HERBERT SMITH FREEHILLS

FUTURE CITIES SERIES: FORGING DATA SECURITY FOR TOMORROW

05 November 2020 | Insight
Legal Briefings – By **Kate Macmillan**

If modern cities have never been more reliant on computers, they've also never been more exposed to cyber threats. Our latest Future Cities commentary asks: what now?

The pandemic has shown us just how dependent society is on computers connected to the internet and the information that is used and stored. This dependence has also increased, with many regarding the pandemic as an accelerator for digitalisation. Yet this time has also highlighted that we are far from where we should be in relation to using computers and information safely and considerations should be given to what we have learned during the pandemic to shape the future landscape.

This article is part of our Future Cities Series where our experts explore the pressures facing our cities in the post-Covid era and map out the key issues and industry themes in re-thinking urban life.

Cyber criminals have had a field day during the pandemic. In the early stages, they took advantage of people's disorientation, thirst for human connection and lack of cyber security awareness. There was a huge spike in phishing – the most common way criminals obtain access to systems – with Google blocking 100m phishing emails, with a "coronavirus" tag as a lure, in a single week. As the pandemic went on the criminals' focus changed to ransomware, causing Interpol to issue a purple notice alerting police in all of its 194 member countries to the heightened threat. The targets of ransomware now include non-traditional sectors such as manufacturing and the traditional financial demands have grown substantially. Many criminals will have gained undetected footholds in organisations, which may cause significant further harms at a later date.

In Germany, we have seen the first legal action in relation to a cyber attack directly causing loss of life as led by prosecutors in Cologne. During a ransomware attack, hackers rendered a hospital's systems inoperable causing a patient scheduled for life saving treatment to be transferred to another hospital 30km away, during which the patient's life was lost. It has been reported that the attackers took advantage of a well-known vulnerability in a piece of virtual private network software.

On top of that, citizens are becoming increasingly concerned about what information is held on them and what it might be used for. There has been widespread and well publicised concern about the privacy and security provisions of some of the most commonly used virtual conferencing platforms. Fear and suspicion regarding what may be done with the information on contact tracing apps has hindered their use in many places. Similarly, public concern is growing around disinformation – with armies of bots picking up and amplifying misleading and inaccurate content in some cases.

Once computers connected to the internet have a greater ability to affect the world in a direct physical manner, it's not difficult to see the vital importance of cyber and data security. The greater the likelihood of harms, the greater care is needed to manage those risks.

At the heart of cybersecurity is the triad of confidentiality, availability and integrity – the cornerstone of any organisation's cyber and data security infrastructure. To understand this in practice, take, for example, a notional embedded medical device with an internet connection that might monitor a heartbeat and, if it detects an irregular heartbeat, shock the heart back to a normal rhythm. In relation to this you might be concerned about the confidentiality issue (someone knowing you have it); even more concerned about the availability threat (someone disabling it) or an integrity threat (someone changing how it works).

As technology develops we will continue to be concerned about confidentiality and are likely to become even more concerned than we are now about availability and integrity. Pre-pandemic we were on a trajectory towards ever increasing use of computers and data. A future of high speed wireless connectivity; an internet of things – "smart" everything collecting, using and communicating data; autonomous algorithms; machine learning and artificial intelligence; cloud computing and robotics.

The pandemic has offered an opportunity to consider carefully the structures we need to give us the digital world we want: to take advantage of all the benefits cyber and data offer whilst preserving human life and values.

The law is playing an important role in helping us prepare for, and adapt to, the future. Recognising that digitalisation and cybersecurity are two sides of the same coin, countries are introducing a raft of laws aimed at boosting their overall level of cyber security and data protection. Take the NIS Regulations (the Security of Network and Information Systems Regulations), for example, which are aimed at boosting the overall level of cyber and physical resilience. In the first instance these are aimed at network and information systems for the provision of essential services and digital services but may be extended to apply to a greater number of sectors. Citizens are using class actions brought under the General Data Protection Regulation – the most lobbied piece of EU legislation we've ever had and regarded by many as a powerful piece of human rights law – to stand up to surveillance and data misuse by states and businesses alike. Campaigns for accountability and responsible technology are attracting greater traction than they have before. The minds of some of our most talented lawyers are applying themselves to the future. Take Lord Sales of the UK Supreme Court's thoughts on how to create structures to "reaffirm human agency at the individual level and at the collective democratic level" in his brilliant lecture on "Algorithms, AI and the Law."

The pandemic has shown that change is part of life – and that it comes often at a pace which we do not expect and which may feel uncomfortable. Change is not to be resisted. As Darwin reminds us: "It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change". Many have expressed regret that we did not conduct a risk/benefit analysis in relation to the use of the internet in its infancy. A useful way to view this period is as a prompt to take a hard look at the trajectory of change we're upon and to ensure it leads us to a cyber and data future we like.

RELATED TOPICS

Data and privacy
Emerging Technologies

FEATURED INSIGHTS

FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

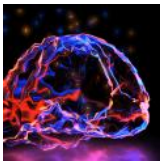
BROWSE BY:

- TECH, DIGITAL & DATA

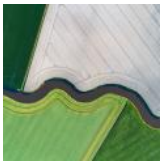
- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

RELATED ARTICLES



COMPUTER SAYS NO – WILL FAIRNESS SURVIVE IN THE AGE OF AI?



Preparing for CBAM – The EU extends carbon policies despite trade tensions

Global M&A Outlook 2023: Headwinds, tailwinds and fog

KEY CONTACTS

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

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

REBEKAH GAY
PARTNER AND JOINT GLOBAL HEAD OF INTELLECTUAL PROPERTY, SYDNEY
+61 2 9225 5242
Rebekah.Gay@hsf.com

MARK ROBINSON
PARTNER, GLOBAL CO-HEAD OF TMT SECTOR, SINGAPORE
+65 68689808
Mark.Robinson@hsf.com

KATE MACMILLAN
CONSULTANT, LONDON
+44 20 7466 3737
kate.macmillan@hsf.com