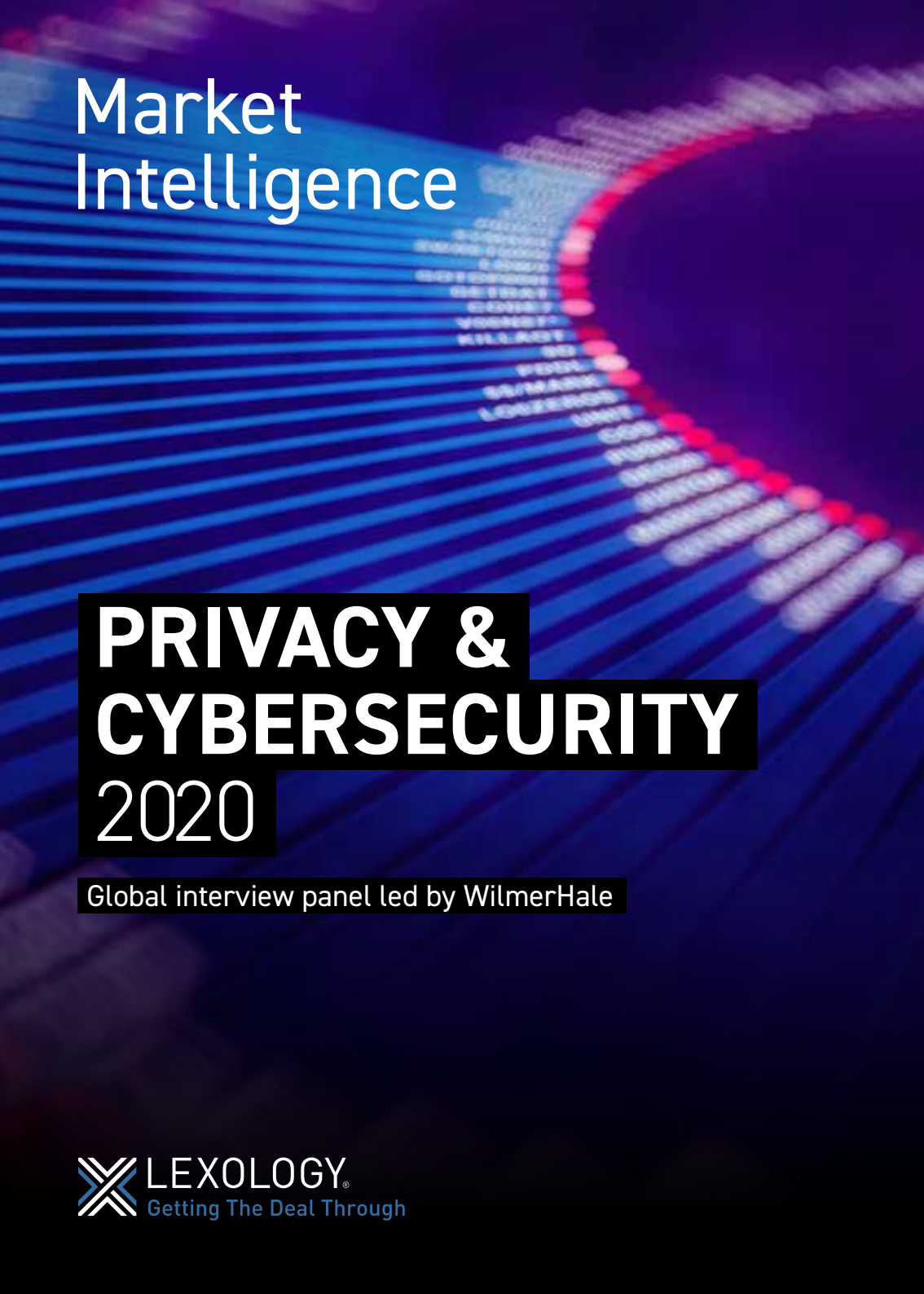


Market Intelligence

PRIVACY & CYBERSECURITY 2020

Global interview panel led by WilmerHale

LEXOLOGY®
Getting The Deal Through

LEXOLOGY
Getting The Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

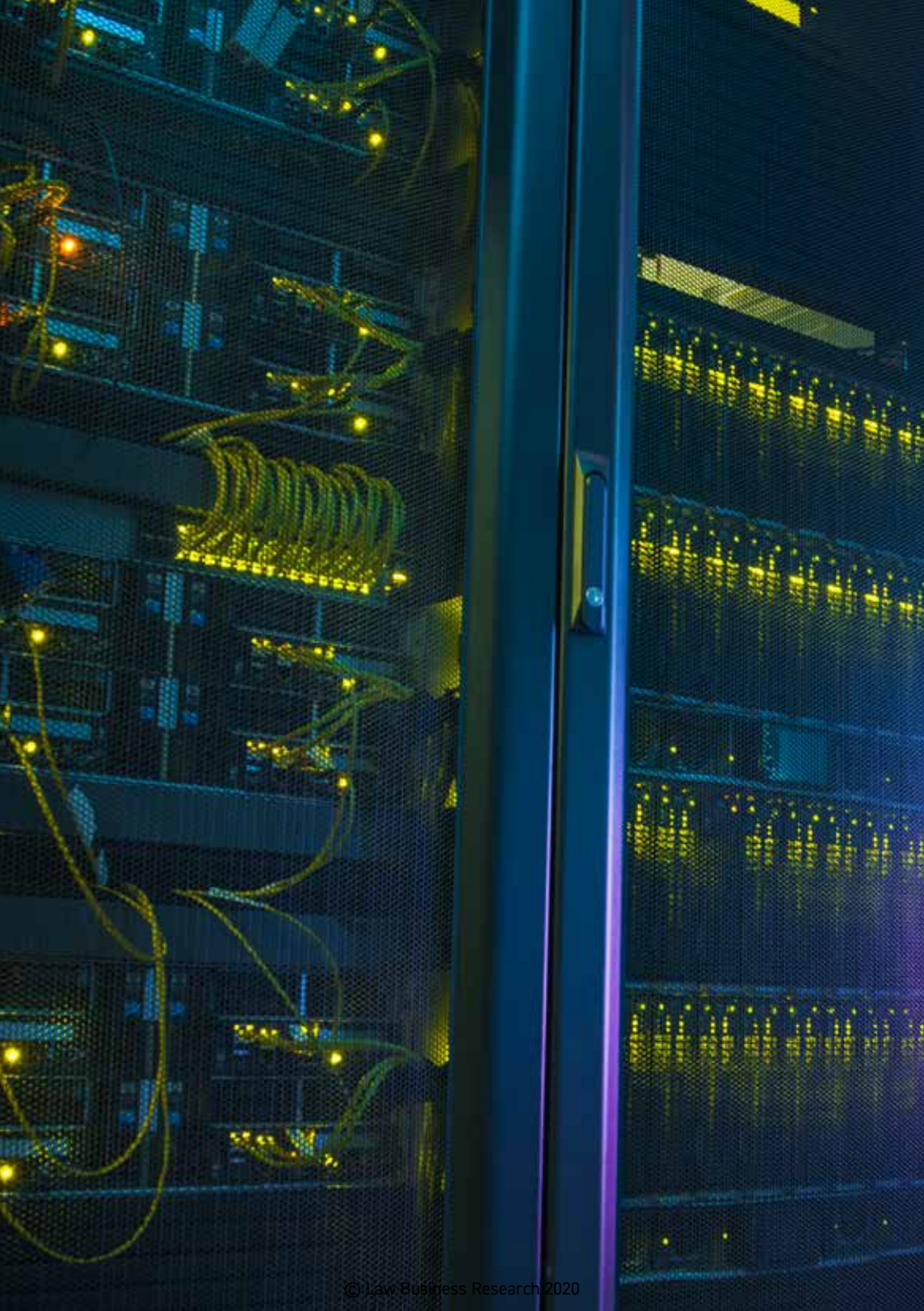
Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Cover photo: shutterstock.com/g/handmadefont

ISBN: 978-1-83862-419-4

Printed and distributed by Encompass Print Solutions

Privacy & Cybersecurity 2020



Global Trends

WilmerHale partner Jason Chipman advises companies on complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States and related export controls. He has assisted companies in nearly every sector of the economy on data security best practices and incident response and is frequently asked to assist with corporate due diligence for transactions involving complex data security and privacy issues. Mr Chipman currently serves as a non-resident fellow at the National Security Institute.

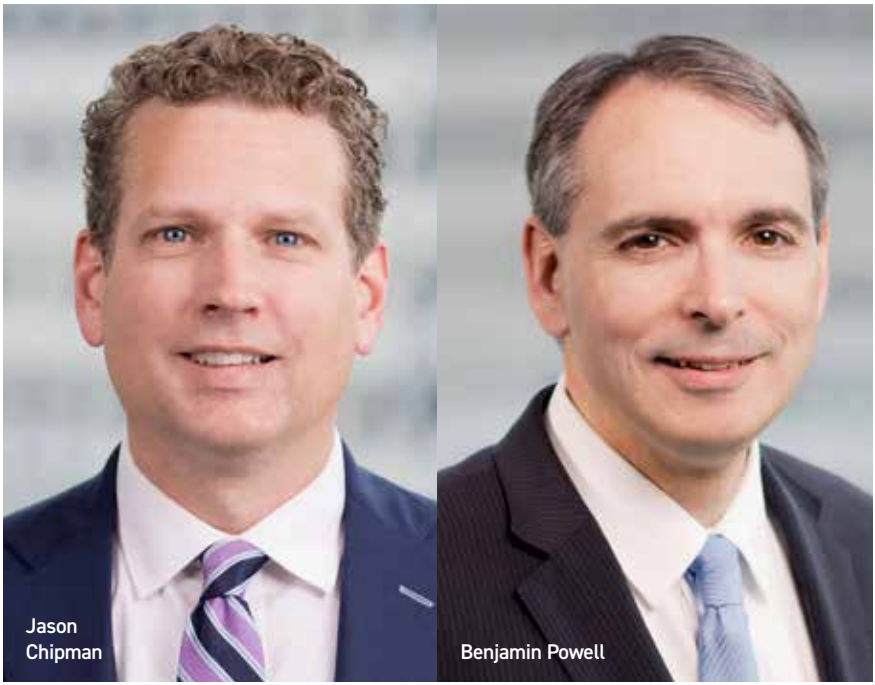
WilmerHale partner Benjamin Powell has advised companies on major cybersecurity incidents and incident preparedness across virtually every sector of the economy, including the banking, investment management, software, retail, energy, defence and intelligence, media and entertainment, pharmaceutical, cloud services, and government contracting. He is recognised as a leading attorney in handling complex regulatory matters relating to international investment and mergers, including matters involving the Committee on Foreign Investment in the United States and the Defense Security Service.

Photo: shutterstock.com/g/regissercom

Cybersecurity continues to represent a growing risk for companies around the world, with cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and 'hacktivists' continuing to grow on a global basis. The covid-19 pandemic has made this trend particularly acute as businesses around the globe work to navigate a more distributed work force and, potentially, more vectors for cyberattacks. In the United States, the Federal Bureau of Investigation warned in 2020 of spikes in 'business email compromises', where hackers target financial systems (eg, procurement departments and bank wire instructions). At the same time, destructive cyberattacks, disruptive ransomware impacting corporate information systems and traditional malware attacks continue to threaten company networks. Governments in Europe, Asia and North America have been responding to these trends, with particular focus on privacy or security controls for companies possessing large amounts of personal information. In this environment, maintaining an effective corporate cybersecurity programme is the standard expectation for all businesses, and the ability to respond efficiently and effectively to data security emergencies will be important for avoiding potentially disruptive cybersecurity incidents in the future.

Jurisdictions around the world continue to create and refine regulatory requirements for businesses identified as possessing important data meriting special protections. In the United States, while data security continues to be handled through sector-specific regulations, there is a growing push to create national privacy legislation potentially similar in scope to the General Data Protection Regulation (GDPR) in Europe. At the same time, US states are taking action of their own. More than 10 states in the United States are exploring the creation of new privacy rules that would include basic data safeguarding requirements. This trend is most notable with regard to the California Consumer Privacy Act, which went into effect in 2020 and includes new privacy controls to obtain consent for use of data, to secure personal data and to maintain the ability to delete data upon request. This means that companies operating in the United States face a patchwork of state and federal regulatory requirements that may impact their data security obligations with trends moving toward a GDPR-like model for data security controls. State attorney- generals in the United States continue to devote substantial resources to policing private-sector data breach notification compliance. At the federal level, data security regulatory requirements are most onerous for specific economic sectors believed to possess higher-risk data, such as federal government defence contractors, banks and healthcare companies. The National Institute of Standards and Technology recently issued new guidance for security controls applicable to companies that possess sensitive US defence information.

In Europe, concern about covid-related cybersecurity threats is also high in 2020, with guidance from EU regulators to companies about the need for particular



vigilance with regard to health-sector data and systems. EU regulators have also placed particular attention in recent months on the handling of data related to the covid-19 pandemic, calling for uniform approaches to the use of mobile apps and similar technologies to track infections. At the same time, companies in the EU continue to grapple with compliance with the 2018 Network and Information Security Directive (NIS Directive) and the GDPR, both of which introduced major data security regulatory changes for certain companies operating in the EU, which triggered a wave of corporate activity to update privacy policies and put in place appropriate compliance controls. The NIS Directive established a set of data security requirements applicable to companies operating critical infrastructure and certain digital content providers. In particular, the NIS Directive required covered companies to provide regulators with data breach notification any time an incident impacts the continuity of their ability to provide essential services irrespective of whether personal data is compromised as a result of the incident. The GDPR, by contrast, focuses on protections for personal data and establishes specific rules for collecting, storing and processing personal information, and also mandates data breach notification to regulators (within 72 hours if feasible) when personal information is compromised. GDPR

"Changing and expanding cybersecurity standards will continue to complicate company network security operations."

has also simplified data breach notice in Europe for some companies by creating a system that allows organisations to provide notice to the data protection authority of their controller jurisdiction.

In China, the government issued in March 2020 new personal information security requirements. The new rules are ostensibly voluntary but it is likely that Chinese regulators will expect companies operating in China to comply with the requirements, which include new rules allowing individuals to have control over how their personal information is used and rules on protecting personal information obtained by companies. The new Chinese standards implement portions of the 2017 China Cybersecurity Law, which largely creates rules similar to the GDPR, such as standards for collecting, storing and handling personal data, mandate user consent for data processing and limit 'secondary uses' of certain personal data. Similar to action in Europe, these reforms have ushered in a new focus on compliance and new breach reporting obligations that are changing the ways international companies deal with data security incidents.

It appears likely that data security requirements will continue to expand globally in the near term. For international companies, changing and expanding cybersecurity standards will continue to complicate company network security operations, with special handling rules applying to the hosting and processing of sensitive data, such as personal data about consumers, critical infrastructure and financial-sector data. Cybersecurity will remain a major issue for such organisations and will continue to require technical, legal and communications experts to work together to manage the risk of data security incidents.

Jason Chipman
jason.chipman@wilmerhale.com

Benjamin Powell
benjamin.powell@wilmerhale.com

Wilmerhale
Washington, DC
www.wilmerhale.com

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this *Privacy & Cybersecurity* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Covid-19 response
M&A risks
Latest regulatory trends
Cloud hosting

an LBR business

ISBN 978-1-83862-419-4