COVID-19: EXPLORING OPPORTUNITIES: WILL YOUR TECHNOLOGY SURVIVE THE OUTBREAK? (GLOBAL)

14 July 2020 | Global
Legal Briefings – By **Julian Lincoln, Partner, Peter Jones, Partner, and David Ryan, Senior Associate**

The effects of the COVID-19 pandemic across the globe continue to evolve on a daily basis. While this pandemic is first a public health and humanitarian crisis, the impacts of COVID-19 on global and national economies, businesses, supply chains, and the everyday lives of the world's population are already significant and anticipated to escalate.

As we continue to emerge from the immediate impacts of COVID-19, a number of solutions and approaches embraced by organisations as initial responses have proved to be catalysts, accelerating changes in human behaviour and speeding up technological advances quicker than anticipated. Equally, it is clear that efforts to recover and refocus business will be required to survive and succeed in the 'new normal'. Accepting the mantra of "never wasting a crisis", business leaders, investors and governments have the opportunity to proactively plan for technology, data and information needs, and assess necessary risks, to ensure the global economy and society can rebound in a rebuilt world. Successful digitisation of business operations can drive enterprise transformation, ushering in a new standard of efficiency, resilience and convenience for the future.

This briefing highlights key practical implications of COVID-19 for all organisations' data and technology environments, which is the first step to planning for the future.

Senior executives and leaders in all businesses must promptly and proactively manage technology, data and information needs, flows and risks across the enterprise, to ensure that these vital elements of the global economy remain functional as the challenges of COVID-19 manifest.

This briefing highlights key practical implications of COVID-19 for all organisations' data and technology environments.

1. NETWORK CAPABILITY

The capability of communications and other networks infrastructure to meet the demands driven by the COVID-19 pandemic are to some extent unknown. Broadband networks are anticipated to experience both increased volume of demand, and, importantly, fundamentally different types of demand, from their normal BAU.

- *How will you assess network capacity in the face of changed network demands and ways of working: can your personnel's home networks support homeworking?*

Material impacts on broadband network functionality may be caused by private households' transition from being primarily consumers of data over broadband networks and largely passive in terms of data production, to potentially being active creators of significant amounts of data (e.g. through video conferencing). Especially in hybrid communications infrastructure environments, the underlying design of many network elements is essentially asymmetrical (allowing for business-sufficient download speeds but providing limited upload capacity), and it may well be that the increased upload demands of remote workforces in a modern data-driven economy cause significant downgrades or loss of performance in these networks.

Furthermore, at a macro level, whilst our national networks are resilient and our telcos have great network optimisation technologies, fundamentally, our networks were not constructed in anticipation of core CBD loads being distributed across suburban networks.

- *Do you and your personnel have the ability to failover to a mobile (e.g. 4G or wireless) connectivity solution if broadband networks suffer capacity issues or fail?*

- *Does your organisation's infrastructure and operating model allow for continued operation at materially reduced network speeds and how will you change processes and operations to accommodate restricted network speeds?*

2. LICENCING CAPACITY

Businesses transitioning rapidly to remote working models may find that their existing licensing environment does not provide sufficient capacity for a substantial part of their workforce to work remotely or for the general licence needs of a distributed technology environment.

- *Technology functions need to move quickly to audit their existing licensing landscape and source necessary licence capacity to meet the changing requirements of their businesses.*

While enterprise infrastructure will often have the capability to support a remote workforce (noting that infrastructure must be assessed and appropriately scaled) businesses are facing a common challenge of insufficiently provisioned VPN, security and other infrastructure licences necessary to meet mass remote working technology needs. The security, application and infrastructure vendor community is working collaboratively to support customers' licensing needs as they respond to COVID-19.

Organisations must also be careful to observe licence / use metrics or limitations, to breaching use restrictions or limitations.

- *Do you need to audit your core technologies enlivened in remote working to ensure contractual compliance with terms, including, location and usage restrictions?*

3. INFORMATION SECURITY

The mass deployment of more open operating models like homeworking inherently impacts organisations' information security risk profile. Personnel and technology vendors accessing systems and data remotely creates risk of technology and network security breaches, data may be stored or processed by local environments that lack enterprise security controls, and personnel may work in shared locations risking disclosure of sensitive or confidential information.

- *Have you assessed where information may be stored or processed as a result of homeworking?*
- *Have you considered what will happen to information stored in personnel's local environments when homeworking ends?*

Organisations must adopt both technology and process measures to manage the risk of information security breach, including by hostile actors. Assessment of the need for delivery of encryption, VPN and firewall technologies to enable homeworking, and adoption of a more aggressive posture of monitoring and responding to cyber threats, are key considerations for technology and risk functions in the context of homeworking deployment.

- *Have you completed a holistic information security risk analysis of homeworking?*

Are you able to deploy or scale up additional security or encryption solutions or channels?

4. BUSINESS CONTINUITY & DISASTER RECOVERY

Businesses' risk, technology and operations functions should assess whether existing business continuity and disaster recovery (BCDR) frameworks are fit for purpose and deployable in an environment where many or all personnel are working remotely and 'normal' on-premise business operations are shut down.

- *Do you know where your key BCDR plans are? Are they current and can they be activated in practice? Now might be a great time to review these plans.*

BCDR plans are often developed on the assumption of localised crises and may not be effective in the context of a trans-national event like COVID-19.

- *Will your planned failover sites be available if a disaster occurs today?*

Technology managers should also asses how remotely working personnel (and a remotely distributed technology environment) will be impacted by a disaster event.

- *Will existing BCDR processes effectively manage business continuity in the context of a largely remote workforce and a remote IT infrastructure environment?*

5. DELIVERING TECHNOLOGY FOR HOMEWORKING

Reliable technologies and access to systems and applications are key enablers of effective homeworking arrangements. Businesses' technology functions need to assess and pivot to meet the particular requirements of a remote working technology environments, which are inherently less standardised and more user-driven than 'traditional' enterprise technology environments.

- *Clearly communicate to homeworking personnel any changes from their 'BAU' technology working environment (e.g. unavailability of certain applications or systems on a remote basis).*
- *Provision and deploy fall-back / failover technology solutions where available: ready availability of workarounds is essential to maintaining operations.*

Provisioning for the needs of 'first-time' standup of homeworking requires careful practical assessment of the requirements of your business and personnel. Be mindful of both internal factors (your ability to support homeworking) and external factors (your personnel's experience with homeworking) when establishing technology arrangements to support homeworking.

- *Do you have the capacity (including in arrangements with your technology services vendors) to provide fit-for-purpose technology helpdesk support to homeworking personnel at required volumes?*

- *Can you remotely deploy application updates and security patches across an enterprise-wide remote access / distributed technology environment?*

- *Have you articulated your organisation's expectations regarding protection of sensitive and confidential information (whether physical or virtual) in homeworking environments?*

The effects of the COVID-19 pandemic on economies and society are evolving rapidly. We are encouraging all organisations to take a proactive posture in preparing for the impacts of COVID-19, and to ensure that their technology environments are on a sufficiently agile footing to respond to iterative and fast-moving changes to enterprise technology needs. While it may not be viable to treat each risk to your business arising from COVID-19, careful and holistic planning will enable leaders to most effectively position their response to the COVID-19 crisis.

More on Navigating the COVID-19 Outbreak

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

JULIAN LINCOLN
PARTNER, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

PETER JONES
PARTNER, SYDNEY
+61 2 9225 5588
peter.jones@hsf.com

DAVID J RYAN
SENIOR ASSOCIATE, MELBOURNE
+61 3 9288 1831
david.j.ryan@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2020

SUBSCRIBE TO STAY UP-TO-DATE WITH LATEST THINKING, BLOGS, EVENTS, AND MORE
Close

© HERBERT SMITH FREEHILLS LLP 2020