IN
INTERNATIONAL NEWS

ISSUE 2 2020

GLOBAL PRIVACY & CYBERSECURITY

READ MORE

WHISTLEBLOWER PROTECTION
NON-COMPETE PROVISIONS
MATERIAL ADVERSE EFFECT CLAUSES
DISTRESSED COMPANIES

McDermott
Will & Emery

INTERNATIONAL NEWS

EDITOR
Andrea Hamilton
Partner
Brussels
+32 2 282 35 15
ahamilton@mwe.com

IN THIS ISSUE

As we move into the next phase of the Coronavirus (COVID-19) pandemic, the test, track and trace approach being adopted by governments is generating myriad data privacy concerns. Added to this are the challenges created by new privacy laws in California, the end of the Brexit transition period, and the recent judgement in Schrems II that affects the US Privacy Shield mechanism. There has never been a more pressing need for robust global privacy and cybersecurity advice.

Although the pandemic continues to impact global business, creative thinkers are identifying solutions to economic distress and are examining the viability of material adverse effect clauses in their markets. And, of course, developments unrelated to the pandemic, such as the forthcoming EU Whistleblower Directive and the Federal Trade Commission's focus on non-compete provisions in transaction agreements, continue to challenge companies.

Please contact me if you have any comments on our articles or would like to discuss any of the issues raised.

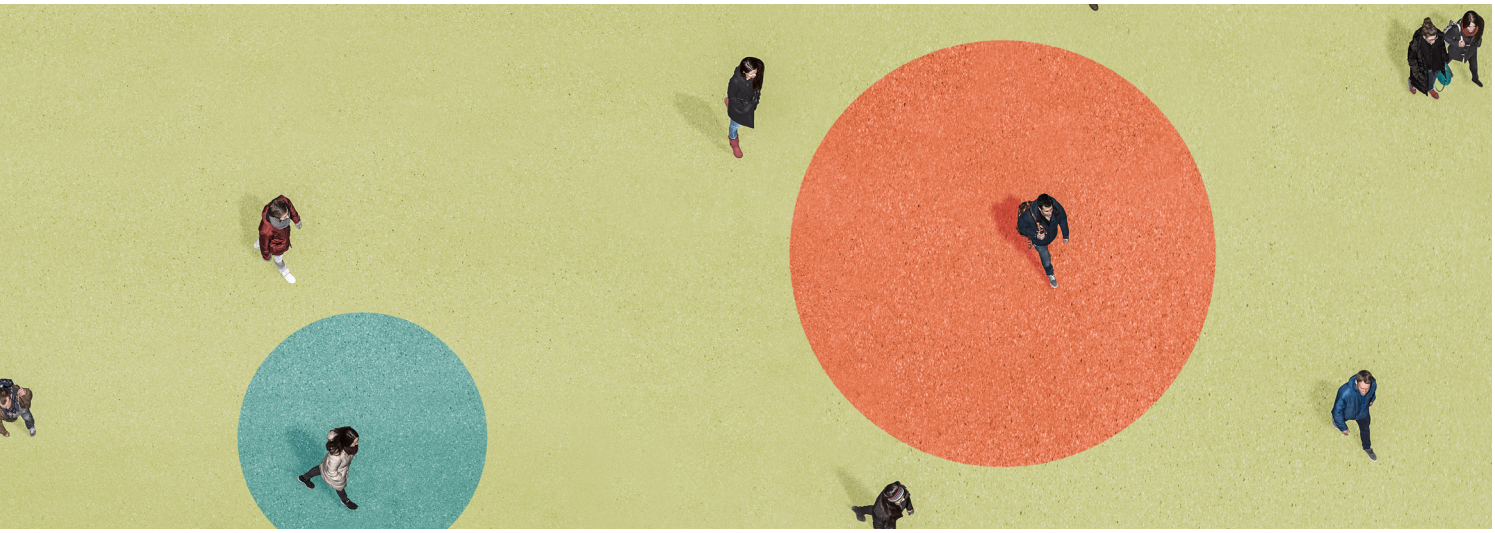
PUBLICATION EDITORS
Aileen Devlin
Kate Hinze

CREATIVE SERVICES
Elliot James Pence

TABLE OF CONTENTS

PRIVACY CONSIDERATIONS FOR COVID-19 DIGITAL CONTACT TRACING

Laura E. Jehl and Deepali Doddi



Contact tracing is a key tool in the global effort to mitigate the spread of Coronavirus (COVID-19). Digital contact tracing, however, presents significant data privacy risks.

Generally, contract tracing refers to an effort by public health officials to identify individuals with whom a patient who has tested positive for an infectious disease has been in close proximity. Public health officials will inform these individuals that they were exposed to a contagious patient and encourage them to monitor their symptoms and quarantine for a period of time.

In response to COVID-19, governments around the world have explored using digital contact tracing, by which smartphone users download an application (app) to enable public health officials to track infected individuals' contacts. In addition, private sector companies are exploring how digital technologies can be used for contact tracing on employees as they re-enter the workplace.

TYPES OF GOVERNMENT DIGITAL CONTACT TRACING

From a data privacy perspective, the most intrusive digital contact tracing has involved government surveillance of users' movements and locations. For instance, the Chinese Government has assigned mandatory, colour-coded quick response (QR) codes to residents based on whether they self-report having COVID-19 symptoms, or coming into contact with confirmed or suspected cases in the last two weeks.

Residents who are assigned red QR codes are required to quarantine for 14 days, while those who receive green QR codes may move freely about their cities, as long as they scan their smartphone apps before gaining entry to public spaces, such as the subway, retail stores, places of employment and restaurants. If a resident is later confirmed to have COVID-19, public health authorities can use the scanned QR code data to identify all individuals who have come into contact with the infected resident.

Other governments have used smartphone geolocation data not only to facilitate contact tracing, but also to enforce quarantine orders. Hong Kong, for example,

has required all visitors to self-quarantine for two weeks upon arrival, and to wear an electronic wristband linked to a smartphone app that relays their geographic coordinates to public health officials to alert them of any violations of quarantine.

Consumer trust is critical for adoption by a sufficient number of users.

Other governments have elected to use geolocation data in their digital contact tracing efforts, but have made the sharing of such data with government officials voluntary. New Zealand has encouraged residents to download the NZ COVID Tracer, a smartphone app that they can use to scan government QR code posters to "check in" at sites and create "digital diaries" of their daily movements, which are stored locally on users' smartphones. If a user checks in at a site visited by an individual with a confirmed or suspected case of COVID-19, the user will receive a notification alert and a call from public health officials. The user may then voluntarily send their entire digital diary to public health officials for contact tracing purposes.

Other, less privacy-intrusive methods of contact tracing do not involve government collection or monitoring of location information at all. Several US states are piloting a digital contact tracing system that relies on Bluetooth technology, whereby app users' smartphones exchange and record random Bluetooth keys transmitted by beacons when the users are in close proximity to one another. An infected user may voluntarily input a positive diagnosis into the app, which will then use the list of Bluetooth keys that were associated with the infected user to identify and notify others with whom the user's smartphone had been in proximity.

Similarly, Singapore has created an app and wearable device to collect, encrypt and locally store Bluetooth proximity data on individuals' devices, rather than in a centralised government database. The app enables users to voluntarily inform public health officials if they test positive for COVID-19. There have been concerns, however, that using Bluetooth technology does not generate results that are as accurate as those derived from precise geolocation data.

Some apps that collect neither geolocation nor Bluetooth data are being used by public health officials to supplement manual contact tracing. The US state of Georgia, for instance, is piloting an app that allows users to voluntarily submit information about their COVID-19 diagnoses and contacts, which government tracers can use as a starting point.

DATA PRIVACY IMPLICATIONS OF DIGITAL CONTACT TRACING

The data privacy implications of digital contact tracing are significant, as many methods involve the collection of both sensitive health and location information.

Transparency

The success of many digital contact tracing initiatives instituted by western governments depends on users' willingness to participate. Consumer trust is critical for adoption by a sufficient number of users to render a contact tracing app effective. It is imperative that there is transparency regarding the types of information an app will collect, how long it will store such information, and the third parties who will have access to the information. Government agencies and private entities offering contact tracing apps should ensure that individuals receive adequate notice of their privacy and data security practices.

Centralisation v Decentralisation

Under a centralised approach to contact tracing, all Bluetooth, geolocation and diagnosis information is compiled in a central system. This is generally run by a public health authority but, in some cases, may be shared with or administered by a third-party technology provider.

Under a decentralised approach, however, geolocation or Bluetooth data is stored locally on users' smartphones, unless the users decide to voluntarily transmit the information to the government agency or private company. The app enables each user's smartphone to regularly check the locally stored data against a list of infected individuals' anonymised identifiers to determine whether or not the user's phone has recently been in proximity with an infected individual's phone.

A decentralised approach may be more palatable for users from a privacy standpoint, because sensitive personal information is likely less susceptible to a cyber attack, unauthorised access or improper surveillance than if it was stored in a centralised repository. However, a centralised approach allows public health officials to monitor and promptly respond to all incoming information, which may make it a more effective contact tracing tool.

CONTINUED ▸

Data Minimisation

"Data minimisation" refers to the core data privacy tenet that an entity should neither collect nor maintain more information about an individual than is necessary to accomplish the purpose for which it is being collected. A contact tracing app that continues to collect users' geolocation information in the post-pandemic era, for example, would run afoul of this principle.

A decentralised approach may be more palatable for users from a privacy standpoint.

To comply with it, government agencies and companies should cease collecting app users' information and delete any stored contact tracing information once it is no longer needed for COVID-19 mitigation efforts, to comply with legal requirements, or for another appropriate purpose.

Bluetooth Data Linkage Issues

Bluetooth-based contact tracing apps typically collect only a random Bluetooth identifier from a COVID-19-positive user who inputs his or her diagnosis. It may, however, be possible for a government agency or private company to link metadata associated with the infected user's Bluetooth identifier, such as the user's smartphone IP address, to the user's identity and location.

Workplace Surveillance

Companies seeking to use digital contact tracing in the workplace may encounter barriers in the form of employee surveillance laws. Because contact tracing apps may track an employee's physical location not only when onsite, but also when the employee is off-duty, the app may be considered a form of surveillance that may be regulated by employment or data protection laws.

Efforts to Regulate Digital Contact Tracing

In the United States, federal lawmakers have introduced several bills intended to protect the privacy of COVID-19 personal data. Senate Republicans have proposed the COVID-19 Consumer Data Protection Act, which would impose notice and consent requirements on regulated entities that collect geolocation data, proximity data, and health information related to COVID-19 under certain circumstances. Senate Democrats have proposed a bill to create a Coronavirus Containment Corps, which would require the US Centers for Disease Control and Prevention to collaborate with state and local governments to develop a national contact tracing strategy that ensures privacy protections for COVID-19 patients. At the time of going to press, neither bill has advanced beyond these proposals.

European privacy regulators have also issued guidance on privacy considerations and risks associated with contact tracing. For example, the UK Information Commissioner's Office published guidance on "data protection expectations" for COVID-19 contact tracing app development, emphasising principles of transparency, data minimisation, and the use of pseudonsmised identifiers when possible. Likewise, the French Commission nationale de l'informatique et des libertés issued an emergency opinion on the French Government's implementation of a national contact tracing app, including recommendations for enhancing users' privacy protections.

LAURA E. JEHL
Global head of the Privacy and Cybersecurity Practice
Washington, DC
ljehl@mwe.com

DEEPALI DODDI
Associate
Chicago
ddoddi@mwe.com

THE UNCERTAIN "STATE" OF US DATA PROTECTION LAW: CALIFORNIA LEADS THE WAY

Laura E. Jehl and Austin Mooney

When it comes to US data protection law, all eyes are on California.

The California Consumer Privacy Act of 2018 (CCPA), which took effect this year, introduced a complicated data protection framework for the personal information of California residents, imposing a variety of new obligations on affected businesses. Although the interpretation of many of the CCPA's provisions remains unsettled—and proposed regulations are still pending—the CCPA's original architects have already advanced another proposed law, the California Privacy Rights Act (CPRA), which will be decided in a statewide referendum this November. If enacted, the CPRA would substantially amend the CCPA, granting consumers additional rights and imposing further liability on businesses.

Whether or not it passes, the proposed CPRA highlights the fluid state of the US legal environment for data protection, which has left businesses around the world struggling to account for the uncertain risks and compliance costs posed by these developments.

It did not have to be this way. The developments in California are due in part to the failure of the US Congress to enact comprehensive federal data protection legislation. Despite widespread support, compromise on a federal standard remains elusive, with legislators unable to agree on critical questions, such as whether or not the law will pre-empt state laws like the CCPA.

CCPA: ORIGINS AND OVERVIEW

The CCPA originated as a state "ballot initiative," a type of referendum that is uniquely powerful in California. After negotiations with the California legislature, the initiative's sponsors withdrew the initiative from the 2018 ballot in exchange for the enactment of a slightly watered-down version of the CCPA through the standard legislative process.

As enacted, the CCPA applies to the broadly-defined "personal information" of California residents, granting individuals various rights with respect to businesses that process their information. Businesses that process California personal information and either exceed US$25 million in annual revenue, process

CONTINUED ▸

the data of more than 50,000 consumers per year, or generate 50% of their revenues from data sales, are subject to the law. Because a business need satisfy only one of these thresholds to be covered by the CCPA, the law applies to a wide range of companies, including many that have only a handful of California customers or otherwise incidentally process the personal information of California residents. Notably, businesses need not have a physical presence in California—or even in the United States—to be subject to the CCPA.

The CPRA would modify the definition of "sale" to explicitly encompass digital advertising.

Perhaps the most interesting right under the CCPA is the right of consumers to opt-out of "sales" of personal information. Whether or not a data transfer amounts to a "sale," as defined by the CCPA, depends on a number of factors, including the purpose of the transfer, whether or not any "value" was provided in exchange, the contract terms, and how the data is ultimately used. The applicability of these provisions remains hotly contested, especially in data-centric industries such as digital advertising. Many companies have opted to take risk-based positions while waiting for the meaning of these provisions to be clarified.

In addition to the CCPA's privacy rights, which are enforceable only by the California Attorney General (AG), the CCPA grants California residents a private right of action to sue companies whose unreasonable security practices lead to a data breach. This right only extends to breaches of certain sensitive categories of personal information, such as financial account information. Impacted individuals can obtain guaranteed statutory damages of US$100 to US$750 per person, a fact that has already resulted in a surge of class action lawsuits following the law's entry into force in January 2020.

The AG is also responsible for issuing regulations. The proposed final regulations would clarify a number of procedural and substantive ambiguities in the CCPA's text and impose additional recordkeeping and procedural requirements on businesses. At the time of publication, however, the final regulations are still pending administrative approval and are unlikely to take effect until October 2020 or later, adding to the compliance uncertainties that businesses face.

THE CPRA JOINS THE FRAY

Without doubt, the CCPA's impact is large. By the state of California's own estimates, compliance costs alone will exceed US$50 billion for covered businesses. Dozens of amendments have been carefully considered by California legislators; in drafting the CCPA regulations, the AG produced over 500 pages of analysis.

Despite this effort, the proposed CPRA would substantially amend the CCPA.

The proposed changes are numerous. As one example, the CPRA would create a right for California consumers to "limit" the processing of "sensitive personal information," which is a new subcategory of personal information that combines and builds on existing "sensitive data" categories under US and EU law. While the steps companies would take to comply with such requests would be similar to the obligations they face under the CCPA in relation to consumer requests to opt out of the "sale" of their data, the applicability of this right is potentially far broader, and many companies that do not "sell" personal information under the current law would have to substantially revise their data practices to comply with the CPRA. Further, the law would modify the definition of "sale" to explicitly encompass digital advertising, with significant implications for the vast majority of websites.

Unlike the ballot initiative behind the CCPA, which was ultimately withdrawn, advocates have given no indication that a legislative compromise will be reached for the CPRA. Early signs point to widespread support for the initiative, which will be voted on in November. If passed, most of the provisions would not take effect until 2023, but preparations for many businesses would need to begin immediately.

FEDERAL LEGISLATION REMAINS STALLED

The surge in data protection law in California can be attributed in large part to the ballot initiative process and the efforts of a group of well-funded advocates. These developments can, however, also be partly attributed to the failure of the US Congress to pass even baseline federal data protection legislation, leaving the states to respond to heightened public support for privacy regulation on their own.

Without doubt, the CCPA's impact is large.

Congress has the power to pass laws regulating data protection throughout the entire country and, if it wishes, to pre-empt state laws such as the CCPA. A federal standard is supported by members of both political parties, business interests, and privacy advocates alike, and various stakeholders have proposed legislation that would establish such a standard.

Despite this widespread agreement on the need for a federal law, little consensus has emerged on the details. Proponents have split along two primary fault lines: the mechanisms for enforcement, and the scope of state pre-emption. Democratic politicians and privacy advocates have tended to support strong enforcement, including private rights of action and minimal pre-emptive effect, allowing more-restrictive state laws like the CCPA to remain in force. Republicans and business interests, on the other hand, have generally advocated against private enforcement and in support of wide-reaching pre-emption.

Adding to the impasse, other issues that intersect with online privacy, such as the moderation of social media content, have given rise to sharply partisan debates, threatening the viability of any bipartisan efforts to reach a compromise, especially in a Presidential election year.

Accordingly, while a US federal data protection law is possible in the coming years, it is not likely to happen anytime soon and, even if passed, its potential impact on state laws like the CCPA is unclear. For the foreseeable future, then, businesses that collect or process California data will need to grapple with the moving target of California law.

For more information, visit McDermott's CCPA Resource center at www.mwe.com/ccpa.

LAURA E. JEHL
Global head of the Privacy and Cybersecurity Practice
Washington, DC
ljehl@mwe.com

AUSTIN MOONEY
Associate
Washington, DC
amooney@mwe.com

DATA PROTECTION DURING AND AFTER THE PANDEMIC: CONSOLIDATE, UPDATE AND INNOVATE

Ashley Winton and Sophie Wood

With part of the workforce now returning to the office, and part of the workforce remaining at home, this is the perfect time to revisit data protection compliance strategy.

Having adapted products, processes, services, facilities and IT systems in response to Coronavirus (COVID-19), businesses should now refocus on their legal and business fundamentals as they move towards returning to the office. Compliance policies should be updated, Brexit contingency plans reinvigorated, and upcoming legal and regulatory changes anticipated.

While taking these steps, businesses should bear in mind a number of key data protection and IT/cybersecurity fundamentals, and take the opportunities afforded by the return to work period to kick-start new initiatives.

PROMOTE RECORD KEEPING AND ACCOUNTABILITY

Two key components of the General Data Protection Regulation (GDPR) are record keeping and data protection impact assessments (DPIAs).

In any investigation, the relevant Data Protection Authority will first want to see comprehensive records. Whilst many of the Data Protection Authorities permitted a lower standard of data protection compliance during the COVID-19 pandemic, along with a regime of reduced enforcement, this will not be considered an excuse for a lack of record keeping.

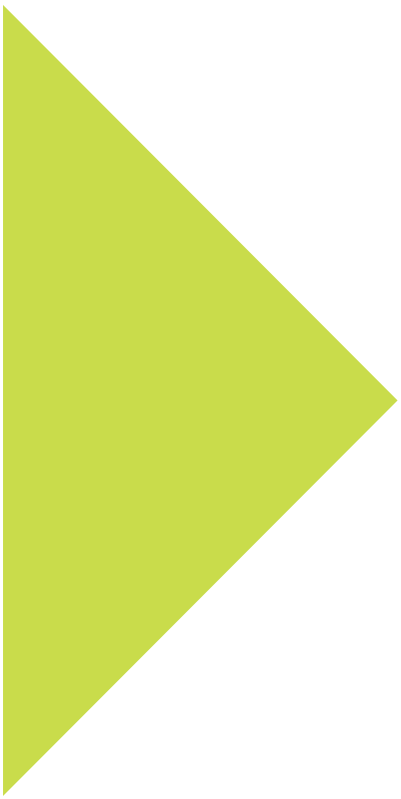
Even if a company has been enjoying a lower level of data protection compliance as a result of COVID-19, it will still need to justify that lower level. A DPIA is a great tool for helping to determine and to document that lower standard of compliance. Its inherent process of record keeping allows a company to effectively track the areas of relaxed compliance so that they can be pulled back up to an acceptable standard post-pandemic.

As a note of caution, however, although regulators have adopted a lower data compliance standard, a court may not adopt a similar approach in any privacy law suit against the company. In this situation, a DPIA would provide helpful evidence to show that due consideration was given to the company's responsibilities and to data subject's rights.

The relevant Data Protection Authority will first want to see comprehensive records.

UPDATE DATA PROTECTION NOTICES AND POLICIES

Data protection notices and policies should be reviewed regularly to ensure continuing compliance with laws and evolving regulatory guidance. Since the entry into force of the GDPR, a substantial amount of regulatory guidance concerning the pandemic and remote working has been released at both EU and Member State levels. With the change in work practices resulting from the pandemic, many data protection notices and polices should now be updated.



ENSURE COMPLIANCE OF INTERNATIONAL DATA TRANSFER STRATEGIES (EU-UK DATA FLOWS)

In the absence of an EU Commission adequacy decision, after the end of the Brexit transition period, on 31 December 2020, businesses must ensure that all EU-UK data flows continue to comply with applicable data protection requirements.

A strategy will be needed, in both the short and long term, to manage international data flows. Business should consider whether or not standard contractual clauses offer sufficient coverage in the long term, or whether binding corporate rules would offer the most robust long-term solution. Now is a good time to get ahead of this issue.

See page 11 for an overview of the additional impact that Schrems II will have on international data transfers.

BEWARE AN INCREASE IN SOCIAL ENGINEERING, RANSOMWARE AND OTHER ACTIVITIES

The COVID-19 pandemic brought with it an expected flood of increased hacking activity. With employees moving to remote working, there are now many more ways in which hackers can gain access to company systems. These range from an increase in phishing emails on COVID-19 related topics, fake approaches by the firm's IT "help desk", third party "support" to help fix home internet or router problems, or technical exploits arising from insecure home WiFi or routers.

A DPIA would provide helpful evidence.

Businesses should determine whether or not their IT security policy suites appropriately cover continuing remote working. Typically, it may be necessary to update remote working policies and "bring your own device" policies, and to make adjustments to breach response policies. Companies should also explore whether or not heightened IT system monitoring could be enabled for employees working from home. All these steps will require the updating of appropriate policies and notices.

CONTINUED ▸

UPDATE CYBER INCIDENCE RESPONSE PLANS

This greater likelihood of breaches means that it is important to have in place an effective cyber incidence or breach response plan. These plans should be adapted to take into account increased remote working and the need for remote detection.

Third parties who will assist in the response, such as cyber investigators, Payment Card Industry Forensic Investigators, lawyers, insurers and PR companies should be identified and retained in such a way that they can get to work quickly. Timescales for data breach reporting to regulators and affected individuals should be understood and taken into consideration, as this can now be as low as four hours for companies subject to the Payment Services Directive No. 2.

Finally, with the greater likelihood of follow-on class actions or other litigation, care should be taken that the correct rules are followed with regard to document preservation and legal and litigation privilege, so that certain reports can be protected from disclosure to third parties.

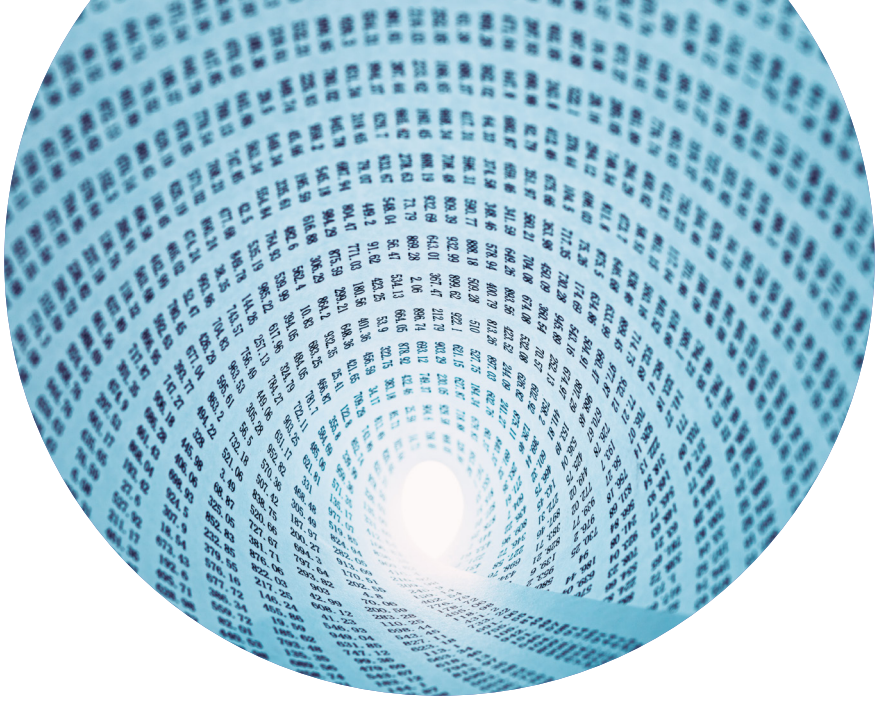
REVIEW THIRD-PARTY COMMERCIAL CONTRACTS

Businesses should review IT supply and IT outsourcing agreements to ensure that these contain the mandatory language prescribed by Article 28 GDPR. Failure to include this language amounts to a breach of the GDPR and exposes businesses to unnecessary commercial risk.

Brexit will also have an impact on IT agreements. To mitigate risk, companies should review indemnities providing protection for high-risk IT liabilities, such as GDPR, to ensure they are effective for both UK and EU GDPR risks.

ASHLEY WINTON
Partner
London
awinton@mwe.com

SOPHIE WOOD
Associate
London
smwood@mwe.com



DOUBLE TROUBLE FOR DATA TRANSFERS POST-BREXIT AND POST-SCHREMS II?

Ashley Winton and Dr. Laura Scaife

The recent landmark Court of Justice for the European Union (CJEU) case C-311/18 (Schrems II), and the end of the Brexit transition period on 31 December 2020, will have a significant impact on the smooth running of international business.

On 16 July 2020, Europe's highest court, the CJEU, ruled in *Data Protection Commissioner v. Facebook Ireland Limited*, Maximillian Schrems that individuals in Europe had insufficient redress against US bulk interception rules when their personal data was transferred to the United States under the US Department of Commerce "Privacy Shield" mechanism. This ruling followed a long running campaign by the activist, Max Schrems, who's prior case to the CJEU invalidated the predecessor to the Privacy Shield, the Safe Harbor.

It is a general tenet of European data protection law that, when personal data is exported from the European Union, any further processing must be to European standards unless the local data protection laws are considered "adequate" by the European Commission. Self-certification under the US Privacy Shield mechanism was a popular method for providing adequate data protection amongst US based service providers which had European customers and regularly needed to transfer personal data from Europe to the United States.

Schrems II impacts not only the over 5,300 US companies that enjoyed Privacy Shield self-certification, but also the many thousands of EU and US companies that rely upon US companies in their supply chain for data processing. This supply chain could include outsourcing, cloud services, data processing, data storage, telecommunications and the like.

CONTINUED ▸

As a consequence of Schrems II, companies with operations in Europe must now check whether or not their suppliers, and any of their suppliers' sub-contractors or vendors, were relying on Privacy Shield. If they were, those businesses must now use an alternative method of legal compliance.

The most popular method of alternative compliance is the use of Standard Contractual Clauses (SCCs). These are form contracts published by the European Commission and executed between data exporters and data importers. They permit the lawful export of personal data from the European Union and essentially provide that personal data is protected to a European standard. SCCs contain a provision that requires the exporter and importer to check that there is no local law or other circumstances that could adversely affect the protection of the personal data.

This will require a complex and comprehensive assessment.

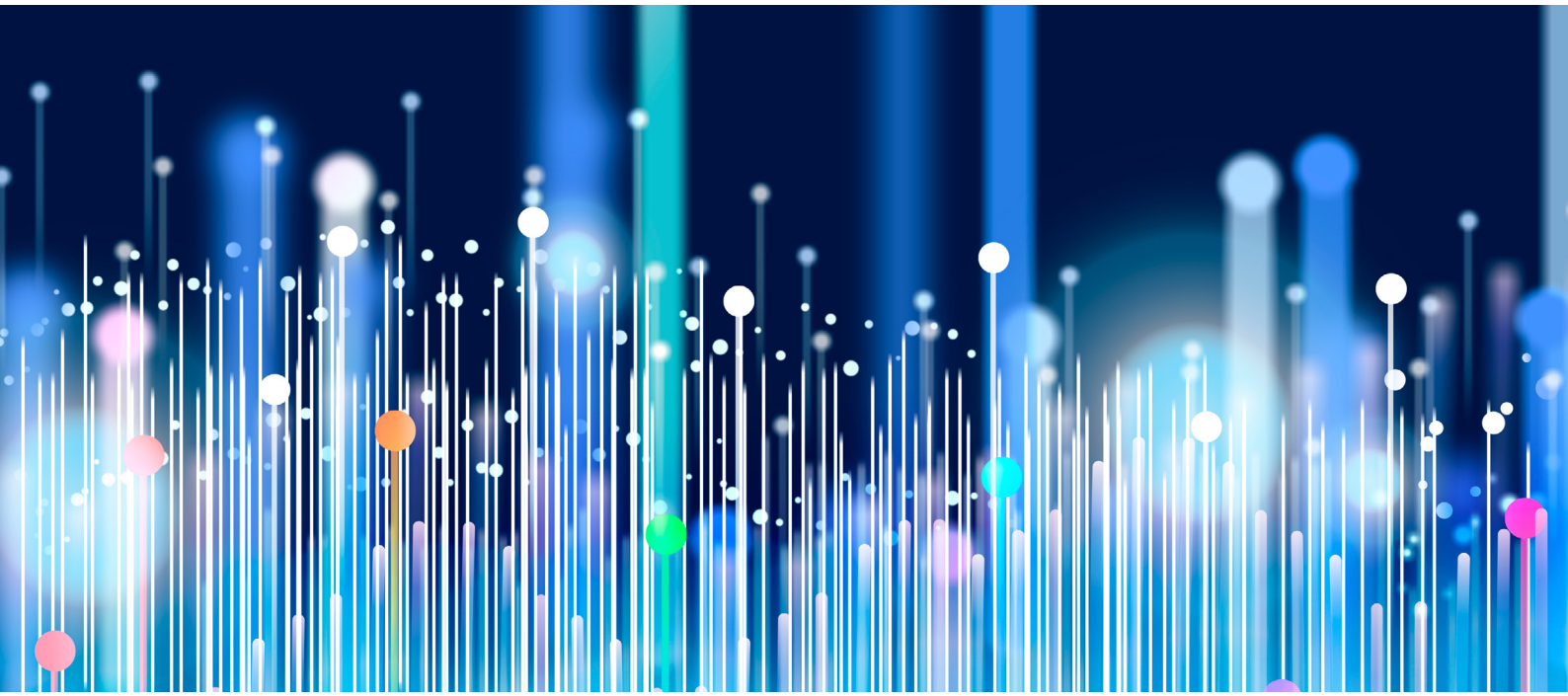
The CJEU also ruled in relation to these SCCs. Companies must now assess each SCC to make sure there are no local laws that can adversely affect the protection of personal data to European standards. Many companies will have thousands of these contracts in place. Although it is often easier for the data importer to undertake this assessment, as they will have the same contract in place with many of their European customers, under law it is the data exporter, or the customer, that is responsible for this assessment being done correctly and on a case by case basis

BREXIT

Technically, the United Kingdom has already left the European Union. Practically, however, the United Kingdom is in a transition period, during which all laws remain as they were until 31 December 2020. After this date, no EU laws, including the General Data Protection Regulation (GDPR) will form part of UK law. One key feature of the GDPR is that it permits the free flow of personal data amongst EU Member States.

Although the UK Government has already passed the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019, which will ensure that, on 1 January 2021, the UK data protection regime is essentially equivalent to the GDPR, this will not on its own be sufficient to allow the free flow of personal data from the European Union to the United Kingdom. What is required is for the European Commission to determine that UK data protection law is "adequate".

This will require a complex and comprehensive assessment, made more complex because, like the United States, the United Kingdom has extensive legislation allowing for bulk surveillance of communications. The EU assessment will therefore need to examine not just that legislation, but also the



ability for individuals in Europe to have adequate redress against the UK Government where their consider that their European data protection and privacy rights have been infringed.

Many companies will have thousands of these contracts in place.

In a recent communication, the European Commission recognised that an adequacy determination by December 31 is unlikely, and that companies should immediately take compliance steps to ensure that personal data can be legally transferred from the European Union to the United Kingdom, and that personal data previously received from the European Union is protected.

The most obvious compliance mechanism are the SCCs, but as we now know from Schrems II, rather than just signing these contracts, companies must undertake a case by case assessment.

Our Schrems II special report outlines practical guidance and next steps to ensure businesses are prepared for what's next following Schrems II.

ASHLEY WINTON
Partner
London
awinton@mwe.com

DR. LAURA SCAIFE
Associate
London
lscaife@mwe.com

START PREPARING FOR THE NEW EU WHISTLEBLOWER DIRECTIVE

Jacques Buhart, Nisrin Abelin and Caroline Ruiz Palmer

The new "Whistleblower Directive", which enables whistleblowers to reveal potentially unlawful activities while being shielded from retaliation, must to be transposed by Member States into domestic law by October 2021. Businesses should take note of several key provisions.

The legal regime applicable to whistleblowers across the European Union is fragmented. Only nine EU Member States currently have comprehensive laws. The remaining countries offer only partial rules, limited to certain sectors and specific wrongdoing. In practice, whistleblowing tends to be focused on the reporting of corruption concerns in the financial services sector.

In order to set minimum common standards across the European Union, the European Commission proposed a new directive on "the protection of persons reporting on breaches of Union law". Following approval by the European Parliament on 16 April 2019, Directive (EU) 2019/1937 received European Council approval and was officially adopted by the European Union on 7 October 2019.

The Directive must be transposed by Member States into domestic law by October 2021.

MATERIAL SCOPE (ARTICLE 2)

The material scope of the Directive relates to breaches of EU law in a broad range of areas, including public procurement; nuclear, radiation, product and food safety; transport; financial services; environmental and consumer protection; and data privacy. While there are certain areas of law to which the Directive does not apply (see below), Member States will be free to extend the scope of whistleblower protection.

The Directive also covers breaches affecting the European Union's financial interests (as referred to in Article 325 of the Treaty on the Functioning of the European Union), and breaches of the rules of the internal market, such as breaches of competition law rules.

The Directive is not intended to affect the application of EU or national law regarding the protection of classified information, the protection of legal and medical professional privilege, the secrecy of judicial deliberations and rules on criminal procedure.

PERSONAL SCOPE (ARTICLE 4)

The broad personal scope of the Directive encompasses all individuals "working in the private and public sectors who acquired information on breaches in a work-related context", regardless of the nature of their responsibilities.

The Directive protects employees, the self-employed, shareholders, and persons working under the supervision or direction of contractors. Surprisingly, whistleblowers can be individuals whose work-based relationship is yet to begin but have nonetheless acquired information regarding a breach of EU law during the recruitment process. The Directive also applies to persons reporting information on breaches acquired during a work-based relationship that has since ended.

The Directive extends its protection to colleagues or relatives of the whistleblower, who may suffer retaliation in a work-related context; and even to legal entities that the whistleblower owns, works for, or is otherwise connected with in a work-related context.

REPORTING SYSTEM (ARTICLES 7, 8, 10 AND 15)

The Directive creates a dual reporting system, consisting of both internal reporting to an impartial person or designated department within an organisation, and external reporting to an independent and autonomous authority, as designated by Member States.

Although internal reporting is encouraged in the first instance if "such channels are available" and "can reasonably be expected to work", the decision to choose between external reporting channels and internal reporting channels lies with the whistleblower and will depend "on the individual circumstances".

The Directive imposes an obligation on certain public and private organisations to set up an internal procedure to handle whistleblower reports.

With respect to the private sector, this obligation applies to companies with more than 50 employees (or with an annual turnover of €10 million), private legal entities of any size operating in the area of financial services, and those vulnerable to money laundering or terrorist financing, as regulated under EU Acts. Given how low these thresholds are, many small companies will be required to integrate these reporting procedures, creating a significant implementation burden.

In the public sector, this obligation applies to States, regions, and municipalities with over 10,000 inhabitants, or any other public entity.

Companies must acknowledge receipt of a report, to the whistleblower, within seven days, and "follow-up" within three months. Authorities are also obliged to acknowledge receipt to the whistleblower within seven days, unless this will threaten the whistleblower's anonymity, and follow-up within three months. In exceptional cases, the follow-up can be extended to a maximum of six months.

As a last resort, whistleblowers have the right to report to the media and to non-governmental organisations. Recourse to the media is also permitted in the first instance when there are "reasonable grounds to believe that an imminent danger for the public" exists.

The term "public interest" is not defined in the Directive and its meaning is therefore subject to the whistleblower's interpretation, which may also vary depending on the sector concerned. A lack of clear and objective criteria may result in whistleblowers bypassing internal and external reporting channels.

SCOPE OF WHISTLEBLOWERS' PROTECTION (ARTICLES 5 AND 19 TO 24)

Subject Matter of the Protection

Under the Directive, protection is granted against breaches or omissions: "i) that are unlawful and relate to the Union acts and areas falling within the scope of the Directive; ii) or defeat the object or the purpose of the rules in these Union acts and areas."

These protections are extended to any person who has reasonable grounds to believe the information gained in his/her work environment was true at the time of reporting, and complies with the requirements of the Directive in relation to reporting channels and procedure.

CONTINUED ▸

According to the Directive, the whistleblower's intent should be irrelevant when determining whether or not the protection should be granted. The Directive does not impose a condition of "good faith". Instead, it requires that the whistleblower has "reasonable grounds to believe" that the information is true.

Whistleblowers have the right to report to the media and to non-governmental organisations.

This means there is a real risk of abuse by malicious individuals, such as an unsuccessful job applicant. Article 23 does, however, provide for penalties against reporting persons "where it is established that they knowingly reported or publicly disclosed false information".

Prohibition of Retaliation

The Directive defines retaliation as threatened or actual acts or omissions that cause unjustified detriment to the whistleblower and have been triggered by the reporting, and provides a non-exhaustive list of direct and indirect behaviours that constitute retaliation.

After the whistleblower has demonstrated a *prima facie* case of retaliation following an alert, the alleged retaliator needs to prove that they were not acting in retaliation and their actions were based exclusively on justified grounds. Proving a negative act is likely to be a difficult task.

Anonymous Reporting

The Directive requires that the confidentiality of whistleblowers and of anyone mentioned in their report be preserved, while leaving it to Member States to decide whether or not reporting may be anonymous.

Penalties

The Directive requires Member States to "provide for effective, proportionate and dissuasive penalties" against those who retaliate against whistleblowers.

NEXT STEPS

Questions remain about whether or not Member States will make use of their power to extend the scope of the Directive, and how it will impact on existing national whistleblower laws, such as *Loi Sapin II* in France. It is also unclear how the Directive will interact with other laws and regulations, such as the General Data Protection Regulation. In addition, its "one-size-fits-all" approach will create bureaucratic burdens for sectors that already possess a legal framework for the reporting of certain infringements, such as the financial sector,

In light of the uncertainties and opportunities for abuse, the Directive will doubtless prove tricky to implement in practice. It does, however, provide employers across all industries with the opportunity to adopt a uniform and global approach to whistleblowing. Companies should seek advice and start preparing now to hit the October 2021 deadline.

JACQUES BUHART
Partner
Paris and Brussels
jbuhart@mwe.com

NISRIN ABELIN
Associate
Paris and Brussels
nabelin@mwe.com

CAROLINE RUIZ PALMER
Associate
Brussels
cruizpalmer@mwe.com

FEDERAL TRADE COMMISSION ZEROS IN ON PROBLEMATIC NON-COMPETES

Joel R. Grosberg and Lisa P. Rumin

In the last year, the US Federal Trade Commission (FTC) has demonstrated its willingness to challenge non-compete provisions in transaction agreements. Careful tailoring of a provision can mitigate the risk that antitrust enforcers will challenge the non-compete as substantially lessening competition.

Non-compete provisions help protect a buyer's significant investment in an acquired business. Although non-compete clauses often play a vital role in M&A deals, they are not immune from antitrust scrutiny.

Since September 2019, the FTC has challenged non-compete provisions in at least three transactions. These demonstrate that the Commission and other antitrust enforcers are closely scrutinising non-competes and will not hesitate to challenge problematic provisions, even when the underlying transaction raises no substantive antitrust issues or when the provision relates to minority investments.

Parties to a commercial transaction can easily manage this scrutiny by tailoring the scope of the non-compete to the transaction at hand.

Antitrust enforcers will look to internal documents and testimony as evidence.

WHAT HAS THE FTC RECENTLY CHALLENGED?

On 1 April 2020, the FTC challenged a series of agreements between Altria Group and Juul Labs whereby Altria agreed to refrain from directly or indirectly competing for closed-system electronic cigarettes in the United States in exchange for a 35% stake in Juul. Altria also agreed to refrain from undertaking research and design efforts to develop productions or technology that would compete with Juul. The non-compete provision prevented Altria from competing in the relevant market for effectively a six-year period. This challenge is significant because it related to the non-compete provision for a minority investment.

CONTINUED

The FTC alleged that, as a result of the non-compete, consumers lost the benefit of head-to-head competition between Altria and Juul, and between Altria and other competitors. The FTC also alleged consumers would be deprived of benefits from Altria's continuing innovation efforts to develop new and improved products. Although the complaint is heavily redacted, the FTC appeared to cite an internal document concerning Juul's negative reaction to Altria's proposal to modify the non-compete during the parties' negotiations.

On 3 January 2020, the FTC filed a complaint challenging Axon Enterprise's acquisition of Vievu from Safariland, and several non-compete provisions between Axon and Safariland. The transaction agreements contained a series of non-competes regarding products and services, customers and employees, many of which restricted competition for business areas that were unrelated to the acquired business. Each of the challenged non-competes had a duration of at least 10 years.

The FTC alleged that the non-competes substantially lessened competition because they were not reasonably limited in scope to protect a legitimate business interest. By refraining to compete for products, services, customers, and employees that were unrelated to the acquired business, the non-competes went "far beyond any intellectual property, goodwill, or customer relationship necessary to protect [...] Axon's investment in Vievu." Even if they had been reasonably limited to protect a legitimate business interest, the FTC alleged that the non-competes were overbroad and longer than reasonably necessary. Ultimately, Axon and Safariland agreed to rescind the non-competes.

On 13 September 2019, the FTC challenged the purchase by NEXUS Gas Transmission of a natural gas pipeline from North Coast Gas Transmission. The FTC did not have concerns with the transaction itself and challenged it solely on the grounds of the problematic non-compete, which prevented the sellers of the pipeline, including North Coast, from competing in three counties surrounding the Toledo, Ohio area for three years. Before the sale, the parties competed with each other in the Toledo, Ohio, area, but the non-compete would have barred North Coast from competing with Nexus post-transaction, even with the other pipelines it was not selling.

The FTC alleged that the non-compete was overbroad because it was not reasonably limited in scope to protect a legitimate business interest, explaining that "a mere general desire to be free from competition following a transaction is not a legitimate business interest." Even if the non-compete protected a legitimate business interest, the FTC alleged the geographic scope was overbroad because it prevented North Coast from competing for any opportunity in the restricted area, including opportunities that were unforeseen at the time of the deal. After the FTC filed its complaint, the parties agreed to eliminate the non-compete.

MITIGATING ANTITRUST RISK IN NON-COMPETE PROVISIONS

There are few cases analysing non-competes in the antitrust context, but the recent FTC challenges provide useful guidance for parties considering a non-compete as part of an upcoming transaction, including in connection with minority investments

The purpose of a non-compete is to protect the buyer's investment in the acquired business by preventing the seller from immediately re-entering the business following the sale. A non-compete should therefore be **necessary to protect the buyer's legitimate business interest** in intellectual property, goodwill, or customer relationship related to the acquisition. The non-compete should protect against the risk that the seller will appropriate the goodwill it is selling to the buyer.

A non-compete should **apply only to the primary product or service transferred** in the deal. The parties cannot simply agree "to be free from competition" in products unrelated to the transaction at hand. In some cases, a non-compete may restrict competition in ancillary products where the seller has concrete plans to enter or expand into the product and retains a business interest similar to the product being sold. In such cases, the antitrust agencies would likely carefully scrutinise the non-compete to determine whether or not the broad scope appropriately protects against a legitimate concern that the seller could easily re-enter the business being transferred in the sale and compete against the buyer.

Similarly, the **geographic scope must be reasonably tailored** and should not apply to irrelevant locations. A good rule of thumb is that the restricted area should be limited to the geographic area in which the seller offered products or services, or had contracts at the time of the transaction. Antitrust enforcers may consider ease of entry and the availability of viable alternative locations.

A non-compete should be **reasonable in duration**. In the recent cases, challenged provisions had durations of three, six, and over 10 years. While the FTC did not specifically call out the duration of the non-competes in the Altria/Juul or Nexus/North Coast cases, a non-compete that is borderline objectionable in other areas is likely to draw increased scrutiny if the duration is too long.

Antitrust enforcers will **look to internal documents and testimony as evidence** of an anti-competitive non-compete. In at least two of the recent cases, the FTC cited "hot documents" or testimony detailing the parties' views regarding the non-competes. In the Axon case, the FTC cited a statement from the Chief Executive Officer describing one of the non-competes as the "hidden jewel in the deal."

Parties should **pay close attention to non-competes located in ancillary agreements** that are negotiated as part of the deal, and not just focus on merger agreements or purchase agreements. In two of the recent cases, some of the challenged non-competes were located in ancillary agreements.

The **Federal Trade Commissioners are divided and have expressed competing views** on non-competes. Given that it is a Presidential election year, parties considering transactions should be mindful that the FTC's views on non-competes could become more hostile should the balance of the Commission change.

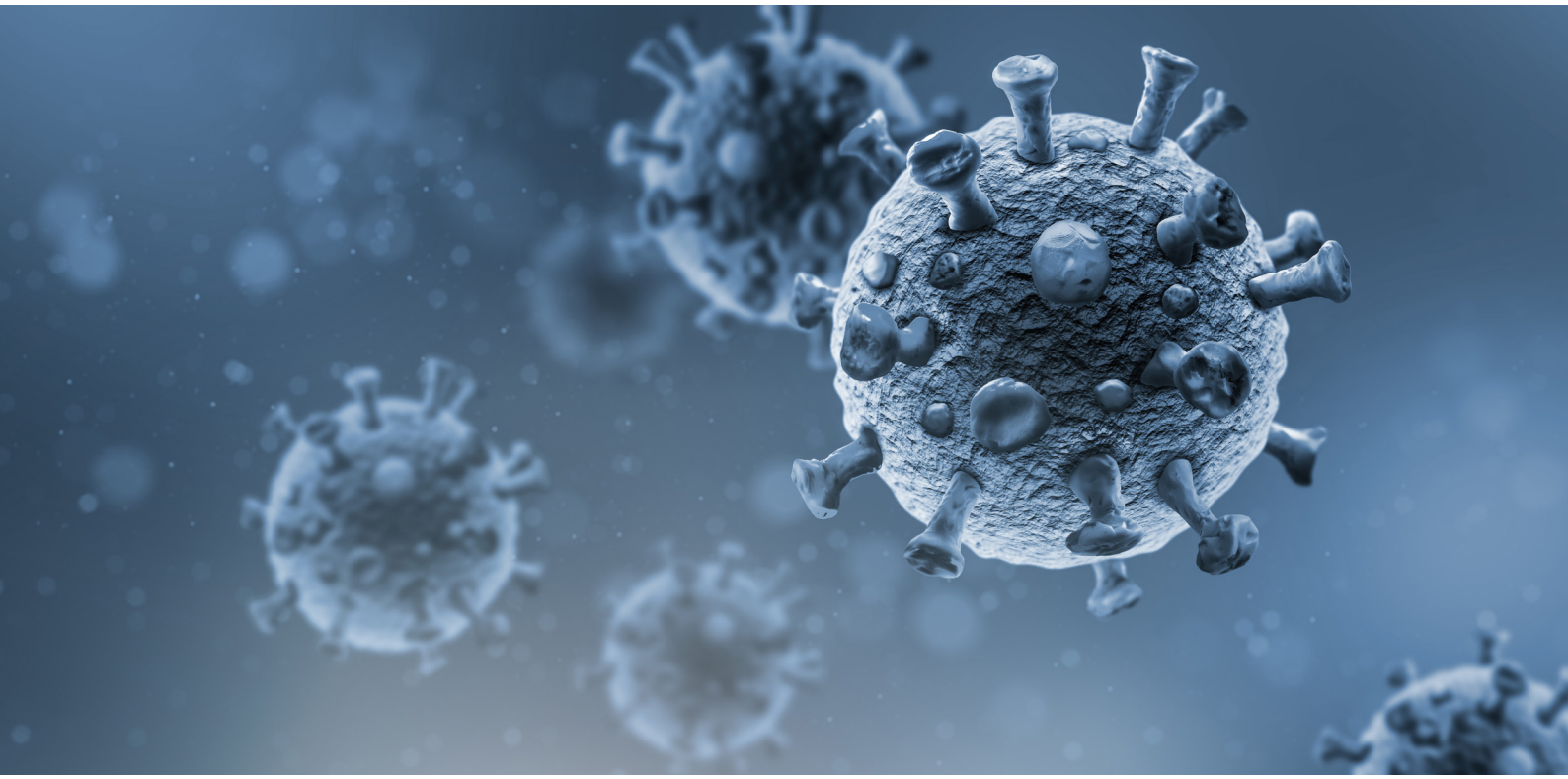
In one of the recent challenges, the FTC's two Democratic Commissioner issued a separate statement cautioning that "[t]oo many firms impose non-compete clauses to avoid the discipline of a functioning marketplace", urging the FTC "to be sceptical of non-competes that unnecessarily suppress competition" and encouraging the FTC to continue "to closely scrutinise contract terms that impede free and fair markets."

JOEL R. GROSBERG
Partner and Co-head, Antitrust Mergers Focus Group
Washington, DC
jgrosberg@mwe.com

LISA P. RUMIN
Associate
Washington, DC
lrumin@mwe.com

DEVELOPMENTS IN MATERIAL ADVERSE EFFECT CLAUSES IN M&A

Nicholas Azis, Thomas Sauermilch, Nicole Yoon, Nicolas Lafont, Dr. Tobias Koppmann, Fabrizio Faina and Nicholas Jupp



The Coronavirus (COVID-19) pandemic has brought Material Adverse Effect (MAE) clauses in M&A transactions into renewed focus. In several announced M&A transactions, parties have sought to terminate or renegotiate agreements, and even commenced litigation based on MAE clauses.

MAE law and practice differs widely among key jurisdictions, such as the United States, France, Germany, Italy and the United Kingdom.

UNITED STATES

WHAT IS THE FUNCTION OF AN MAE PROVISION IN US M&A?

MAE clauses are always included in US M&A agreements. They are frequently used as a stand-alone closing condition and as a qualifier in the bring-down condition of the continued truthfulness at closing of representations made in the agreement. If an MAE occurred, or the representations would no longer be true and reasonably be expected to result in an MAE, a buyer may refuse to close and ultimately terminate the agreement.

HOW IS AN MAE TYPICALLY DEFINED?

An MAE is broadly defined as any event that has, or would reasonably be expected to have, a material adverse effect on the target group's business, assets, financial condition or results of operations, subject to certain carve-outs. It can also include the seller's inability to consummate the transaction. Clauses typically do not quantify an MAE.

The finding of an MAE in the United States is subject to specific case law.

The finding of an MAE in the United States is subject to specific case law. Delaware, for example, has the most influential MAE case law. It applies a very high bar to finding an MAE, requiring that it must be "material when viewed from the long-term perspective of a reasonable buyer" and result in a durationally significant reduction in the target's long-term earnings power.

In *Akorn v. Fresenius Kabi* (2018), the Delaware Chancery Court provided some guidance on quantitative benchmarks that are likely to influence future decisions: a 40% decline in earnings as indicative of a stand-alone MAE, and a 20% decline in valuation as indicative of an MAE in the bring-down condition. These benchmarks are not dispositive, cases are fact-intensive and may turn on qualitative evidence.

WHAT ARE THE TYPICAL CARVE-OUTS AND EXCEPTIONS?

Typical carve-outs include effects from general economic conditions; conditions in the industry; changes in law or accounting principles; failure to meet projections; deal announcement and certain force majeure events, *e.g.,* war and natural disasters. These are also referred to as "systemic" risks that a buyer is expected to bear, except to the extent that certain carved-out risks affect the business disproportionately.

WHICH ELEMENTS ARE TYPICALLY NEGOTIATED?

While certain market standards have developed, the inability to consummate the transaction, the definition of "disproportionate" and "durational" effects, and certain carve-outs that shift risk in an unacceptable manner, are frequently up for negotiation. A buyer may not be prepared to accept the risk of earthquakes in a seismically active region, for example, or carve-outs for "known" conditions.

WHAT ARE THE CURRENT TRENDS AND ISSUES?

Issues in deal terminations include whether, absent an explicit MAE carve-out, the risk of pandemics is captured in the general systemic carve-outs, *e.g.,* general economic changes or changes in law.

The trend in carve-outs is to include pandemics, but buyers are increasingly demanding more specific closing conditions in addition to an MAE, such as no material loss of key customers, or no material impact on earnings before interest, taxes, depreciation, and amortization (EBITDA).

Committed acquisition financings are expected to continue to adopt the MAE definition of the M&A agreement.

FRANCE, GERMANY AND ITALY

WHAT IS THE FUNCTION OF AN MAE PROVISION IN M&A IN FRANCE, GERMANY AND ITALY?

In addition to being sometimes used as a stand-alone closing condition, an MAE or material adverse change provision is frequently used in the warranty relating to the absence of material changes between the date of the latest accounts and the signing of the acquisition agreement. This warranty is occasionally repeated or "brought-down" at closing. The MAE clause is, however, rarely used to qualify only the bring-down of the seller's warranties at closing.

HOW IS AN MAE TYPICALLY DEFINED?

An MAE is generally broadly defined as covering any event that has, or could reasonably be expected to have, a material adverse effect on the target's business and, occasionally, on its future prospects. It is relatively uncommon (and very rare in Germany) to include the target's inability to consummate the transaction in the definition of an MAE.

Owing to a lack of specific case law, the enforceability of an MAE provision depends on its drafting. This is why the MAE is frequently quantitatively defined as a percentage of the purchase price or a fixed euro amount, by reference to an accounting metric, such as EBITDA, or simply as a loss. A financial threshold may raise issues such as how amounts recovered from insurance, or provisions booked in the accounts regarding the MAE event, affect its calculation.

CONTINUED ▸

WHAT ARE THE TYPICAL CARVE-OUTS AND EXCEPTIONS?

The majority of MAE provisions include one or more carve-outs. They usually relate to general economic, market and industry conditions, as well as changes in law and accounting principles. MAE provisions often capture only the target's material subsidiaries or business units.

The current market trend is to specifically exclude pandemics.

Occasionally, there are exceptions as to the absence of a disproportionate effect of these carve-outs on the target business.

WHICH ELEMENTS ARE TYPICALLY NEGOTIATED?

The financial threshold defining the MAE, as well as the carve-outs relating to changes in market and industry conditions (including whether or not such changes are limited to certain countries, and whether or not a disproportionate effect exception should apply) are generally heavily negotiated. In Germany, the consequences of enforcing an MAE clause, such as a termination fee, is also a topic for negotiation.

WHAT ARE THE CURRENT TRENDS AND ISSUES?

At the beginning of the pandemic, the possibility of invoking an MAE clause in deals signed before the pandemic was a hot topic, especially in relation to broadly defined MAE provisions. The current market trend is to specifically exclude pandemics (including COVID-19) from MAE definitions, as a pre-existing condition. In sectors directly affected by the pandemic, buyers may seek to obtain specific closing conditions covering the consequences of the pandemic on the target.

Until the syndicated and leverage loan markets are more active again, it is unclear whether or not MAE provisions will be widely used in the financing documentation.

UNITED KINGDOM

WHAT IS THE FUNCTION OF AN MAE PROVISION IN UK M&A?

An MAE clause in private treaty transactions is a closing condition giving the buyer rights (including termination) where adverse events occur that render the transaction no longer viable on the agreed terms. In UK public takeovers, the ability to invoke a material adverse effect requires an even higher threshold akin to contractual frustration. For example, in the aftermath of 9/11, the invoking of MAEs by WPP Group PLC following its offer for Tempus Group PLC, and during COVID-19 by Brigadier following its offer for Moss Bros Group PLC, were both rejected.

HOW IS AN MAE TYPICALLY DEFINED?

MAEs include any fact, matter or event which could or could reasonably be expected to materially and adversely affect the business, assets and operations of the target group.

WHAT ARE THE TYPICAL EXCEPTIONS?

Exceptions include

- Any adverse change or event arising from
  - Business or economic conditions
  - National, international, political or social conditions
  - Changes in markets or laws or their interpretation
- A failure to meet any projections, forecasts or revenue predictions
- Changes that apply to industries or markets in which the group operates
- Matters that have been disclosed or arise from the announcement of the transaction or a change of control of the target.

WHICH ELEMENTS ARE TYPICALLY NEGOTIATED?

Negotiations will focus on the subjective/objective interpretation of the MAE clause and whether or not the clause is forward looking and triggered by events that could reasonably be expected to have material adverse effects. Other areas of negotiation typically include group/individual application and financial thresholds.

WHAT ARE THE CURRENT TRENDS AND ISSUES?

In private treaty transactions, MAE clauses are heavily negotiated, but seldom triggered or litigated, and mostly seen in larger transactions with an international dimension. Limited conditionality is borne out of the sellers' focus on agreeing a certain funds deal, with limited opportunity for the buyer to terminate once the deal is signed.

Leading case law's high watermark in *Grupo Hotelero Urvasco v Carey Value Added* [2013] requires that adverse change be i) material, ii) not temporary, and iii) financial condition is determined by reference to information covering the relevant period. Parties exercise remedies upon a breach of a material term and instead utilise MAE to negotiate changes/pricing. COVID-19 has given rise to some buyers terminating acquisition agreements, resulting in potential litigation, although UK and supra-national regulators have urged caution before the exercise of remedies and reputation remains a key consideration.

NICHOLAS AZIS
Partner
London
njazis@mwe.com

FABRIZIO FAINA
Partner
Milan
ffaina@mwe.com

DR. TOBIAS KOPPMANN
Partner
Munich
tkoppmann@mwe.com

NICOLAS LAFONT
Partner
Paris
nlafont@mwe.com

THOMAS SAUERMILCH
Partner
New York
tsauermilch@mwe.com

NICHOLAS JUPP
Associate
London
njupp@mwe.com

NICOLE YOON
Associate
New York
nyoon@mwe.com

SOLUTIONS FOR SPONSORS AND PORTFOLIO COMPANIES DURING MACROECONOMIC DISTRESS

Mark Fine and Aymen Mahmoud

Sponsors and companies face a number of practical and financial difficulties at the moment. There are, however, steps that can be taken to mitigate these.

Perhaps the most critical challenge is liquidity. Unlike previous periods of economic distress, 2020 has seen few liquidity shortages, but businesses should ensure they maintain a strong cash position by using liquidity monitoring modelled against any bank covenant models, and monitor the situation on a 13-week basis, or more frequently, to identify liquidity issues early. This information should help to inform whether or not discussions with lenders are required. An early dialogue with lenders can often be a highly effective tool in securing required amendments or even additional liquidity. It may also be helpful for companies to actively maintain frequent cash management sweeps to reduce cash inefficiency.

Sponsors and companies may have access to many avenues of liquidity, whether through government schemes or permissive financing documentation. Advisors are undertaking analyses with a view to offering short and medium term solutions.

An early dialogue with lenders can often be a highly effective tool

One tactic of recent times, deployed to good use by private equity sponsors, is to consider acquisitions or divestitures to rebalance periods of underperformance or to optimise long-term issues. Target assets may be available at attractive pricing levels and may add much-needed earnings before interest, taxes, depreciation, and amortisation to a struggling balance sheet, whether or not that struggle is temporary.

Discussions with lenders may not always be straightforward, but maintaining an early dialogue may represent the difference between i) a consensual amendment of a covenant profile, and/or other operational matters, to allow a business to continue to operate normally; and ii) an expensive and protracted negotiation. While information available to a company or sponsor might be imperfect, and audits may not be available or useful, intelligent information sharing can save time and money.

Consider acquisitions or divestitures to rebalance periods of underperformance.

As companies' focus turns to operational matters, they may look to internal modelling strategies, active supply chain management, adjustments of inventory, tax analyses and internal reorganisations. Engagement with advisors on these matters can sometimes appear to represent unnecessary expenditure but may in reality generate significant savings. Two-way engagement with advisors is important in helping sponsors and companies to identify and implement effective changes.

Workforce management is always a challenge during economic stress, but government schemes may offer a useful alternative to a rationalisation, which might in itself be costly, and expensive, recovery-based recruitment later. Employers should consider the possibility of variable or non-cash elements to maintain an incentivised workforce.

It is clear that management teams and sponsors face a difficult task in balancing operational matters with careful and forward planning. Early engagement with all stakeholders in an efficient and cost-effective manner will help ensure that businesses remain properly supported.

MARK FINE
Partner
London
mdfine@mwe.com

AYMEN MAHMOUD
Partner
London
amahmoud@mwe.com

mwe.com

McDermott
Will & Emery