may not be secure and may be intercepted or later acquired by unauthorised parties.'

This follows VTech's admission on 27 November that unauthorised access was gained to customer data from multiple countries housed on one of its app store databases on 14 November. Various data protection authorities, including the Hong Kong Office of the Privacy Commissioner for Personal Data and the Office of the Australian Information Commissioner, then began checks on VTech's compliance with security requirements under their national legislation.

"VTech adding this wording would not override obligations under the UK Data Protection Act ('DPA') to implement technical and organisational measures to keep personal data secure," said Stefano Debolini, Associate at Sheridans. "However, it's worth letting users know there are risks when they send data online which can't necessarily be addressed by a supplier. If someone executes a man-in-the-middle attack, there may be little a service provider can do. If a UK service provider collects personal data, the DPA obligations would apply despite this wording, but T&Cs could be used to warn users about the risks, and assure them that appropriate measures are taken to keep personal data secure once it is received."