MACFARLANES

DATA PROTECTION AND CYBER-CRIME – VIEWS FROM THE HOUSE OF COMMONS

A report commissioned in the wake of the TalkTalk hack in October 2015 by the House of Commons Culture Media and Sport Committee was published earlier this week and made 17 recommendations relating to the protection of data online. The suggestion that CEO compensation should at least be in part linked to effective cyber-security inevitably caught the attention of the media, but the other recommendations are naturally of interest too, providing views on post-event scrutiny and how best to mitigate damage in situations where the profile of the breach might attract Parliamentary attention. Much is made of the inevitability of some form of cyber-attack on businesses large or small, so understanding how a company's actions might be judged by such a committee are helpful indicators for anyone trying to gauge what might be deemed reasonable behaviour. Please note that this is not an analysis of the minimum required standards to escape censure.

- **Board level responsibility** – the Committee was clearly impressed by Baroness Harding's response as CEO to stand up and take charge of the TalkTalk investigation. Interestingly, and despite the general tone of the wider cyber-security debate to try to make the C-suite genuinely accountable, the Committee do not appear to endorse that approach. They suggest that it is right that the CEO should lead the response, but that "*someone able to take full day-to-day responsibility with Board oversight*" should be in charge of cyber-security and sanctioned if the company has not taken sufficient steps to protect itself from a cyber-attack. A helpful indication of a general presumption that Board members need not resign in cases where hitherto calls for such a reaction might have arisen, but pity the executive whose warnings to improve security for the impending attack are not heeded or funded by the Board: all of the accountability and none of the perks. Time for a discussion around additional compensation?

- **Escalating fines** – there is clearly overlap here between the Commons' recommendation that the ICO should be able to fine companies for not including security in their network design, the new EU General Data Protection Regulation (GDPR) requirements for security by design and the new EU regime on fines for data loss. The Committee's recommendation indicates an intention to incentivise companies to look at the threat seriously with the frequency of attacks – anyone not applying security as a criteria for network design will in future be criticised.

- **Claims by customers** – pending the Supreme Court hearing of the *Vidal-Hall v Google* case to clarify the right for customers to sue for personal distress, the Committee expresses the view that it should be easier for customers to sue for compensation. There is however no analysis of the respective role of an ICO fine and a claim by the customer – it is the customer's data, so is it right to both fine the Company and make them pay individuals? Does this loss ultimately fall to insurers? There should certainly be a route for individuals to recover actual financial loss, and the claim cost should be low, but we ought to be wary of opening floodgates given how much personal data is also freely given away to online businesses daily in return for the facility of the internet. Consumers ought not to have it both ways.

- **ICO budget** – as identified in the new GDPR, the UK Government will need to provide adequate resources to the ICO. The Committee noted the paucity of current enforcement resource and invited the ICO to scope its budget as soon as possible so as to enable the UK to meet its regulatory obligation (the UK remaining in the EU being the underlying assumption). It is a good time to be asking for budget in this field.

- **Annual reports to the ICO** – the Committee recommendation that a business should report annually about their cyber-security programmes and procedures would require considerable resource for the ICO to process. The size of the corresponding budget request for resource to process such reporting may well ensure this recommendation is considered with due care, although it makes a good point regarding driving a proactive agenda, rather than only reporting breaches.

The profile of cyber-risk remains necessarily high, having risen with considerable speed up the agenda over the last five years. The coincidence of this with the GDPR is certainly helpful in driving awareness of the immediacy of the threat. Much can still be done to limit exposure to attacks, and much of the Committee's focus is on accelerating the incentives for businesses to protect their assets and reduce the overall cost to the economy. This wider concern is to be welcomed, even if a further debate on the need for a difference in treatment between data which is personal and data which is private, might well relieve some of the greater challenges posed by current data protection law.

CONTACT DETAILS
If you would like further information or specific advice please contact:

RUPERT CASEY
PARTNER
DATA PROTECTION
DD +44 (0)20 7849 2256
rupert.casey@macfarlanes.com

JUNE 2016

MACFARLANES LLP
20 CURSITOR STREET LONDON EC4A 1LT
T +44 (0)20 7831 9222 F +44 (0)20 7831 9607 DX 138 Chancery Lane www.macfarlanes.com

This note is intended to provide general information about some recent and anticipated developments which may be of interest.
It is not intended to be comprehensive nor to provide any specific legal advice and should not be acted or relied upon as doing so. Professional advice appropriate to the specific situation should always be obtained.

Macfarlanes LLP is a limited liability partnership registered in England with number OC334406. Its registered office and principal place of business are at 20 Cursitor Street, London EC4A 1LT.
The firm is not authorised under the Financial Services and Markets Act 2000, but is able in certain circumstances to offer a limited range of investment services to clients because it is authorised and regulated by the Solicitors Regulation Authority.
It can provide these investment services if they are an incidental part of the professional services it has been engaged to provide. © Macfarlanes June 2016