cybersecuritylaw&practice

STRATEGIC ANALYSIS BY DATAGUIDANCE
VOLUME 02 ISSUE 04 APRIL 2016 WWW.E-COMLAW.COM

US Senators' encryption bill forces discussion

US Senators Richard Burr, Chairman of the Senate Intelligence Committee, and Diane Feinstein, put forward a discussion draft entitled the 'Compliance with Court Orders Act of 2016' on 7 April 2016, which would require companies served with a court order to provide 'technical assistance' to government investigators when seeking to access encrypted data.

"The draft is the result of increasing commercial use of encryption and its impact on law enforcement, exacerbated by the recent enthusiasm in Silicon Valley for encryption that locks out everyone, including the company that provided it," explains Stewart A. Baker, Partner at Steptoe & Johnson.

Alan S. Tilles, an Attorney at Shulman Rogers, believes that the discussion draft forces the conversation regarding government back door access to personal data stored on mobile devices, which is sorely needed. "What we need to do is strike an appropriate balance between our need to be secure in our personal privacy with our need to be secure from harm. This balance represents one of the most important issues of the 21st century," says Tilles.

IN THIS ISSUE

DoJ secret investigation powers could result in web boundaries

Microsoft filed suit in a US federal court in Seattle on 14 April 2016 against the Department of Justice ('DoJ'), alleging that the DoJ is violating the US Constitution by preventing Microsoft from notifying its customers about government requests to access data stored in the cloud.

Microsoft's suit argues that Section 2705(b) of the Electronic Communications Privacy Act ('ECPA'), which allows US courts to order cloud services providers to withhold notifying customers of government access to their data based on a 'reason to believe' that disclosure may hinder an investigation but which does not require any evidence for such a belief, violates the Fourth Amendment, which affords people and businesses the right to know if the government searches or seizes their property, and the First Amendment, which enshrines Microsoft's rights to talk to its customers and discuss how the government conducts investigations. Microsoft's complaint states that 'People do not give up their rights when they move their private information from physical storage to the cloud' and requests Section 2705(b) be declared unconstitutional.

"The DoJ is not considering the international ramifications of its actions," says Michael Zweiback, Partner at Alston & Bird LLP. "The consequence of all this is that there are going to be countries in the EU that are going to fragment the web and repatriate their data because of unrestrained enforcement activities by the US government."

Microsoft believes that the US government has exploited the transition to cloud computing and the fact that the old statutes did not envisage the developments in digital technology, in order to expand its power to conduct secret investigations.

In regards to the outcome of Microsoft's suit, Zweiback thinks that it has at least raised the issue in Congress that such an over extension of US enforcement powers will have a massive impact on US providers of cloud computing. "The US government needs to be respectful of Europe's concerns about data privacy otherwise we will see the creation of structural boundaries across the web," adds Zweiback. "What I expect the court will do and what needs to happen is that the ECPA should be amended to require that a duration for which a warrant needs to remain under seal is established and an evidentiary demonstration of why the investigation will be impeded if the customer is informed should be required."

IAIS highlights vulnerability of insurance sector to cyber risks

The International Association of Insurance Supervisors ('IAIS') published on 14 April 2016 its Issues Paper on Cyber Risk to the Insurance Sector ('Paper'), which details how the insurance sector is exposed to cyber risk and warns of its vulnerability to cyber incidents.

The Paper draws on a 2015 survey carried out amongst IAIS members *inter alia* on practices and regulatory challenges relating to cyber risk. "A significant concern for the insurance industry is cyber exposures that companies may be held to have assumed under non-cyber policies," says Paul Bantick, UK Focus Group Leader in Technology, Media and Business Services at Beazley. "This is a worry for both clients and insurers. In the absence of affirmative cyber cover, clients cannot be confident that they are insured - there is a high likelihood that insurers will refuse claims that they have not priced into their premiums - and insurers with inadequate exclusionary language may find court decisions going against them."

The Paper outlines the potential impacts of cyber incidents on insurers, which can include reputational damage for instance, and discusses the weaknesses discovered within the sector by regulators, such as concerns over staff user privileges and whether these are adequately controlled.

The IAIS is now seeking public comment on the Paper via an online consultation until 13 May 2016. Following this it aims to produce a finalised paper and proposed resolutions in late June or early July.