Technology M&A 2022

Contributing editors
Arlene Arin Hahn and Neeta Sahadev
White & Case LLP

Diverse & distinctive

LEXOLOGY
Getting The Deal Through

WHITE & CASE

Diverse & distinctive

Most Innovative Law Firm in North America

The Financial Times North America Innovative Lawyers 2020

Received the highest ranking on the American Lawyer Diversity Scorecard among the *Am Law* top ten firms by revenue for eight consecutive years.

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

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

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

First published 2018
Fourth edition
ISBN 978-1-83862-727-0

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Technology M&A 2022

Contributing editors
Arlene Arin Hahn and Neeta Sahadev
White & Case LLP

Lexology Getting The Deal Through is delighted to publish the fourth edition of *Technology M&A*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Arlene Arin Hahn and Neeta Sahadev of White & Case LLP, for their continued assistance with this volume.

London
September 2021

Contents

Introduction

Arlene Arin Hahn and Neeta Sahadev

White & Case LLP

We are pleased to introduce this fourth edition of *Lexology Getting The Deal Through: Technology M&A*. The covid-19 pandemic reinforced the importance of technology and its rapid penetration into every facet of our lives, and we continue to see technology being a leading and dominant contributor of mergers and acquisitions.

Global M&A deal value in the second half of 2020 reached the highest half-year figure in history, according to Mergermarket data. Further, during the first quarter of 2021, Mergermarket reports that global M&A activity reached the most active annual opening on record, led by larger deal values, but fewer deals. This rise in deal value appears to have been partially led by the technology sector. Although the number of deals in technology, media, and telecommunications (TMT) declined in 2020, the value still climbed up 56.8 per cent, from US$543.4 billion to US$851.8 billion, compared to the previous year.

The M&A market has also seen an unprecedented number of M&A transactions involving special purpose acquisition companies (SPACs), with technology being the most active sector for SPACs. According to Dealogic and Mergermarket data, M&A tied to SPACs has been spiking, with 99 deals totalling US$219.5 billion globally in the first quarter of 2021, surpassing all of 2020.

While the covid-19 pandemic and related remote working orders may be reaching an end in some parts of the world in 2022, the M&A market is likely to continue to see growth in areas such as video conferencing, home streaming, cloud services, contactless payments, e-commerce, cybersecurity and other essential technologies for remote living and working.

The purpose of this guide is to provide an overview of the various factors affecting technology M&A transactions across various jurisdictions. We begin by exploring the laws, regulations and policies that affect the structure and execution of technology M&A transactions, typically involving IP, data privacy and competition legal considerations. Many technology M&A transactions also deal with sensitive sectors or regulated industries, creating the possibility of mandatory governmental reviews, or prior approval or authorisation, particularly for those transactions involving foreign investors.

Our commentators also describe the due diligence processes in their respective jurisdictions. Specifically, we describe what a buyer will need to review and evaluate to confirm a target's ownership or rights to use critical IP assets, and how counsel confirms whether the IP is subject to any liens or security interests. In addition, we explore what information is publicly available for searching and confirming the ownership of IP assets, and what requirements exist under applicable law for the effective transfer of IP rights from employees and contractors. Our commentators also discuss how to assess data protection and cybersecurity risks for the purposes of M&A diligence, legal requirements for the transfer of rights under IP-related agreements, and the processes and procedures for developing software, including the use of open-source components.

The representations and warranties and other deal terms for technology M&A transactions are also discussed. Our commentators describe what is customary or the 'market' with respect to representations and warranties, covenants and closing conditions for technology M&A agreements across various jurisdictions, as well as the duration of survival periods and liability allocation for breaches of representations and warranties.

With the continued disruption of traditional industries by both the emergence of new technologies and global events such as the covid-19 pandemic, the technology M&A sector is poised to continue to grow and the demand for tech-savvy legal advisers is set to continue to rise. We hope this book provides our readers with practical guidance and reference points for getting the technology M&A deal through. We want to thank all of the writers and editors for their contributions and dedication to this guide.

China

Vivian Tsoi, Xiaofeng Gong and Yan Yan

White & Case LLP

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

1 What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

The Chinese government regulates technology transactions through several laws and regulations. The key laws and regulations are summarised below.

Transfer of technology

The Civil Code, 1 January 2021

The Civil Code is a codification of PRC private laws that regulate property and personal rights, which replaces the PRC Contract Law, and a series of other standalone civil laws. This law defines 'technology transfer agreements' as including:

- patent transfer agreements;
- patent application rights transfer agreements; and
- know-how transfer agreements.

The law sets out the rights and obligations of the transferor and transferee under technology transfer agreements, as well as the liabilities for breach of contract. For example, the law provides that the transferor shall guarantee that it is the legal owner of the technology to be transferred and that such technology be complete, accurate, valid and able to achieve the goals agreed to by the parties.

Pursuant to this law, the transferee must keep confidential the 'secret' part of the technology to be transferred within an agreed scope and term. If the transferor fails to transfer the technology as agreed, it must return part or all of the purchase price it received for the transfer and will be liable for breach of contract. If the transferee fails to pay the purchase price as agreed, it will have to pay the liquidated damages set forth in the agreement. If the transferee fails to do so, it must terminate using the patents or know-how, return relevant technical materials, and is liable for breach of contract. In addition, the law provides that any technology contract that illegally monopolises technology (see below) or infringes a third party's technology, is invalid.

The Interpretation of the Supreme People's Court Concerning Some Issues on Application of Law for the Trial of Cases on Disputes Over Technology Contracts, 1 January 2005 and lastly amended on 1 January 2021

This interpretation further explained the meaning of 'illegally monopolises technology' in the Civil Code described above. Applicable situations include:

- restricting the other party's technology development based on the transferred technology or use of any improved technology;
- prohibiting the other party from obtaining similar or competing technology from third parties;
- restricting the other party from reasonably implementing the technology;
- forcing the other party to accept additional conditions for the purpose of implementing the technology;
- unreasonably restricting the other party's sources of raw materials, accessories or equipment; or
- prohibiting the other party from questioning the validity of the technology.

The Patent Law, 1 April 1985 and lastly amended on 1 July 2021

According to this law, patent and patent application rights can be transferred. To transfer the patent or the patent application rights, parties need to enter into a written contract and apply to the China National Intellectual Property Administration (CNIPA) for registration. The transfer will be effective on the date of registration.

The Copyright Law, 1 June 1991 and lastly amended on 1 July 2021

According to this law, copyrights, other than rights of publication, authorship, alteration and integrity, may be transferred. To transfer copyrights, the parties must enter into a written contract, and they may choose to file such a contract with the National Copyright Administration or its local branch.

The Trademark Law, 1 March 1983 as lastly amended on 1 November 2019

The law provides that, to transfer registered trademarks, parties need to enter into a transfer agreement and apply to the Trademark Office of the CNIPA (the Trademark Office) for approval. The Trademark Office will make a public announcement once it approves the transfer and the transferee will have title to the registered trademark on the date of the announcement.

The Computers Software Protection Regulation, 1 January 2002, and the Computer Software Copyright Registration Measures, 20 February 2002

According to these two regulations, to transfer software the parties must enter into a written contract. They may choose to register said the contract with the China Copyright Protection Centre.

The Integrated Circuit Layout Design Protection Regulations, 1 October 2001 as lastly amended on 1 March 2013

According to this regulation and its implementing rules, to transfer an integrated circuit layout design, the parties must enter into a written contract and register the contract with CNIPA. The transfer will be effective upon the date of registration. In addition, if a Chinese entity intends to transfer its layout design to a foreign person, it shall submit such a transfer to the relevant governmental authorities for approval when applying for the transfer contract registration.

Cross-border transfer of technology

The Special Administrative Measures (Negative List) for the Access of Foreign Investment (2020 version) and the Special Administrative Measures (Negative List) for Foreign Investment Access in Pilot Free Trade Zones (2020 version), both dated 23 July 2020

The Negative Lists set out industries that are restricted or prohibited from receiving foreign investment. Foreign persons may not invest in certain industries in which the Chinese government does not wish to disclose relevant technologies or sensitive information, such as the development and production of precious plant or animal species, genetic diagnoses and therapies, and selective breeding and seed production of transgenic agricultural products.

The Measures for Security Review of Foreign Investment, 18 January 2021 (the NSR Measures)

The NSR Measures provide that the government may conduct a national security review of a foreign investment that has or may have an impact on national security. 'Foreign investment' thereunder includes greenfield foreign investment, investor's acquisition of equity interests or assets of a PRC-incorporated company or foreign investment in other forms. A foreign investment may be subject to mandatory filing for national security review, if it is (1) in sectors related to national defense and security, such as arms and arms-related industries; or in geographic locations in close proximity of military facilities or defence-related industries facilities; or it (2) involves critical sectors significant for national security, such as critical agricultural products, critical energy and resources, critical equipment manufacturing, critical infrastructure, critical transportation services, critical cultural products and services, critical information technology and Internet products and services, critical financial services and key technologies; and will result in foreign investors' obtaining actual control of the target company.

The governmental agency responsible for PRC national security review is the Working Office established under the National Development and Reform Commission (NDRC) and jointly led by the NDRC and the Ministry of Commerce (MOFCOM). The Working Office has the right to terminate the transaction or ask the buyer to dispose of relevant equity interest or assets to eliminate relevant adverse effects. Foreign buyer and/or the target company can conduct a pre-filing consultation with the Working Office, to ascertain whether a transaction is a covered transaction. For a covered transaction, the parties are not allowed to complete the transaction before obtaining the clearance of national security review.

The Foreign Trade Law, 1 July 1994 and lastly amended on 7 November 2016

According to this law, the Chinese government divides technologies into three categories:

1 technology that may be freely imported or exported;
2 technology that is restricted from import or export; and
3 technology that is prohibited from import or export.

Companies that import or export technologies in category (1) must register the import or export contract with MOFCOM or its designated department. Companies that import or export restricted technologies in category (2) must obtain permits from MOFCOM or other relevant authorities. In addition, the state may restrict or prohibit the import or export of certain technology due to other reasons, such as:

- the protection of national security, social public interest, or human health or safety;
- exhausted natural resources; and
- maintaining the state's international financial status or balance of international payments.

The law further provides that the state may adopt any measure to regulate the importing and exporting of technology relating to nuclear materials (including fissionable material, fusion material and derivatives that may generate the abovementioned materials), weapons and other military supplies or for the purpose of maintaining international peace and security during wartime.

Regulations on Administration of Import and Export of Technologies, 1 January 2002 and lastly amended on 29 November 2020

This regulation provides that MOFCOM will categorise technologies that are restricted or prohibited from being imported or exported. MOFCOM may revise these categories from time to time. Contracts for importing or exporting restricted technologies may only take effect when an import or export permit is issued, while contracts for importing or exporting unrestricted technologies may take effect upon signing.

Foreign Investment Law of the People's Republic of China and its implementing rules, 1 January 2020

The new Foreign Investment Law and its implementing rules took effect on 1 January 2020. The law provides that the state encourages technology cooperation on the basis of free will in foreign investment. Technology cooperation conditions shall be determined under the principle of fairness towards all investing parties through equal consultation. No administrative agencies or their employees may force the transfer of any technology (by the foreign investors or the foreign-invested enterprises) by administrative means.

Laws and regulations on the transfer of technology in certain industries

In addition to the general technology transfer regulations mentioned above, the Chinese government has enacted special rules regulating the transfer of technologies in certain industries, including in the areas of medical, aviation, health food, chemicals, biological products, nuclear materials, equipment, non-nuclear materials used for reactors and relevant technologies and military technology.

For technology transfers subject to governmental approval, parties usually include obtaining the relevant approvals as a condition precedent to the closing of the transaction.

Government rights

2 Are there government march-in or step-in rights with respect to certain categories of technologies?

Various government authorities will be involved with a technology transfer in different areas. For example, the transfer of intellectual property must be filed with China National Intellectual Property Administration (for patents, trademarks and integrated circuit designs), the National Copyright Administration (for copyright) and the China Copyright Protection Centre (for computer software); the transfer of nuclear power-related technology will need approval from China Atomic Energy Authority, the China Commission of Science Technology, the Industry for National Defence and MOFCOM; and the transfer of regulated chemical-related technology will need approval from the State Bureau of Petroleum and Chemical Industry.

According to the National Security Review Measure, foreign buyers' acquisition of equity interests or assets of a PRC-incorporated company in certain sensitive sectors (eg, in the defence industry, or critical agricultural products and critical information technology and internet products and services sectors) will constitute a covered transaction that requires mandatory filing for national security review. If the Working Office considers the transaction to have a materially adverse impact on national security, it has the right to terminate the transaction or ask the buyer to dispose of relevant equity interest or assets to eliminate relevant adverse effects.

In addition, according to the Foreign Trade Law, the government may restrict or prohibit the import or export of certain technology to:

- protect national security or public policy;
- protect human health or safety, animal or plant life, or environmental health;
- implement measures related to the importing or exporting of gold or silver;
- protect scarce resources or exhausted natural resources;
- limit the market of the export destination;
- maintain a trading order;
- establish a certain domestic industry;
- protect domestic agriculture, stock farming or fishery industry; or
- maintain the state's international financial status or balance of international payments.

The law further provides that the state may adopt any measure to regulate the import or export of goods and technology relating to nuclear materials (including fissionable material, fusion material and derivatives that may generate the above-mentioned materials), and import and export of weapons and other military supplies to protect national security or adopt any measure to regulate the import or export of technology for the purposes of maintaining international peace and security during a war. Companies that import or export restricted technologies must obtain permits from MOFCOM.

Legal assets

3 How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

Patent and patent application rights

According to the Patent Law, to transfer patent or patent application rights, the parties need to enter into a written contract and apply to CNIPA for registration. The transfer will be effective on the date of registration.

Copyright (including computer software)

According to the Copyright Law, to transfer copyright, the parties need to enter into a written contract, that includes:

- the name of the work;
- type of the rights being transferred and the relevant territory;
- consideration and payment method and date; and
- liabilities for breach of contract.

The Implementing Rules of the Copyright Law provide that parties may choose to file the copyright transfer agreement with the National Copyright Administration or its local branch, but such a filing is not mandatory. The transfer will be effective on the effective date of the transfer contract.

Trademarks

The Trademark Law provides that to transfer registered trademarks, the parties need to enter into a transfer agreement and apply to the Trademark Office for approval. The Trademark Office will make a public announcement once it approves the transfer and the transfer will become effective upon such an announcement.

Integrated circuit layout design

According to Integrated Circuit Layout Design Protection Regulations and its implementing rules, to transfer an integrated circuit layout design, the parties need to enter into a written contract and register the contract with CNIPA. The transfer will be effective on the date of registration. In addition, if a Chinese entity intends to transfer its layout design to a foreign person, it shall submit the approval of the transfer that was issued by relevant authorities when applying for the transfer contract registration.

Other technologies

Chinese law does not provide specific formalities for the conveyance of non-registered technologies, such as know-how. Usually, such technology can be transferred in the manner and on the date as agreed to by the parties.

DUE DILIGENCE

Typical areas

4 What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

With respect to technology and IP assets in technology M&A transactions, to help identity issues that may affect the valuation or closing of the transaction, due diligence normally focuses on the following areas:

- title and encumbrances of the technology and IP assets, for example:
  - whether the IP assets are owned by the target or licensed to the target by a third party;
  - whether the intellectual property is developed by the target or acquired from a third party; or
  - whether the IP assets are subject to any pledge;
- IP-related agreements, including relevant employee invention assignment or work-for-hire provisions in employment contracts, IP licences or assignment agreements, and IP-related provisions in commercial contracts;
- IP disputes and infringement claims, including all past, pending and threatened infringement and other IP-related claims and proceedings;
- IT assets (eg, software systems and support services); and
- data privacy, including the target's internal policies and practices on the collection, use, transfer and protection of personal information.

For carve-outs or asset purchases, the parameters of due diligence will be the technology and IP assets to be acquired. Due diligence is also necessary to properly define and describe the scope of assets and rights and liabilities pertaining to such assets, in the asset purchase agreement.

In a share acquisition, in addition to the typical due diligence areas for an asset transfer, the buyer should review, from a commercial standpoint, whether the target has all the technology and IP necessary to operate its business as a going concern after closing. Particular care must be paid to the IT-related agreements to identify change of control provisions that may be triggered by the contemplated transaction.

Customary searches

5 What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

Public searches on the following online databases or using the following tools are customarily performed when conducting technology M&A due diligence in China:

- the National Enterprise Credit Information Disclosure System, maintained by the State Administration for Market Regulation, for the target's corporate particulars;
- the Patent Search and Analysis System of CNIPA for registered patents and published pending patent registrations;
- the China Trademark Database of the Trademark Office for registered trademarks and pending trademark registrations; and
- the '.cn' domain name database of China Internet Network Information Centre for '.cn' domain names.

The buyer may also run a public search at the website of the Copyright Protection Centre of China (CPCC) for registered copyright works (including software). Under Chinese law, copyright is an automatic right and is not created upon registration. Many copyright owners (especially software owners) nonetheless register their copyrighted works with the CPCC as evidence of title in case of infringement claims.

Registrable intellectual property

6 What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

Registerable intellectual property includes patents (ie, inventions, utility models and industrial designs), copyright, trademarks, plant variety rights and layout designs of integrated circuits. Non-registrable intellectual property includes trade secrets and know-how. In China, copyright works can be registered with the CPCC, but registration is not a prerequisite for the creation of a copyright.

To verify the title of registrable intellectual property, the buyer should request registration certificates or receipts of acceptance of registration applications for registered and pending registrations. Public searches with relevant registration authorities (eg, the CNIPA and the Trademark Office) are normally performed to independently verify the title of the registered intellectual property.

In terms of non-registrable intellectual property, the buyer may review confidentiality policies, non-disclosure agreements, IP assignments, and work-for-hire provisions under relevant contracts, to form a general view on the ownership status of key unregistered intellectual properties.

Liens

7 Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

Yes, certain intellectual property (ie, registered trademarks, patents and copyrights) can be pledged under Chinese law. Pledges over registered trademarks, patents and copyrights are perfected by registering of such a pledge with the competent authority (ie, the Trademark Office, CNIPA and CPCC, respectively). The release of pledges is also effectuated upon registration of the release with said authorities. The time required for completing the process of perfecting or releasing pledges varies depending on the type of pledged intellectual property. For instance, perfecting or releasing a pledge of patents with CNIPA normally takes a week.

If there is any encumbrance, such as a pledge, over intellectual property or technology assets that are to be acquired, the release of such encumbrances, if required, is typically affected on or prior to closing and after the signing of the relevant asset or share purchase agreement.

Employee IP due diligence

8 What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

For employee-created and contractor-created intellectual property and technology, the buyer would need to review the intellectual property ownership and assignment or work-for-hire clauses under relevant employment or development contracts. Public searches will also be undertaken to verify the current title of those intellectual properties being registered or pending registration with the competent authorities.

Under Chinese law, title to copyrights and patents developed or created by the target's employees in the course of performing their employment duties or by utilisation of materials and tools provided by the target automatically vests in the target. However, unless otherwise agreed, ownership of contractor-created copyrights and patents automatically vests in the contractor. Assignment of title of contractor-created patents to the target is deemed effective upon registration of the assignment with CNIPA. No registration formalities are required for the assignment of copyright.

Transferring licensed intellectual property

9 Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

The transfer or assignment of licensed intellectual property and technology by its owner does not require consent of the licensee. Note that transfers or assignments of trademarks and patents are effectuated upon registration of such a transfer or assignment with the Trademark Office and CNIPA, respectively. The transfer of registered patents or pending patent registrations by a Chinese individual or entity to a foreign individual is deemed a technology export, which may be subject to certain approval or filing requirements under the Chinese export control regime.

The transfer or assignment by a licensee of its rights and obligations pertaining to licensed intellectual property and technology normally requires consent of the licensor, unless the licence agreement states otherwise.

There is no differentiation between exclusive and non-exclusive licences in connection with the above-mentioned transfer or assignment.

Software due diligence

10 What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

Software due diligence undertaken by the buyer's lawyers will normally be focused on the title and encumbrances over the target's software copyright. In China, it is still not common for a target to provide code scans for third-party or open source code as part of due diligence.

Other due diligence

11 | What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

Data security and protection has become an increasingly hot-button area for due diligence with respect to some emerging technologies (eg, big data). The potential buyer must have a thorough understanding of the target's internal policies and practices regarding the collection, processing, storage and transfer of personal data, and the target's privacy and information security measures. Data privacy experts may be engaged to conduct standalone data privacy due diligence on the target to assess the target's compliance with privacy and data security requirements and standards, and to identify potential risks that may affect the valuation of the target or create any residual liabilities to the buyer.

PURCHASE AGREEMENT

Representations and warranties

12 | In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

It is customary to include representations and warranties for intellectual property, technology, cybersecurity and data privacy. For intellectual property and technology, representations and warranties usually cover title or the right to use, there has been no infringement, full disclosure on restrictions, and no breach of material contracts. For cybersecurity and data privacy, representations and warranties will at least cover compliance with applicable laws and regulations and industry guidelines.

Customary ancillary agreements

13 | What types of ancillary agreements are customary in a carveout or asset sale?

Customary ancillary agreements typically include transitional trademark licences, cross-licence agreements, and transition services agreements.

Conditions and covenants

14 | What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

Typical intellectual property or tech-related pre-closing conditions include signing assignment agreements for intellectual property or inventions, obtaining consents or waivers for asset transfers, correcting chain of title issues, obtaining necessary governmental approvals, and submitting applications to the Chinese registration authorities for the transfer of patents, trademarks, copyright and integrated circuit layout designs. Typical post-closing conditions or covenants include completion of registration of IP transfers (as it generally takes several months for the registration to be completed). Whether remediation of source code issues will be a pre-closing or post-closing condition depends on the commercial negotiations.

Survival period

15 | Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

The statute of limitations for patent, trademark and copyright infringement under Chinese law is two years. The survival period for representations and warranties generally ranges between one and two years.

Breach of representations and warranties

16 | Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

The liability cap for breach of IP-related representations and warranties is typically the same as the general liability cap for breach of nonfundamental representations and warranties. The general liability cap can range from a certain percentage of the purchase price to 100 per cent of the purchase price.

17 | Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

Liabilities for breach of IP representations and warranties are generally subject to the same de minimis thresholds, baskets or deductions (or other limitations) as the other representations and warranties, unless buyer has a specific concern regarding the target's intellectual property.

Indemnities

18 | Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

The parties may negotiate specific indemnities relating to intellectual property. A target's data security or data privacy compliance issues has increasingly become a point for negotiation of specific indemnities as Chinese law compliance on these two issues has become more stringent. The parties will focus on indemnification for regulatory fines imposed on the target, or any compliance issues that may affect any regulatory permits issued to the target for operations affecting data security or data privacy.

Walk rights

19 | As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

Generally, all representations and warranties, including with respect to intellectual property, are brought down at closing, subject to a materiality qualifier. The common practice is to have a materiality qualifier.

UPDATES AND TRENDS

Key developments of the past year

20 What were the key cases, decisions, judgments and policy and legislative developments of the past year?

The Civil Code

The People's Congress enacted the Civil Code of the PRC on 28 May 2020, which took effect on 1 January 2021. The Civil Code is a codification of PRC private laws that regulate property and personal rights, which replaces the PRC Marriage Law, the PRC Succession Law, the PRC General Principles of the Civil Law, the PRC Adoption Law, the PRC Guarantee Law, the PRC Contract Law, the PRC Property Law, the PRC Tort Law and the PRC General Provisions of the Civil Law.

The Measure for Security Review of Foreign Investment

The National Development and Reform Commission (NDRC) and the Ministry of Commerce (MOFCOM) jointly issued the Measure for Security Review of Foreign Investment (the NSR Measures) on 19 December 2020, which became effective on 18 January 2021.

The NSR Measures provides that the government may conduct a national security review of a foreign investment that has or may have an impact on national security. 'Foreign investment' thereunder includes greenfield investment, acquisition of equity interests or assets of a PRC-incorporated company or investment in other forms. A foreign investment may be subject to mandatory national security review if it:

- is in sectors related to national defense and security, such as arms and arms-related industries; or in geographic locations in close proximity of military facilities or defence-related industries facilities; or it
- involves critical sectors significant for national security, such as critical agricultural products, critical energy and resources, critical equipment manufacturing, critical infrastructure, critical transportation services, critical cultural products and services, critical information technology and Internet products and services, critical financial services and key technologies; and will result in foreign investors' obtaining actual control of the target company.

The governmental agency responsible for PRC national security review is the Working Office established under the NDRC and jointly led by the NDRC and MOFCOM. The Working Office has the right to terminate the transaction or ask the buyer to dispose of relevant equity interest or assets to eliminate relevant adverse effects. Foreign buyers and/or the target company can conduct a pre-filing consultation with the Working Office, to ascertain whether a transaction is a covered transaction. For a covered transaction, the parties are not allowed to complete the transaction before obtaining the clearance of national security review.

WHITE & CASE

Vivian Tsoi
vtsoi@whitecase.com

Xiaofeng Gong
xiaofeng.gong@whitecase.com

Yan Yan
yan.yan@whitecase.com

Unit 02-07, 41/F, HKRI Centre One, HKRI Taikoo Hui
288 Shimen Road (No. 1)
Shanghai 200041
China
Tel: +86 21 6132 5900
www.whitecase.com

Czech Republic

Jan Andruško

White & Case, s.r.o., advokátní kancelář

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

1 What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

The key Czech laws implicated particularly in technology M&A transactions are Act No. 231/2001 on Radio and Television Broadcasting, as amended (the Media Act) and Act No. 127/2005 on Electronic Communications, as amended.

The former governs the rights and obligations of radio and television broadcasters and their registration with the Council for Radio and Television Broadcasting (CRTB). The latter regulates the use of the radio spectrum, the allocation and use of radio frequencies, the rights and obligations of electronic communications services providers and end customers, and data protection.

The governmental approvals required for technology M&A transactions depend on a particular type of technology M&A transaction. For instance, a direct change of shareholders of a licensed TV or radio broadcaster company is subject to prior approval of the CRTB. Obtaining such prior approval is generally included as a condition precedent in the relevant transaction documentation (eg, purchase agreement).

In certain types of technology M&A asset deals, additional governmental approvals may be required. For instance, the transfer of radio frequency allocations is subject to prior approval of the Czech Telecommunication Office (CTO), which is also generally included as a condition precedent in the relevant transaction documentation (eg, an asset purchase agreement).

Government rights

2 Are there government march-in or step-in rights with respect to certain categories of technologies?

While step-in rights or march-in rights do not have an identical equivalent in Czech law, below are Czech law concepts that best approximate march-in or step-in rights.

The CRTB is entitled to revoke the existing licence granted to a broadcaster under certain specific circumstances, for instance, if the licensed broadcaster:

- failed to start broadcasting within a particular period after the grant of the licence became effective;
- failed to broadcast for a particular period after the commencement of broadcasting (save for cases involving technical obstacles);
- committed a certain administrative offence stipulated in the Media Act; or
- was convicted of an intentional crime.

Similarly, in connection with intellectual property, the Czech Industrial Property Office (CIPO) (the main public authority having competence in the area of IP rights enforcement) is entitled to revoke a registered trademark under certain specific circumstances, for instance, if within a continuous period of five years prior to the application for revocation, the trademark has not been put to genuine use in connection with the goods or services in respect of which it is registered, and there are no proper reasons for non-use; in consequence of acts or inactivity of the proprietor, the trademark has become the common name in the trade for a product or service in respect of which it is registered; or the relevant trademark misleading the public, particularly as to the nature, quality or geographical origin of the goods or services for which it is registered.

The CIPO can also grant a non-exclusive right to use an invention if its owner does not exploit the relevant invention or exploits it insufficiently and has not accepted a valid offer to enter into a licence agreement regarding the invention within a reasonable time from such offer having been made.

Further, the CTO is entitled to change the allocation of radio frequencies to a particular operator, especially if such change is necessary to comply with the obligations of the Czech Republic arising from an international treaty or the Czech Republic's membership in the European Union or another international organisation.

Legal assets

3 How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

Generally, Czech law distinguishes two main areas of intellectual property. The first includes copyright and related rights, that is, literary, graphic, architectural, artistic and musical copyrights, as well as copyright-related rights, such as rights of performing artists, publishers and record producers (computer programs and databases are also protected under copyright law). The copyright and related protections attach automatically as of creation – such works are not registered. Consequently, legal title to copyright and related rights are conveyed contractually (licence agreements).

The second includes industrial property rights (IPRs), that is, patents, industrial designs, utility models, topography of semiconductor products, trademarks, geographical denomination and appellations of origin. Registration principles apply to IPRs. Thus, to receive legal protection, an application for registration must be filed with the CIPO.

Consequently, a transfer of IPRs is subject to registration with the CIPO. Along with the application for registration of transfer, the IPRs transfer document (transfer agreement) must be submitted to the CIPO. For the transfer of trademarks, filing a confirmation of transfer (in the form set out by the CIPO) is sufficient.

To transfer IPRs registered with the European Union Intellectual Property Office (EUIPO) or the World Intellectual Property Organization

(WIPO), appropriate applications for the registration of transfer must be filed with the appropriate authority (directly with the EUIPO for EU-wide protection, and via the CIPO for IPRs registered with the WIPO).

The CTO must be notified in writing of the transfer of radio frequency allocations by way of legal succession without undue delay.

DUE DILIGENCE

Typical areas

4 What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

Due diligence for IP assets from a legal point of view customarily includes a detailed analysis of:

- all intellectual property applied for or owned by the target;
- any intellectual property used by the target at any time during the preceding three years, and any licences or other arrangements permitting the target to use such intellectual property;
- any intellectual property owned by third parties, the use or exploitation of which is or may be necessary or desirable for carrying on the business of the target, and of procedures that currently are or may need to be followed to avoid the infringement of any such rights;
- any licences or other arrangements permitting third parties to use intellectual property owned by the target;
- any objections to, or infringement (including alleged) by third parties of the target's intellectual property and vice versa;
- any circumstances where the benefit, or the right of use, of any intellectual property may be lost or adversely affected (including on a change of control of the target), as well as any fact or matter that might make any of the intellectual property invalid or unenforceable;
- any claims by employees or former employees in any inventions, works or other developments made by such former employees while employed, and any facts or circumstances that may give rise to any such claims;
- any encumbrances or security interests granted in the target's intellectual property; and
- all disputes, arbitrations, proceedings or settlements relating to intellectual property.

Due diligence for technology assets from a legal point of view customarily includes a detailed analysis of the following:

- all IT hardware used, together with details of their ownership and any licences or agreements relating to them;
- all software used, together with copyright ownership in the software, any software licences and access to source code;
- all software or hardware maintenance or support arrangements for the target;
- information on any personal data processed by the target and compliance control with respect to the relevant legislation governing the usage of personal data; and
- any encumbrances or security interests granted in the target's technology assets.

In transactions involving the transfer of IP and technology assets, the clients customarily engage also other advisers, who are specialists in this area and who review, for example, the operability and suitability of the technology assets.

In transactions involving carve-outs, substantial attention is given to the intellectual property owned by the seller's group outside the transaction perimeter, but necessary for the conduct of business of the target and IT services provided by the seller's group to the target, and vice versa, to identify the relevant separation issues that should be covered by the transitional services agreement (TSA) and the brand licensing agreement (BLA).

Customary searches

5 What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

Due diligence of targets in the Czech Republic customarily involves searches of the following public registers, which are not technology specific:

- the Commercial Register;
- the Trade Licensing Register;
- the Insolvency Register;
- the Criminal Records Register;
- the Central Register of Executions;
- the Cadastre of Real Estate; and
- the Register of the Ultimate Beneficial Owners.

Particular to technology M&A, additional intellectual property and technology databases and public registers are customarily searched:

1 the Patent and Utility Model Database;
2 the Industrial Design Database;
3 the Trade Mark Database;
4 the Database of Geographic Denomination;
5 the Appellation of Origin;
6 the Database of Allocated Radio Frequencies;
7 the Database of Undertakings in Electronic Communications; and
8 the list of broadcasters, retransmission operators and on-demand audio-visual media service providers.

The registers (1) to (5) allow searches of owner, applicant or originator data. The Database of Allocated Radio Frequencies only allows searches by frequency data, making it time-consuming to perform the relevant searches.

Registrable intellectual property

6 What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

Intellectual property rights under Czech law can be divided into copyright and related rights (these are not registered) and industrial property rights (IPRs) (registration principles apply).

Upon submission of IPRs application with the Czech Industrial Property Office (CIPO), the applicant is granted the right of priority, which protects the applicant against subsequent applications for the same and is granted automatically for patent applications, utility model applications and national trademarks applications.

Additional EU and international IPRs protections also exist. The EU trademarks priority claim can be filed using the EU trademark application within the set period of time. The international right of priority may also be granted, if the international trademark application is filed with the World Intellectual Property Organization (WIPO) via the appropriate national office (ie, the CIPO) within the set period of time.

For due diligence typically undertaken with respect to intellectual property (eg, review of the registrations, objection proceedings, arrangements permitting third parties to use IP owned by the acquiring target).

Liens

7 Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

Czech law permits liens or security interests on both IPRs and technology assets, with the exception of geographical denomination and appellations of origin.

In the case of IPRs that are registered in public databases or registers (ie, the Patent and Utility Model Database, the Industrial Design Database and the Trade Mark Database), the lien or security right is registered in such public register at the request of any of the parties to the pledge agreement. Therefore, when conducting due diligence, it is possible for acquirers to perform a search of such registers to determine whether there are any liens or security interests registered in respect of particular IPRs.

For technology assets (eg, a particular hardware or technological equipment) that are not registered in any of the aforementioned public registers, the lien or security right can be registered in a special register maintained by the Notarial Chamber of the Czech Republic, the Registry of Securities. Any notary is entitled to provide, upon request, a copy or an extract of the record in the Registry of Securities or a certificate confirming that a particular asset is free of any security interest.

Employee IP due diligence

8 What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

Due diligence of employee-created intellectual property and technology typically comprises detailed analysis of the following:

- employment contracts (in particular, the definition of the type of work performed by an employee and whether such definition covers all possible employee-created intellectual property or technology);
- any licences provided by employees for employee-created intellectual property or technology; and
- whether employees are authorised to transfer their property rights to third persons per their employment contracts.

Due diligence of contractor-created intellectual property or technology typically entails of detailed analysis of work contracts and licence agreements with the contractors relating to intellectual property and technology.

The general rule under Czech copyright law grants employers the ability to exercise property rights over the work employees create in connection with their employment on the employees' behalf. If the employer desires to transfer such property rights to third parties, the employer must acquire approval of the creator-employee (such permission is considered irrevocable and valid for all future transfers), except for transfer of the business enterprise, where such approval by creator-employee is not necessary.

Under Czech copyright law, for contractor-created work, the contractor is deemed to have provided a licence to the client. Unless agreed otherwise, the contractor remains free to license such work to third persons, if such licensing is not contrary to the legitimate interests of the client.

A special rule exists for computer software and databases, which are considered to be employee-created, even if they are contractor-created and the customer shall be deemed to be the employer.

Transferring licensed intellectual property

9 Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

The general rule under Czech law provides that an IP licence cannot be transferred to a third party without the licensor's consent. The Czech Civil Code provides an exception under which, unless the parties agreed otherwise, the licensor's consent is not necessary for transfer of intellectual property as part of the business enterprise (however, in these cases, IP rights cannot be transferred when such transfer is excluded by the relevant licence agreement or by the nature of such IP right itself).

In the case of transfer by way of legal succession, the licence is transferred to the acquirer automatically, unless such transfer is excluded by the licence agreement.

Software due diligence

10 What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

In the Czech Republic, the software due diligence is typically part of operational or technical due diligence (not legal due diligence). During legal due diligence, we customarily review only licence agreements, and contractor and employee contracts related to the development or licensing of software.

Other due diligence

11 What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

There is no special legislation for special or emerging technologies in the Czech Republic. Therefore, the Czech law treats modern technologies such as artificial intelligence or autonomous driving systems and software as assets (in line with the general definition of assets under the Czech Civil Code).

New legislation with respect to modern technologies, especially artificial intelligence and robots, is being discussed at the EU level. On 27 January 2017, the European Parliament adopted a report with recommendations to the European Commission on Civil Law Rules on Robotics, which urged the preparation of a draft legislative framework relating to the development and use of artificial intelligence within the next 10 to 15 years. The report also highlighted that there are no legal provisions specifically applicable to robotics but existing legal regimes and doctrines may be applied, although some aspects need specific consideration. Therefore, the report recommended supporting a technology-neutral approach to intellectual property that is applicable to the various sectors in which robotics could be employed. Since 2017, the Commission has held discussions and published working documents on this topic.

PURCHASE AGREEMENT

Representations and warranties

12 In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

The warranties for intellectual property, technology and data privacy form part of a standard set of warranties that is, to some extent, included in most M&A transactions. In general, the set of warranties for intellectual property, technology or data privacy is heavier in technology

M&A transactions than in M&A transactions involving manufacturing or similar targets.

The relevant warranties customarily comprise the following.

With respect to intellectual property:

- the ownership of material intellectual property necessary for the target's conduct of business;
- no notices on infringement of the target's intellectual property by a third party and vice versa;
- disclosure of all material licences to use third-party intellectual property necessary for the target's conduct of business; and
- assignment of employee-created intellectual property.

With respect to technology:

- the materially good working order and regular maintenance of IT systems and no material functionality failure thereof;
- validity and no notice of breach of material IT contracts;
- possession of source codes to all software necessary for the target's conduct of business; and
- with respect to data privacy, compliance with material data protection legislation.

The inclusion of cybersecurity warranties is not widespread in the Czech Republic M&A transactions.

In technology M&A transactions involving targets active in the telecommunications industry, the set of warranties includes, in particular, the warranties on due possession of the relevant regulatory licences and radio frequency allocation decisions.

Customary ancillary agreements

13 What types of ancillary agreements are customary in a carveout or asset sale?

The customary ancillary agreements in technology M&A transactions include transitional services agreement (TSAs) and brand licensing agreement (BLAs).

The TSAs typically govern the post-completion provision of services that, before the completion of the transaction, were provided to the targets at the seller's group level and vice versa. A provision stipulating that either party can request the provision of an omitted service (ie, a service that has been provided prior to carve-out, but is omitted from the TSA) is generally included in the TSAs. The targets benefiting from the transitional services of the seller's group are required to draw up a migration plan setting out the detailed steps of becoming self-sufficient in terms of services provided under the TSAs.

BLAs provide for licences to trademarks and domain names owned at a group level that are bespoke to the target's business. These agreements also contain provisions regarding rebranding and the discontinuation of use of the licensed intellectual property.

Conditions and covenants

14 What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

The condition precedents are typically limited to the purchaser's obligation to obtain the necessary competition and regulatory approvals for the transaction. Depending on their materiality, tech-related issues arising out of due diligence are customarily dealt with by way of the seller's pre-completion obligations.

Such pre-completion obligations usually depend on the particular issues identified in the course of due diligence and include, for instance:

- renewal of domain name registrations;
- assignment of employee-created IP rights;
- obtaining ownership to intellectual property where only a right of use in respect thereof has been granted to the target; or
- obtaining change of control consents from licensors under the licence agreements relating to third-party intellectual property used by the target.

Survival period

15 Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

The scope of fundamental warranties that are subject to a longer survival period is typically limited to the warranties relating to the seller's authority to enter into the agreement and title to the shares or assets being transferred, thus IP warranties are not typically included. Therefore, IP warranties are subject to the same survival periods as other operational warranties. The survival periods for such operational warranties vary considerably depending on the type of M&A transaction, and can range from a period of 12 months up to five years. However, this depends on the nature of the transferred business and, under certain circumstances, IP warranties may be included within the fundamental warranties, in particular where IP is a core part of the transferred business.

However, in certain technology M&A transactions, parties set the survival period at double of the survival period for operational warranties (36 months).

Breach of representations and warranties

16 Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

Similar to survival periods, no specific liability cap for a breach of IP warranties is generally included in the transaction documentation. The liability cap for operational warranties vary considerably depending on the type of M&A transaction and can range from a single-digit percentage of the purchase price up to 50 per cent of the purchase price. However, in certain technology M&A transactions, parties set the liability cap for breach of IP warranties at 70 per cent of the purchase price.

17 Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

In terms of IP warranties, it is not standard to carve these out from the de minimis thresholds, baskets or deductibles, or other limitations on recovery. The warranties provided for under the transaction documentation are customarily subject to the same limitations on liability, regardless of the subject matter to which they relate (except for maximum liability cap, which is typically higher for fundamental warranties).

Indemnities

18 Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

The specific indemnities provided for in a definitive agreement are customarily limited to coverage for the specific risks identified in the course of due diligence. Such specific indemnities can include:

- indemnification for claims of infringement of a third-party's intellectual property confirmed by a binding court decision;
- employee claims in respect of the development of intellectual property outside of the scope of their employment duties; and
- the lack of legal title for the processing of personal data.

Walk rights

19 As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

In general, the inclusion of a 'walk right' of the acquirer for breach of IP warranties between signing and closing is rather rare (as is the 'bringing down' of all warranties at closing; in some cases, the 'bringing down' of warranties is limited to specific warranties, such as fundamental warranties). If the warranties are 'brought down', usually a similar standard is required at closing as at signing.

However, in certain technology M&A transactions, parties may agree that a breach resulting in the warranties being materially untrue, and such breach resulting in a loss in excess of 50 per cent of the initial purchase price (excluding the earn-out amount, if any), entitles the purchaser to terminate the transaction.

UPDATES AND TRENDS

Key developments of the past year

20 What were the key cases, decisions, judgments and policy and legislative developments of the past year?

In the technology space, a hot topic in the Czech Republic during the course of 2020 was the release of the 700MHz radio frequency band from use by digital terrestrial television broadcasting and its utilisation for wireless broadband electronic communications services. In connection with this release, the transition of digital terrestrial television broadcasting from the current DVB–T standard to a more spectrum-efficient transmission technology, DVB–T2/HEVC, was implemented in the Czech Republic, and the auction process for 5G has been already finalised by the Czech Telecommunication Office and mobile operators were awarded by the allocation of radio frequencies.

Further, in the 2018 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending the Audio-visual Media Services Directive in view of changing market realities was adopted. The adopted amendments to the Audio-visual Media Services Directive introduce greater flexibility for the linear TV broadcasters in respect of the timing of the advertising.

The amendments stipulate that where the member states require that the audio-visual media service providers within their jurisdiction financially contribute towards the production of European works (European works are defined in the Audio-visual Media Services Directive and include, inter alia, works originating in the member states), they may also require that media service providers targeting audiences in their territories but established in other member states make such financial contributions, which shall be proportionate and non-discriminatory.

In addition, pursuant to the amendments, member states shall ensure that media service providers of on-demand audio-visual media services under their jurisdiction secure at least a 30 per cent share of European works in their catalogues and ensure the promotion of those works.

The amendments also stipulate that product placement shall be allowed in all audio-visual media services, except in news and current affairs programmes, consumer affairs programmes, religious programmes and children's programmes and set out specific requirements for programmes that contain product placement.

The member states were required to bring into force the laws, regulations and administrative provisions necessary to comply with the aforementioned Directive (EU) 2018/1808 by 19 September 2020. However, the Czech Republic is still in the process of implementing Directive (EU) 2018/1808.

Currently, discussions are being held relating to the simplifying of certain notarial processes in response to covid-19 pandemic.

WHITE & CASE

Jan Andruško
jan.andrusko@whitecase.com

Na příkopě 854/14
Nové Město
110 00 Praha 1
Czech Republic
Tel: +420 255 771 225
www.whitecase.com

France

Nathalie Nègre-Eveillard, Bertrand Liard and Clara Hainsdorf

White & Case LLP

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

1 What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

While foreign investment in France is generally not subject to restrictions, technology M&A transactions may fall under the scope of identified 'sensitive sectors' for which a prior authorisation by the French Ministry of Economy is required. Under current legislation (following recent foreign investment reforms), these sensitive sectors include:

- electronic communication services and networks;
- certain dual-use goods and technologies;
- encryption and decryption systems for digital applications (cryptology);
- interception, detection of correspondence or conversations;
- security audits and certification of IT systems or provision of similar services;
- capture of computer data;
- security of information systems;
- space operations;
- electronic systems used in public security missions;
- research and development activities in cybersecurity;
- artificial intelligence;
- robotics;
- additive manufacturing and semiconductors; and
- sensitive data storage.

Should the target company or target asset be active in a 'sensitive sector', the prior clearance of the French Ministry of Economy is required as a condition precedent for the following three types of transactions:

- the acquisition, directly or indirectly, of a controlling interest in a French company (a share deal);
- the acquisition of all or part of a branch of activity of a French company (an asset deal); and
- the acquisition of 25 per cent or more of the share capital of a French company, where the investor comes from a non-EU or non-EEA country).
  - For French listed companies only this threshold was lowered to 10 per cent until the end of 2020.

Other regulatory approvals may also apply in relation to specific regulated technology activities such as encryption, the import and export of which must either be notified to or authorised by the French authorities, depending on the level of encryption.

Government rights

2 Are there government march-in or step-in rights with respect to certain categories of technologies?

Investment by a foreign investor in specific technology businesses or assets may require prior clearance by the French Ministry of Economy.

In addition, the French Ministry of Defence has a right of expropriation over inventions and semiconductors for national defence purposes. In particular, the French state is allowed to expropriate whole or part of an invention for national defence purposes. This rule applies to patented inventions or inventions for which a patent application has been filed.

Legal assets

3 How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

Intellectual property rights can be assigned alone or as part of an ongoing business (an asset deal) or indirectly through the sale of the company holding said IP rights (a share deal).

When assigned alone or as part of an asset deal, trademarks, patents, semiconductors and denominations of origin must be assigned in writing. To be enforceable against third parties, patent, semiconductors and trademark assignments must be published in the relevant IP register, which can be at a national, European Union or international level, depending on the nature of the IP right. Although the French Intellectual Property Code identifies only certain types of copyright that must be assigned in writing, it is recommended that any type of copyright be assigned through a written instrument and that such assignment be as detailed as possible, including in terms of scope, purpose, territory and duration. In France, since software falls under copyright protection, the assignment of software follows the aforementioned copyright assignment rules. There is no mandatory obligation to assign domain names in writing, but it is recommended that they be assigned through a written instrument for evidence and enforceability purposes.

Databases are either copyright-protected (in which case the foregoing copyright assignment rules shall apply) or not, in which case, it is only recommended that they be assigned in writing. For those databases that contain personal data, it is crucial to ensure that such databases are compliant with relevant data protection legislation. Failure to comply may result in the cancellation of the sale or transfer of such illicit databases. In a landmark decision, in 2013, before the EU General Data Protection Regulation No. 2016/678 (GDPR) entered into force on 25 May 2018, when prior formalities were still required to be followed to process personal data, French courts ruled that a database that had not been reported to the French Data Protection Authority was illicit and thus could not be validly sold.

When the assignment takes place indirectly as part of a share deal, there are no specific formalities that need to be followed to ensure proper conveyance of the IP assets. The buyer should, however, ensure that the correct name of the IP rights holder is recorded in the relevant IP register so that such rights are enforceable against third parties.

To protect their technology or know-how, many companies prefer to keep their IP assets strictly confidential and elect not to file an application to register those IP assets. Instead, the companies will enter into non-disclosure agreements that allow them to better control the dissemination of such confidential and competitive information.

DUE DILIGENCE

Typical areas

4 What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

A potential investor or buyer usually carries out searches in publicly available IP databases (eg, INPI for French IP registrations, OAMI for EU IP registrations, or the World Intellectual Property Organization for international registrations) to verify the accuracy of the IP-related information provided by the target company. The findings of the searches usually include the name of the registered owner, the dates of registration and potential expiration, and the existence of any registered licence or security interest or any other potential type of restraint (such as limited class of products or services for trademarks, or non-payment of the renewal fee in a given country for a patent).

Private databases (ie, databases requiring subscription fees) may give additional relevant information, including the existence of any past or pending litigation involving the target company as a claimant or a defendant, or involving the target company's IP assets.

In some cases, such IP databases may also allow the identification of any prior or posterior IP rights owned by third parties, which could constitute an obstacle to the use by the target company (and the potential buyer post-closing) of its IP assets.

With respect to data protection, before the entry into force of the GDPR, the data protection authorities often provided for the list of formalities to be carried out by companies on their respective websites. Even though the GDPR no longer requires formalities to be carried out (since data controllers and processors must keep a register of their data protection activities), such information may still be relevant to assess the target company's compliance for the period before 25 May 2018.

Customary searches

5 What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

A potential investor or buyer usually carries out searches in publicly available IP databases (eg, INPI for French IP registrations, OAMI for EU IP registrations, or the World Intellectual Property Organization for international registrations) to verify the accuracy of the IP-related information provided by the target company. The findings of the searches usually include the name of the registered owner, the dates of registration and potential expiration, and the existence of any registered licence or security interest or any other potential type of restraint (such as limited class of products or services for trademarks, or non-payment of the renewal fee in a given country for a patent).

Private databases (ie, databases requiring subscription fees) may give additional relevant information, including the existence of any past or pending litigation involving the target company as a claimant or a defendant, or involving the target company's IP assets.

In some cases, such IP databases may also allow the identification of any prior or posterior IP rights owned by third parties, which could constitute an obstacle to the use by the target company (and the potential buyer post-closing) of its IP assets.

With respect to data protection, before the entry into force of the GDPR, the data protection authorities often provided for the list of formalities to be carried out by companies on their respective websites. Even though the GDPR no longer requires formalities to be carried out (since data controllers and processors must keep a register of their data protection activities), such information may still be relevant to assess the target company's compliance for the period before 25 May 2018.

Registrable intellectual property

6 What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

Not all types of intellectual property are registrable in France; trademarks, patents, SPCs, utility models, plant variety right, designs and semiconductors are. In contrast to common law countries, France does not provide for registration of author's rights (equivalent of copyrights in the United States).

Software is not registrable. However, source codes may be held in escrow by a third party, such as a public notary or an agency dedicated to software (eg, the APP Agency for the Protection of Programs).

Acquirers will usually need to be provided with the list of intellectual property owned or used by the target company or necessary to run the target company's business on a stand-alone basis. This is particularly important in respect of non-registrable intellectual property since it cannot be found, traced or verified on public databases. The assessment of the nature of non-registrable intellectual property that the target company owns or uses, and of potential associated restraints, can be conducted by reviewing the target company's rights and obligations provided under related contracts.

Due diligence undertaken with respect to registered IP assets include verification of the registered owner's name, the dates of registration and potential expiration, the existence of any registered licence or security interest, or any other potential type of restraint (such as limited class of products or services for trademarks, non-payment of the renewal fee in a given country for a patent, etc). For patents, due diligence may also include verification whether the title is opposed before the EPO or the French PTO.

Liens

7 Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

Yes, specific liens and security interests can be granted on IP rights (eg, trademarks, patents, movies, designs, domain names, software and databases). For unregistered IP rights (such as domain names, software and databases), since there is no legal provision specifically relating to the grant of security interests thereon, it is important to identify the register or the database on which the lien or security interest should be recorded and how to ensure that the lien can be enforced against third parties. Intellectual property rights can also be part of the liens and security interests taken on the tangible and intangible assets of the grantor.

Employee IP due diligence

8 | What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

When intellectual property is developed or created by an employee or a contractor, it is important to ensure that the rights in such intellectual property are vested in the target company. Patentable inventions that are developed by employees as part of their employment and during the performance of their duties are automatically assigned to the employer which must pay additional compensation to the employee for such assignment. Those patentable inventions that are developed by employees outside the scope of their employment but using resources provided by the employer belong to the employee; the employer may, however, ask to be assigned ownership in consideration of a fair price. In this respect, it is important to check whether there is an IP assignment clause associated with an appropriate supplementary remuneration policy. Inventions that are developed by employees outside the scope of their employment using their own resources belong to the employee (article L 611–7 of the French Intellectual Property Code). Software created by employees during the scope of their employment automatically belong to the employer unless the employment agreement provides otherwise (article L 113–9 of the French Intellectual Property Code).

Special attention should be paid to trainee contracts: in the absence of an assignment clause, trainees remain owners of the inventions and software they develop.

All other intellectual property created by employee or contractor belong, from the beginning, to the employee or contractor and, therefore, must be expressly assigned in writing to the employer. In particular, it is recommended that copyright assignments be detailed, in particular, in respect of the scope of the economic rights to be assigned. However, assignment of economic future rights in works is not allowed.

Transferring licensed intellectual property

9 | Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

Transfer or assignment of licensed intellectual property and technology must be registered on the relevant IP register to become enforceable against third parties. In practice, non-exclusive licences are not registered. Depending on the terms of the licence agreement, consent of the licensee may be required for the transfer or assignment of the licensed IP and technology. Indeed, such a transfer will most likely imply the transfer or assignment of the licence itself.

Software due diligence

10 | What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

When software is a key asset of the transaction, specific software due diligence will help with assessing the rights and obligations of the target company associated with such software. The following due diligence is typically undertaken as part of this software audit:

- identifying whether the software owned or used by the target company is proprietary or open source-based and who actually developed the source code (the target company's employees or outside contractors);
- verifying that all of the IP rights in the software are vested in the target company;
- identifying any open source software, including open source software used to develop the target company's software (eg, Apache) and associated licence terms, as those licence terms may apply to the software into which open source components have been integrated (contamination effect);
- detecting vulnerabilities of the software components or those components that are not in use, are slowing the software operation or need to be updated or upgraded; and
- assessing whether the software used by the target company is the most efficient and reliable software for the target company.

It is not customary for targets to provide scans for third-party or open source code.

Other due diligence

11 | What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

The legal framework with respect to special or emerging technologies is itself emerging or non-existent. Additional areas of due diligence undertaken or unique legal considerations with respect to such technologies focus on the following key legal issues:

- for artificial intelligence, whether the software performs tasks that are regulated (eg, providing legal or financial advice);
- for internet of things and autonomous driving, personal data and liability; and
- for big data, on security and personal data, especially focusing on how the system has taken into account the purpose limitation enshrined in the GDPR.

PURCHASE AGREEMENT

Representations and warranties

12 | In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

As technology is of the essence in such transactions, purchasers usually expect to be able to perform extensive technical and legal due diligence on the underlying technology and to obtain a comprehensive set of confirmatory representations and warranties in relation to IP or technology-related matters. The insertion of such IP representations and warranties is generally market practice, although their scope, qualifiers and limitations are negotiated a case-by-case basis.

The IP representations and warranties in technology M&A transactions will typically cover the following aspects (without limitation):

- legal title to the owned registered and unregistered intellectual property;
- no third-party rights;
- payment of royalties and renewal fees;
- proper recording in IP registries;
- past, ongoing or threatened IP disputes;
- investigation by competent governmental authorities;
- no infringement of third-party rights;
- disclosure, existence and validity of third-party licences necessary to run the business;
- absence of change of control or other third-party approvals required;
- compliance with IP-related contracts (such as licences, cooperation or research and development agreements) and data privacy laws; and
- compliance with legislation on employee invention.

Specific disclosures regarding the use of open source software and the absence of software defects is also a customary ask in relation to software-based businesses.

In addition, with the General Data Protection Regulation (GDPR) coming into force and despite French data protection being in existence for 40 years, it is now recommended to include detailed representations on personal data mirroring the various obligations incumbent to data controllers and processors under the GDPR.

In any case, it is important that those representations and warranties be tailored to address the key value items of the acquired businesses or assets, including, where possible, the input from technical experts.

Customary ancillary agreements

13 What types of ancillary agreements are customary in a carveout or asset sale?

The types of ancillary agreements will largely vary depending on the specific features of each transaction. They will generally aim at addressing the status of IP-related assets or contracts with a shared use or dependencies between the disposed business and the seller group organisation.

When certain IP or technology assets or contracts are shared between the disposed business and other activities of the seller, the parties will seek to negotiate appropriate cross-licence agreements, transitional trademark agreements, trademark coexistence agreements, or joint development or cooperation agreements. Ancillary agreements may also include IT transition services agreements and appropriate service level agreements whereby the seller group continues to provide IT services (ie, IT infrastructure or applications) to the disposed business or to the purchaser for a temporary, and usually short-term, period. In such a case, parties will have to discuss the preparation, project management and implementation of an appropriate transition plan and the allocation of the related responsibilities and costs.

It is generally in the interest of both parties to start discussions on the nature and scope of the ancillary agreements as early as is practical in the M&A process as those matters usually require input from legal, financial and operating teams on both sides. In addition, with the increasing influence of the Organisation for Economic Co-operation and Development's base erosion and profit shifting principles (notably regarding transfer pricing and valuation of intangibles), we have seen more in-depth discussions in relation to the pricing of such agreements, and their impact on the overall valuation of the transaction.

Wrong-pockets covenants and further assurance clauses are also commonly included in the acquisition documents to address potential misallocation of IP assets or specific post-closing formalities in enforcing the transfer of IP assets.

Conditions and covenants

14 What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

The acquisition documents usually include specific pre- and post-closing covenants in relation to tech-related matters. For instance, to preserve the substance and value of the acquired assets or business, acquirers will typically insert specific restrictions during the period from signing to closing to prevent the seller from disposing material IP assets, licensing IP assets out of the ordinary course of business, or settling or initiating material IP litigation, in each case without the prior consent of the acquirer. To the extent that third parties' consents are required to transfer identified assets or contracts, the seller may also be requested to seek such consents or to cooperate with the purchaser in this respect. In addition, when the acquirer's due diligence has pointed out specific IP issues that can be remedied, acquirers will generally request the seller to fix those issues at its cost, for instance, by carrying out specific registration formalities with IP offices, renewing trademarks or patent registrations, entering into IP or invention assignment agreements or ensuring compliance with the GDPR. In certain transactions, the scope of the seller's post-closing non-compete covenant can be delineated by reference to the use of a certain type or family of technology.

Survival period

15 Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

While business representations usually survive for an 18- to 24-month period, acquirers in technology M&A transactions tend to negotiate a longer survival period for IP warranties, which may last up to three to five years after the closing, depending on deal-specific features.

Breach of representations and warranties

16 Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

It is a common feature of the French market for IP representations and warranties to be treated as part of the business warranties and to be generally subject to the same aggregate liability cap (expressed either as an absolute figure or as a percentage of the purchase price). However, in recent years, acquirers in a highly competitive tech M&A market have been pressed to lower the general liability cap applicable to business warranties – from 15 to 30 per cent of the purchase price down to 10 per cent, especially when no red flags have emerged from due diligence. In this context, we have seen an increasing number of technology deals where acquirers have pushed to get either a specific cap, or an uplift of the general liability cap, with respect to breaches of IP warranties or data privacy regulations.

17 Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

The IP warranties will usually be subject to the same financial limitations as the other business warranties. By exception, where there are material IP issues, the acquirer may seek specific indemnities for the seller to cover such matters. In such a case, it is usual that all or part of the general limitations (such as de minimis, baskets or deductible) be carved out for the purpose of such specific indemnities or, alternatively, that the parties negotiate a specific set of financial limitations in relation to such specific indemnities.

Indemnities

18 Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

Specific indemnities are not a common feature in the French M&A market, unless they are used to cover specific known issues or circumstances identified through due diligence or disclosure (eg, an ongoing or threatened IP litigation or a known non-compliance related to data security or privacy matters). In such a case, the acquirer will usually be prevented from bringing a warranty claim (as it had knowledge of the issue) but may seek a specific indemnity from the seller to be held harmless from the related liabilities. Similarly, if there have been past technical incidents affecting the disposed business, the acquirer may request the seller to assume the liabilities arising out of such incidents.

Walk rights

19 As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

It is common in France that the seller's representations and warranties be made both at signing and at closing of the transaction and that the same standard (including carve-outs or qualifiers) apply at both times. However, unlike other jurisdictions, it is more the exception than the rule that such bring-down of the warranties be set as a closing condition.

If the specific negotiation context allows for it, the parties might seek to negotiate limited walk rights, for instance, upon the occurrence of extreme events affecting core disposed technologies or IP rights. This may be the case if new events occur during the interim period that would cause a breach of the IP warranties consuming all, or most of, the warranty cap or preventing the continued operation of the disposed business or asset (eg, termination of a core IP licence).

UPDATES AND TRENDS

Key developments of the past year

20 What were the key cases, decisions, judgments and policy and legislative developments of the past year?

Decree No. 2020-15, in implementation of the PACTE Law, extended the term of protection of utility models from six to 10 years. In addition, utility models applications can now be converted into patent applications.

Decree No. 2020-225, also implementing the PACTE Law, allows opposition proceedings against French patents before the French Patent Office.

WHITE & CASE

Nathalie Nègre-Eveillard
nnegre@whitecase.com

Bertrand Liard
bliard@whitecase.com

Clara Hainsdorf
chainsdorf@whitecase.com

19, Place Vendôme
75001, Paris
France
Tel: +33 1 55 04 15 15
Fax: +33 1 55 04 15 16
www.whitecase.com

Germany

Tobias Heinrich, Jost Kotthoff and Mathias Bogusch

White & Case LLP

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

1 What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

When considering German laws and regulations implicated in technology M&A transactions, one may distinguish between foreign direct investment (FDI) restrictions that generally apply in the event of a 'probable impediment' to national security and certain overlapping rules applicable to regulated industries.

Foreign direct investment rules

Pursuant to the German Foreign Trade and Payments Act (AWG) and the German Foreign Trade and Payments Ordinance (AWV), the German Federal Ministry for Economic Affairs and Energy (BMWi) is entitled to review inbound transactions by foreign investors based outside the European Union or the European Free Trade Association (EFTA). The BMWi may prohibit or restrict an acquisition should it be deemed to pose a probable impediment to the 'public order or security' of Germany.

The German rules distinguish between a sector-specific review that applies to certain sensitive industries and a cross-sectoral review applying for all other industries. Both types of review apply irrespective of the size or enterprise value of the business. The BMWi is entitled to review all acquisitions, whether by way of asset or share deal, business combination, joint venture and other types of equity investment.

The scope of the sector-specific review includes arms and military equipment as well as encryption technologies and other key defence technologies, such as reconnaissance, sensor and protection technology or technology based on restricted IP. The sector-specific review applies to direct or indirect acquisitions of any non-German investor reaching or exceeding 10 per cent of the target's voting rights.

The cross-sectoral review generally applies at a starting threshold of 25 per cent of voting rights acquired by a non-EU/EFTA investor unless the target is engaged in sectors identified by the AWV as particularly sensitive, in which case a 10 or a 20 per cent threshold applies, subject to the specific sector and activities involved.

An intervention by the BMWi as part of the cross-sectoral review requires a probable impediment to public policy or security. Whether a review is mandatory or voluntary further depends on the target's business activities. The latest AWV amendment passed in early 2021 addresses 16 new critical activities in addition to the list of 11 target activities that have already been triggering filing requirements and standstill obligations for the respective acquirer. Based on these rules, the review is mandatory if a non-EU/EFTA investor acquires 10 per cent or more of a domestic target that:

- operates 'critical infrastructure' (as legally defined in great detail);
- develops and modifies software specifically for such 'critical infrastructure';
- has been authorised to carry out organisational measures pursuant to the Telecommunications Act or produces or has produced the technical equipment used for implementing statutory measures to monitor telecommunications and has knowledge about this technology;
- provides cloud computing services and such infrastructure;
- holds a licence for providing telematics infrastructure components or services;
- is a company of the media industry which contributes to the formation of public opinion via broadcasting, telemedia or printed products, and is characterised by particular topicality and breadth of impact; or
- provides services which are needed to ensure the trouble-free operation and functioning of the state communication infrastructure.

In addition to the above, the German BMWi has recently introduced a list of 20 mainly technology-related activities where a mandatory filing requirement is triggered when a voting right threshold of 20 percent is acquired by the investor. Such list covers, inter alia, the acquisition of companies operating in the healthcare sector, working with critical raw materials or relevant for the security of food supply. The list further addresses critical technological activities such as:

- remote earth sensing equipment (satellites);
- artificial intelligence systems for specific purposes;
- automated driving and aviation;
- industrial robotics for adverse conditions;
- semiconductor products and necessary equipment (but arguably not input material);
- cybersecurity;
- certain aviation and aerospace activities;
- nuclear technology;
- quantum technology;
- additive manufacturing (ceramics/metal);
- network equipment;
- smart metering;
- personnel with knowledge on federal IT infrastructure; and
- products based on restricted IP (eg, for nuclear or crypto technology or the production of banknotes, etc).

Furthermore, the recent AWV amendment includes important clarifications regarding the acquisition of additional shareholdings after the initial threshold has been reached. In particular, the new AWV includes additional thresholds for additional mandatory filings at 20 per cent (in case the initial threshold was 10 per cent), 25, 40, 50 and 75 per cent. Whenever the next threshold is reached, an additional filing is required (including standstill and criminal sanctions). In addition, the new AWV codifies the practice of including reporting obligations for any additional acquisitions (irrespective of the new thresholds) in mitigation agreements.

Regarding the calculation of voting rights, the BMWi takes a broad view and looks at all entities in the entire acquisition chain from the direct acquirer to the ultimate parent and to shareholders, such as limited partners, also covering cases of 'atypical' control. In contrast to the sector-specific review, which is applicable to all foreign buyers, the general review process only applies to non-EU or non-EFTA-based investors, unless there are indications of abuse or a transaction circumventing FDI control rules.

For all investments for which the AWV stipulates a notification obligation, the underlying agreement will be provisionally void until the clearance has been, or is deemed to be, issued. If there is no notification obligation but uncertainty regarding the scope of the transaction, foreign investors can decide to initiate the review process by submitting an application to the BMWi for a no-objection certificate to obtain legal certainty for a transaction.

Recent acquisitions have shown that the BMWi has become more sensitive to acquisitions by non-EU or non-EFTA investors, especially in the technology sector. Both European and German export control restrictions may also impact M&A transactions in cases where the acquirer is considering exporting technology (including intellectual property, know-how and software) outside Germany to facilitate integration with other group functions.

The German rules are now aligned with the EU Screening Regulation that introduced a European cooperation mechanism for FDI control when it came into force in October 2020. The pending revision of EU Dual-Use Regulation may require additional revisions of the list of critical target activities.

Sector-specific rules applicable to media, broadcasting and fintech

To provide broadcasting services in Germany, as regulated under the German Federal Broadcasting Treaty, a media provider must obtain permission from either the Commission for Approval and Control at the federal government level or the state media authority at the state government level. The Federal Broadcasting Treaty applies to the provision of broadcasting services in the form of linear information and communication services in picture or sound via radio frequencies, including digital information and communication services, such as those used by live stream providers (eg, Twitch or YouTube). In addition, acquisitions (including certain minority investments) of a media or broadcasting company providing services in Germany are subject to the prior approval of the relevant media authority, subject to the provider operating on a state or federal level. In the absence of such approval, the relevant authority may revoke the broadcasting licence previously granted to the provider.

Certain technology business models within the financial industry (such as fintech and insurtech) may constitute regulated activities, the acquisition of which is subject to an ownership control procedure. As part of such proceedings, the acquirer's creditworthiness and financial soundness will be accessed by the German Federal Financial Supervisory Authority (BaFin). In the case of the acquisition of a majority stake, the future business plan is subject to review by BaFin as well. Even if the target considers itself as unregulated, a buyer should in any event perform its own analysis of whether a regulatory licence is required at present or upon the business model advancing further to avoid unforeseen regulatory issues.

Government rights

2 | Are there government march-in or step-in rights with respect to certain categories of technologies?

Under German law, regimes exist that lead to a result broadly comparable to the exercise of government march-in or step-in rights under the Bayh–Dole Act, which affects government-funded research projects in the United States.

In respect of patents, competent courts can, under certain conditions, grant a 'compulsory' licence to commercially exploit a patent if public interest demands such licence. If a patent owner cannot exploit its invention because of a pre-existing patent, the owner of the newer patent may further be entitled to be granted a compulsory licence in and to the pre-existing patent. Similar rules apply to utility models and plant varieties.

Legal assets

3 | How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

Under German law, the number of IP rights affording absolute protection towards all is limited to those IP rights codified in specific acts.

In general, German IP rights other than copyright (industrial property rights) can be transferred by an agreement between the transferor and the transferee without any formal requirements. It is recommended and common, though, to document a transfer of industrial property rights in a written instrument. For the transfer of supranational applications or IP rights, sometimes, a written form is required (eg, transfer of a European patent application under the European Patent Convention and transfer of an EU trademark).

Copyright itself cannot be transferred under German law because of the author's moral rights. The exploitation of a copyrighted work requires a licence, which can go through multiple tiers, stemming from the author's principal exploitation rights.

Under German law, domain names as such are not considered an IP right with the meaning set forth above. The registrar operating the German country top-level domain '.de' (DeNIC eG) in its general terms and conditions and its procedural rules do not envisage a transfer of a domain name as such. Instead, it only envisages a termination of the contract for the registration of the relevant domain name between the current holder of the domain name with the subsequent entering into a new contract for the registration of the relevant domain name with the future holder.

Know-how is also not protected as an IP right within the meaning set forth above under German law. Hence, an in rem transfer of rights in know-how is not possible.

DUE DILIGENCE

Typical areas

4 | What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

Typical areas of intellectual property and technology due diligence undertaken in Germany with respect to technology M&A transactions include:

- identifying all registrations and applications for IP assets owned by the target and confirming the status, lien status, chain-of-title, expiration date (if applicable), scope of protection and ownership thereof;
- identifying all other IP assets (ie, unregistered intellectual property and IP assets that are not capable of registration) owned or used

by the target and confirming the ownership thereof, any restrictions thereon, and the target's scope of rights therein;
- reviewing and analysing the target's agreements with past or present employees, independent contractors and consultants with respect to the creation and ownership of IP assets and the use and disclosure of trade secrets and other confidential information;
- identifying and determining the scope of licences-in and licences-out in respect of IP rights granted by or to the target;
- reviewing and analysing all other IP-related agreements (or intellectual provisions in agreements), including research and development agreements, consulting agreements, manufacturing, supply and distribution agreements, settlement agreements, and IP licensing and assignment agreements;
- determining and analysing the target's process for IP clearance, protection and enforcement and for protecting trade secrets and confidential information;
- determining and analysing any past, present, or threatened intellectual property-related claims or disputes involving the target, such as infringement actions, cease-and-desist letters, requests for intellectual property-related indemnification, disputes with past or present employees or contractors, and claims for remuneration for the creation of intellectual property;
- reviewing and analysing the target's processes and procedures for developing software code, including identifying open source or copyleft code, reviewing source code scans and identifying third-party access to code as well as the target's processes and procedures in respect of employee inventions;
- reviewing and analysing agreements and rights with respect to information and communication technology assets and equipment;
- where the target's business is subject to regulatory requirements with regard to technology (eg, applicable to technology outsourcing in the financial industry sector), reviewing the target's compliance with such requirements;
- reviewing the target's compliance with privacy and data protection laws, contractual obligations and company policies;
- reviewing the target's compliance with company policies with respect to cybersecurity, including IT and data security;
- vetting the extent of relevant certifications and to which extent assessments, such as vulnerability scans and penetration tests, are conducted on a periodic basis;
- vetting the extent and ramifications of any privacy or breaches or security incidents; and
- determining whether and what rights to process and use personal data will be available to the buyer.

Although the due diligence process for share deals and carve-outs or asset purchases are similar, there are several key differences.

If the business to be divested is not organised in the form of separate legal entities, the assets, contracts, rights, liabilities, employees and other resources pertaining to the business will have to be carved out from existing legal entities. As part of such transactions, an additional focus of due diligence is identifying and understanding:
- what is within the scope of the transaction and what is not;
- which resources have to be and can be transferred;
- whether there are any such resources that are in shared use;
- which activities are required to separate the business; and
- which interdependencies exist between the business to be divested and the business to be retained.

Where carve-outs or asset-purchase transactions require the assignment and transfer of IP rights, the buyer should confirm that all desired IP assets may be transferred (and are properly transferred) under the applicable law. The buyer should ensure that any shared rights in intellectual property are properly allocated (usually on the basis of concepts of exclusive use or predominant use) and cross-licensed between the parties post-closing in appropriate fields of use.

If source code or data is being transferred, the right of the seller to transfer any third-party code (including open source) or third-party data (including personally identifiable information) should be properly vetted.

With respect to mergers or share acquisitions, the buyer should review material intellectual property, information and communication technology contracts to determine whether they include change of control provisions triggered by the contemplated transaction; whereas for carve-outs or asset purchases, the buyer should analyse any anti-assignment provisions triggered by the contemplated transaction. In Germany, where a contract is silent on transferability of the contract as a whole, consent by the third-party counterparty to the transfer is required.

German law also provides for transfer of assets by way of (partial) universal succession in the context of transformations under the German Transformation Act (such as statutory mergers or hive-downs). It requires a case-by-case analysis of whether assignment restrictions or change of control termination rights may have an impact in the context of such transformations.

If a carve-out or asset-purchase transaction does not include all employees relevant to the purchased IP assets or business, the buyer should perform sufficient diligence to confirm that there is no 'key person' risk, whether the seller will need to give or receive any (transitional) services, whether any information and communication technology systems or data will need to be migrated or separated, and whether the buyer will be able to use, maintain and exploit the purchased IP assets post-closing.

Customary searches

5 What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

Counsel for the buyer typically conducts:
- searches of publicly available databases (including the German Patent and Trademark Office and domain name registries) to identify and confirm the status, chain-of-title, expiration date (if applicable), scope of protection and ownership of the registered IP rights purportedly owned by the seller;
- trademark clearance and availability searches may be performed to identify potential third-party trademark rights, or 'freedom to operate' searches may be performed to identify potentially problematic patents;
- searches of websites owned by the target to analyse privacy policies, terms of service and other publicly available information regarding the target; and
- if the target is a public company, searches for public disclosures, such as annual reports.

Registrable intellectual property

6 What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

Copyright is not registrable (but authors of anonymous works can apply for registration in a separate register to extend the duration of protection). All IP rights, other than copyright, may be registered.

For IP rights that can be registered and domain names, typically register searches are conducted to assess if the target is the registered owner. Since domain name registrars, in the context of the General Data Protection Regulation (GDPR), have drastically reduced the scope of information that can be retrieved via WhoIs queries without demonstrating a legitimate interest, domain name searches in these registers may become less important going forward.

For non-registrable IP rights, review of underlying employment, development, contractor or licence agreements is important to determine their scope or the relevant rights to use and licences.

Liens

7 Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

Liens and security interests (including security assignments) can be granted on intellectual property. Liens and security interests in trademarks can be registered in Germany, but there is no obligation to do so.

Employee IP due diligence

8 What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

With respect to contractor-created IP, the underlying development or contractor agreements are reviewed for clauses addressing the allocation, transfer and licensing of the IP rights created by the contractor.

The same applies with respect to employee-created IP, it being understood that statutory law in respect of some forms of IP rights provides for legal presumptions or grants of rights regarding employee-created IP. Inventions created or conceived by employees in connection with their employment are subject to a specific regime under which the employee has to notify its employer of the invention. If the employer claims the invention, all title, right and interest is acquired by the employer. The same applies if the employer does not release the invention within a specified period of time. The employee then has the right to claim an appropriate remuneration. As part of customary due diligence, typically the processes and procedures in place at the target are reviewed and any outstanding amounts of employee inventor remuneration or any disputes in connection therewith are sought to be identified.

Transferring licensed intellectual property

9 Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

In general, the terms of a licence agreement govern whether the licence can be transferred or assigned. If the licence is not only a pure right of the licensee, but the licensee also assumes obligations under the licence, transfer of the licence requires a transfer of agreement, which requires the counterparty's consent (which may also be given in advance and is often given in advance to facilitate transfers to affiliates).

Regardless of the above, the transfer of copyright licences in general requires the consent of the copyright owner.

Software due diligence

10 What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

Software due diligence generally consists of the following steps, in no particular order:

- What kind of software is involved (eg, proprietary, self-developed, purchased or open source)?
- Who developed the software?
- Have all rights to the software been allocated or transferred to the target to allow the use of the software for the intended purpose?
- Is the scope and term of the licence appropriate for the intended purpose?
- Do the relevant software agreements contain any termination rights or change-of-control clauses that would enable the respective licensor to terminate the licence?
- For open source software and for software that includes any open source components or libraries, have these parts and the corresponding licence terms been identified accordingly?

Where software is a or the key asset, source code may be scanned by specialised providers for open source components or vulnerabilities within the source code.

Other due diligence

11 What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

In due diligence involving artificial intelligence (AI) products, the following points may be considered:

- the rights in and to the AI (ie, the software itself, and the resources and databases it is based on); and
- the ownership in IP rights for something that the AI may be able to create (current German copyright law and patent law envisages a natural person as an author).

Depending on the field of use, further specific regulations may have to be observed and compliance may have to be checked.

As regards autonomous driving, unique legal considerations include the liability for decisions taken by the autonomously driving vehicle, in particular in the case of death, bodily injury or damage to property caused by such decision.

Big data raises legal issues mainly in respect of data protection and data security compliance, where personal data is part of the big data. Key issues to be considered in this context are:

- Can valid consent of data subjects for processing of their personal data be obtained in a situation where the scope and purpose of the processing is not yet defined when the personal data is collected? and
- Do data points, which in themselves do not allow to identify a natural person, become personal data because, when taken together with other data points included in the big data, they allow such identification?

PURCHASE AGREEMENT

Representations and warranties

12 In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

In share deals, warranties with respect to intellectual property may vary widely in scope and be subject to knowledge and disclosure, but usually contain, at a minimum, the following warranties:

- the target owns (free of liens or rights of third parties) or has a valid right to use the IP rights used in its business, and the schedule listing such IP rights is true, complete and accurate;
- the target is not violating IP rights of third parties;
- there is no written claim or action pending relating to an infringement or misappropriation of IP rights of any third party;

- contracts under which IP rights are licensed to the target are valid and there are no facts known that may lead to them being or becoming invalid;
- there is proper maintenance of IP rights to ensure that the target's registered IP rights continue to be registered and all related fees have been paid when due and all necessary applications for renewal have been filed;
- the target's IP assets are sufficient to continue its business after closing as before (this is usually heavily negotiated);
- completion of the transaction does not negatively impact the target's right to use IP rights co-owned or used by the target;
- the use of IP rights is compliant with law or regulatory requirements;
- there are no (exclusive) licence agreements regarding the target's IP rights;
- no licences, premiums or other compensation are paid for the use of IP rights by the target to third parties;
- the target has all the required rights to inventions made by employees and freelancers;
- the target's IP rights have not unlawfully been obtained or used by third parties;
- IP rights owned by the target are valid, in full force and enforceable; and
- the target has implemented and maintained adequate measures to protect its business and trade secrets.

Typical warranties with respect to information technology would generally be shorter and cover:

- title in and to the target's hardware and software;
- the functionality of and absence of breakdowns for relevant IT systems;
- due maintenance for relevant IT systems (possibly including sufficiency to continue the business as before closing for a certain time period after closing);
- that IT systems are sufficiently redundant and safeguarded;
- the validity of agreements with third parties in relation to hardware or software (in particular, material or business-critical licensing, outsourcing or maintenance agreements);
- compliance with the terms of all licences in respect of open source software or any third-party software;
- there has been no disclosure of the company's source code to third parties; and
- there has been no infection by any material virus or other extraneously induced malfunction.

Typical warranties concerning data privacy commonly cover:

- compliance with data protection and privacy laws, contractual obligations, as well as internal and external (eg, concerning customers) standards and policies in the areas of data protection and cybersecurity (usually heavily negotiated);
- the existence of a compliance management system that is able to ensure the fulfilment of these requirements;
- taking adequate technical and organisational measures to protect against cyberattacks;
- the installation and use of up-to-date and effective security programmes and standards that protect sensitive data (including personal data, customer and supplier data, trade secrets and other confidential information) from unauthorised access;
- if the IT is outsourced to external IT service providers, the existence of effective agreements on the protection of data and any indemnification for damages by the service provider;
- no (ongoing) investigations, lawsuits or threats of lawsuits concerning data security or data protection issues;
- the existence of guidelines, compliance manuals and contingency plans etc, in the event of a cybersecurity breach;
- no past or present data breach or claim of such, resulting in damages, downtime, loss of or unlawful access to personal data; and
- no receipt of any written communication from any applicable authority alleging or enforcing non-compliance with any data protection law, or requesting an audit or compliance check relating to data protection law.

Considering the implementation of the General Data Protection Regulation (GDPR) and rising awareness for cybersecurity risks, there is a trend toward such warranties receiving greater attention by the parties involved in a transaction.

In asset deals, the warranties with respect to IP and technology will typically be similar to the ones for share deals with the exclusion of such warranties that relate to a liability of the entity in itself rather than a liability in connection with certain IP assets or contracts. Since, in an asset deal, IP rights need to be individually identified and transferred, the sufficiency warranty (guaranteeing that the sold IP rights are sufficient to operate the business as before closing) may be of particular importance for the acquirer in deals where whole business units (not just single assets) are acquired.

Customary ancillary agreements

13 | What types of ancillary agreements are customary in a carveout or asset sale?

Ancillary agreements customary in carve-out or asset sales include:

- short-form IP assignments that are typically executed for purposes of recording assignments;
- transitional trademark and other IP cross-licences;
- transitional services agreements;
- IT and data migration agreements; and
- agreements for the separation of IT systems and sites.

Conditions and covenants

14 | What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

Typical IP or tech-related signing or closing conditions include:

- obtaining (confirmatory) invention and IP assignments and confidentiality agreements from former and current employees and independent contractors (if such assignments were not previously obtained, are deficient, or to correct chain-of-title issues or ambiguities);
- third-party consents to change of control or assignment under material IP- or IT-related agreements with third parties or waivers of corresponding rights to terminate;
- amendments to material IP or IT contracts as may be required in order to successfully integrate the target into buyer's business; and
- settlements or releases of outstanding adverse IP claims or actions.

Covenants will typically include specific restrictions on the target's business between signing and closing to prevent a seller, among other things, from disposing material IP assets or entering into material licence agreements outside the ordinary course of business. Covenants may also include specific tasks for the seller, such as remediation measures, carrying out or renewing IP registrations or open-source remediation measures by updating or replacing software to ensure compliance with open source licences and to eliminate potential inadvertent grants of open source licences or disclosure of source code to third parties. Remediation measures may also include clean-ups of cybersecurity incidents or improvements of compliance systems relative to cybersecurity.

Conditions to closing or covenants of the seller that apply to the period after closing may include:

- transitional trademark licences for any retained trademarks and licence or cross-licence agreements for any shared intellectual property; and
- entering into ancillary agreements, including supporting the transition of the business to the buyer's IT systems.

Survival period

15 Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

In the German market, claims based on ordinary business warranties will typically survive for a period of 12 to 24 months from closing. Tech M&A transactions with material IP and technology assets will occasionally recognise longer limitation periods.

Breach of representations and warranties

16 Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

With respect to liability caps, intellectual property, information technology and data privacy warranties will typically be synchronised with other business warranties, subject to few exceptions outside competitive auctions or especially focused on the acquisition of defined IP rights. Caps frequently range from 10 to 30 per cent of the purchase price for slight negligence depending on the target's risk profile and due diligence results obtained by the acquirer. Liability caps are gradually declining owing to the increasing use of warranty and indemnity insurance where acquisition agreements tend to operate with a 'zero liability concept'. Caps also tend to be lower for transactions with a volume of more than €100 million. Against this background, buyers of technology assets, especially from the United States, are pushing increasingly for higher caps specific to intellectual property, and technology warranties where intellectual property and technology constitute the main assets of the target.

17 Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

In the German market, IP warranties will typically be subject to the same limitations as other business warranties. The same applies to warranties relative to the target's technology, cybersecurity or data privacy. If and to the extent, there are known IP risks (such as third-party claims or challenges to IP rights, change of control issues), buyers will frequently seek specific indemnities from a seller that do not apply the same type of limitations as applied for warranty breaches.

Indemnities

18 Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

Specific indemnities usually cover risks identified through due diligence or disclosure that are not yet quantified and cannot be addressed through warranty claims to the extent they are known to the purchaser.

WHITE & CASE

Tobias A Heinrich
theinrich@whitecase.com

Jost Kotthoff
jkotthoff@whitecase.com

Mathias Bogusch
mathias.bogusch@whitecase.com

Bockenheimer Landstraße 20
60323 Frankfurt am Main
Germany
Tel: +49 69 29994 1606
Fax: +49 69 29994 1444
www.whitecase.com

Typical examples include financial risks associated with ongoing IP litigation or disputes, investigations, compliance breaches or data security incidents. Indemnification will typically be requested on a dollar-for-dollar basis (ie, without de minimis thresholds, baskets or deductibles). Depending on the financial exposure associated with the risks that form the basis for the indemnity and the value the parties associate with the respective IP right or other technology asset, the parties will discuss a cap for the liability a seller is prepared to cover. Indemnities will often be associated with the request of the seller to 'hold back' in escrow part of the purchase price to ensure recoverability of the financial risk covered by the indemnity.

Walk rights

19 As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

It is fairly common that intellectual property, technology and data privacy warranties are given both at signing and closing. Having said this, 'walk away' rights for the buyer for breach of warranties and covenants are still rather uncommon (more frequently raised by US buyers) and, if applied, are usually limited to material warranty and covenant breaches or other material adverse effect type events, such as the occurrence of cyberattacks affecting the target business. A seller will perceive any walk away scenario without clear materiality qualifications as reducing transaction certainty, which makes this a heavily negotiated area for discussion when pushed by a buyer.

UPDATES AND TRENDS

Key developments of the past year

20 What were the key cases, decisions, judgments and policy and legislative developments of the past year?

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued its judgment in the *Schrems II* case, invalidating the EU–US Privacy Shield with immediate effect. The EU–US Privacy Shield was one of the most common ways to ensure and document an adequate level of data protection as required under the General Data Protection Regulation (GDPR).

While the Privacy Shield was invalidated, the CJEU declared standard contractual clauses (SCCs) were still valid for ensuring and documenting the adequacy of data protection. However, for data transfers to the United States, the CJEU ruled that SCCs alone are not sufficient to ensure an adequate level of data protection, as they only bind the contracted parties, not local authorities. Consequently, companies have to take additional measures to ensure that the required level of data protection is met, for example, by additional contractual obligations or technical measures.

Implementation of compliance with the GDPR, which is required since 25 May 2018, has been a hot topic and will remain so for years to come. This is mainly driven by drastically increased statutory fines and enforcement as well as potential group liability comparable to that under EU competition law.

Lastly, requirements resulting from the IT Security Act for operators of critical infrastructures, as well as the implementation and proper documentation of reasonable steps to protect business secrets within the requirements of the German Trade Secrets Act remain hot topics in technology M&A.

United Kingdom

Lindsey Canning, Tom Matthews and Philip Trillmich

White & Case LLP

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

1 What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

There are no particular restrictions or obligations contained in applicable intellectual property and data protection laws specific to technology M&A transactions. However, the central role of intellectual property and personal data in technology M&A transactions often means that issues surrounding the ownership, protection and exploitation of IP rights, or compliance with data protection laws, are brought into sharper relief. Key UK statutes that are, therefore, often implicated are:

- the Trade Marks Act 1994;
- the Patents Act 1977;
- the Copyright, Designs and Patents Act 1988;
- the Data Protection Act 2018 (DPA 18); and
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended from time to time) (the PECR).

Furthermore, the General Data Protection Regulation (EU) 2016/679 (the GDPR), as incorporated into domestic UK law (under the European Union (Withdrawal) Act 2018, and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019)), following the UK's departure from the EU (the UK GDPR) is also of significant importance. The UK GDPR is broadly aligned with the GDPR in terms of its substantive requirements. However, provisions concerning supervisory bodies and interactions between EU member states have been amended to reflect the fact that the UK is no longer directly subject to EU law and enforcement regimes. Powers previously held at Union level are now held by the UK's Information Commissioner.

In addition, the Network and Information Systems Regulations 2018 (which implement the EU Network and Information Systems Directive 2016/1148) may be particularly relevant in technology M&A transactions, as they set out specific cybersecurity obligations applicable to digital service providers and providers of services critical to the UK economy.

The National Security and Investment Act 2021 (NSIA) is expected to become effective from 4 January 2022. From its coming into effect, the acquisition of shares or voting rights above certain prescribed thresholds (25, 50, 75 per cent or 'control') in targets operating in seventeen 'sensitive sectors' will require prospective investors to make a mandatory notification to the newly established Investment Screening Unit within the Department of Business Energy and Industrial Strategy (BEIS) before deals can be closed. According to the draft notifiable statutory instrument set to accompany the NSIA, those sensitive sectors are set to include artificial intelligence, computing hardware, cryptographic authentication and data infrastructure. Indeed, the impact of the NSIA is already being felt in the sector as, once operational, the regime contemplates the option for the Secretary of State for Business, Energy and Industrial Strategy being afforded the option to 'call in' transactions completed after 12 November 2019 for retrospective review if those transactions are deemed to pose a potential risk to national security in the UK. Accordingly, investors with technology targets falling within the technology-relevant sensitive sector definition have been engaging with BEIS to gauge whether their deals might be vulnerable to call-in review.

The United Kingdom's export control regime may also be relevant as, under this regime, a licence is required to export certain types of technology or software that have a military use, or which have dual military and civil use and meet certain technical standards. Therefore, depending on the products of the target business, this may be a relevant due diligence item or issue to resolve for an international acquirer.

Government rights

2 Are there government march-in or step-in rights with respect to certain categories of technologies?

The Patents Act 1977 provides under section 55 that any UK government department and any person authorised in writing by a UK government department may, for the services of the Crown, use any patented product or process without the consent of the proprietor.

The UK government has similar rights to make use of any registered design for the services of the Crown without infringing the rights of the owner. There are also specific provisions allowing the Crown to use registered designs during an emergency, such as for the maintenance of supplies and services essential to the life of the community.

The obvious justification for Crown use in each case is national security; however, the Crown's powers have been held to have wider scope than this (eg, allowing importation and use of a patented drug by the National Health Service). In each case, the exercise of this right by the Crown is subject to the payment of compensation, which if not agreed, will be determined by the court.

There are no special rules for Crown use of registered trademarks or copyright.

Legal assets

3 How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

Patents

An assignment of a UK patent will only be effective if it is in writing and signed by or on behalf of the assignor (if the assignment is dated before 1 January 2005, it must also be signed by the assignee). This rule also applies to assignments of UK patent applications and rights in inventions. To effectively assign a European patent application, both assignor and assignee need to execute the assignment.

Prompt registration of an assignment with the UK Intellectual Property Office (UK IPO) is advisable because if a third party benefits from a later assignment without knowledge of a prior unregistered assignment, then that second party will be entitled to ownership of the patent or application in question; if an assignment is not registered within six months of its effective date, the assignee will not be awarded its litigation costs in any patent infringement action involving the patent before the assignment is registered (which may be a substantial amount); and if it is not registered, the assignee will not be able to benefit from all of the rights granted to the owner by statute, including rights to enforce the patent.

UK-registered trademarks

An assignment of a UK-registered trademark must be in writing, signed by or on behalf of the assignor. Again, prompt registration of the assignment is advisable for the same reasons as for UK patents.

UK-registered designs

An assignment of a UK-registered design must be in writing, signed by or on behalf of the assignor. Once again, the assignment should be registered to ensure that subsequent bona fide acquirers of the registered design who do not have notice of the earlier assignment do not take free of it and that the proprietor can exercise all statutory rights granted to the owner.

Copyrights and UK unregistered designs

An assignment of copyright or of an unregistered design right must be in writing and signed by, or on behalf of, the assignor. These rights are not registrable in the United Kingdom, so it is not possible to register any transfer of ownership in them.

Know-how and confidential information

Know-how and other confidential information are largely protected by the common law of breach of confidence. Accordingly, there is no property right in this information, so it is not capable of assignment per se. However, it is possible for the rights in and to know-how and confidential information to be transferred by way of contract.

Domain names

Although comparable to assignment, voluntary transfer of a domain name is technically a termination of the registrar's existing contract with a domain name holder for the right to use a domain name, and the creation of a new contract with a new holder for the right to use the same domain name. This transfer typically has to be in writing, signed by or on behalf of the assignor and contain billing and administrative contacts and details of the new domain name server.

DUE DILIGENCE

Typical areas

4 What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

The following intellectual property and technology due diligence is typically carried out in technology M&A transactions with a UK element:

- identifying all registered IP rights and applications for registration that are purportedly owned by the target group, and verifying that a member of the target group is the registered proprietor or applicant in respect thereof, in particular by carrying out customary proprietorship searches;
- confirming in respect of the target group's registered rights portfolio whether there:
  - have been, or are, any oppositions or challenges to the validity or ownership of these IP rights;
  - are security interests or licences registered against these IP rights; or
  - are any defects in their chain of title;
- identifying all other IP assets that are material to the target group's operations and confirming that all rights in them are either owned without encumbrance by, or are the subject of appropriate licences to, a member of the target group;
- reviewing the terms of any licences of intellectual property granted to, or by, members of the target group and assessing:
  - for licences in, the scope of the rights granted and that they are not likely to be lost as a result of the proposed transaction; and
  - for licences out, that they do not unduly restrict or fetter the operations of the target group or grant rights to third parties that could otherwise undermine the value of that intellectual property to the business;
- reviewing the target group's agreements with past or present employees, contractors and consultants to assess whether a member of the target group owns all rights in inventions and other works created by them and has imposed appropriate confidentiality obligations on them;
- assessing the target group's use of open-source software and the applicable licence terms, including reviewing source code scans, and analysing whether any such software has been deployed in such a manner as to render the target's codebase liable to be redistributed at no charge or made available on an open source basis or on other disadvantageous terms;
- reviewing and analysing all other IP-related agreements (or IP provisions in agreements), including research and development agreements, strategic alliance agreements, manufacturing, supply and distribution agreements, and settlement agreements;
- determining and analysing the target group's IP protection and enforcement policies and procedures and the measures it takes to protect valuable know-how and confidential information;
- identifying and analysing any IP-related claims or disputes in which the target group is or has been involved;
- reviewing agreements relating to the material IT systems used by the target group, including licences, support and maintenance agreements and outsourcing contracts;
- reviewing the target group's compliance with the UK GDPR and DPA 18, in particular as regards its privacy policies, appointment of data processors and cross-border data transfer arrangements;
- vetting the extent and ramifications of any personal data breaches or security incidents; and
- determining whether and what rights to use personal data will transfer to the buyer.

The above investigations are also important for any carve-out or asset-purchase transactions, together with the following additional considerations:

- As carve-outs or asset purchases necessarily involve the separate assignment of assets and contracts, it is particularly important to ensure that all IP rights that should transfer to the buyer will be effectively transferred.
- All licence and other contracts will need to be reviewed to determine whether they can be effectively assigned without the need for

counterparty consent. Under English law, to legally transfer the burden of obligations, a tripartite novation agreement is, strictly speaking, required; however, in many cases it is market practice to give notice of assignment backed up by appropriate contractual indemnities and to rely on achieving assumption of obligations through the counterparty's continued dealings with the assignee.
- Shared IP rights will also need to be properly allocated and cross-licensed between the parties after closing.
- It will also be important to consider the need for technology and knowledge transfer assistance if not all key employees will transfer.
- The purchaser should assess whether appropriate consents have been obtained or if other grounds exist to support the transfer of personal data to it and the subsequent planned use of that data in the purchaser's business.
- Invariably, a carve-out structure gives rise to the need to assess all other key technology and operational interdependencies to determine what transitional and longer-term arrangements need to be put in place to allow for effective separation of brands, IT systems, databases, research and development capabilities and manufacturing, supply and distribution networks.

Customary searches

5 What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

The buyer's counsel will usually carry out:
searches of publicly available databases maintained by the UK IPO;
searches using commercial search database facilities covering multiple jurisdictions, in each case to verify the information provided;
in the data room concerning the target group's registered IP portfolio or to identify all proprietary registered IP rights owned in relation to the target business;
depending on the transaction timetable and value of particular IP rights to the target business, searches carried out to identify:
- potential third-party trademark rights that may impact on the value of the trademark portfolio or pose issues to expansion of the business; or
- potentially problematic patents owned by third parties;
- whois searches for domain name registrant information (but note that due to data protection restrictions, registrant information is often unavailable); and
- searches of websites operated by the target group to analyse privacy policies, terms of service and other publicly available information regarding the target business (including the Information Commissioner's Office Register of Fee Payers).

Registrable intellectual property

6 What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

In the United Kingdom:
- trademarks are registrable with the UK IPO or via WIPO by designating the United Kingdom; however, it is also possible to gain unregistered rights in a trademark;
- copyrights and database rights are not registrable;
- patents are registrable with the UK IPO and registration is required for the protection of patents – this can be done by means of a UK patent application, under the Patent Corporation Treaty or by a European Patent application via the EPO designating the United Kingdom. The European Patent system is not a function of the EU and continues unaffected by Brexit;
- rights in know-how and other confidential information are not registrable;
- design rights are registrable with the UK IPO or under the Hague Agreement by designating the United Kingdom, but there is also unregistered design protection (including semiconductor topography rights as a special type of design right) that may be available (with different eligibility criteria, and with a different scope); and
- domain names are registrable with domain name registrars and registration is required. They are not, however, a personal property right but are rather more analogous to a chose in action or a benefit under a contract.

Liens

7 Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

Under English law, security interests can be taken over IP rights, with the exception of know-how. Security interests over IP rights are often granted under a 'global' debenture securing all the assets of a company and usually are in the form of a legal mortgage or a fixed or floating charge.

There is no obligation to register a charge with UK Companies House in order to perfect the relevant security interest, but failing to do so within 21 days of creation of the charge means that it is void against the liquidator, the administrator and any creditor of the company. Registration of a charge with Companies House is, therefore, highly recommended to anyone who has an interest in the charge.

A security interest taken over UK IP rights also does not need to be registered at the UK IPO for it to be perfected. However, such registration is recommended, because registering the security interest at the UK IPO constitutes notice of the charge, thus ensuring that any later acquirer of the right acquires it subject to the charge. Registration of the charge at Companies House has been held by the courts to not always constitute valid notice if the third-party purchaser could not, in its normal course of dealings, be expected to search the Companies House register.

Buyers typically conduct due diligence on security interests taken over registered UK IP rights by performing searches of the online databases maintained by the UK IPO. If the security interest has been recorded against the relevant IP right, this can be seen on the online records for that IP right. However, as recordal of the security interest is not required for it to be perfected, if the UK IPO database does not show any security interest over an IP right, that is not conclusive evidence that no security interest has been taken over it.

Further, it is not possible to record a security interest that has been taken over unregistered IP rights, as there is no register on which to record the security interest. In the case of companies registered in England and Wales, buyers typically conduct searches of the Companies House register and raise enquiries with the seller to ascertain whether security interests have been taken over the IP rights of the target group, and also ask for a warranty that the IP rights of the target group are not subject to any encumbrances.

If a financing is being paid off in connection with the contemplated transaction, the parties typically agree that any security interests securing this financing would be released at closing. If any such security interest has been recorded at the UK IPO, notice should be given to the UK IPO post-closing to remove the interest from the records of the relevant IP right.

Employee IP due diligence

8 What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

Due diligence in respect of employee-created and contractor-created intellectual property and technology first involves ascertaining the extent to which employees or contractors have been involved in the development of material intellectual property, the location where these employees or contractors are based and the terms on which they have been employed or engaged. This is because the position on first ownership of technology and inventions created or discovered by employees and contractors is a question of national law in the jurisdiction in which the work was carried out.

In the United Kingdom, employers will generally own rights in technology and inventions created or discovered by their employees in the course of their employment (absent any contractual provision to the contrary). Absent an express written assignment, the rights in any contractor-created technology or inventions will remain with the contractor (with an implied licence arguably being granted in favour of the engaging company).

Following disclosure of the relevant employment or contractor agreements, it is necessary to analyse the provisions relating to intellectual property to determine whether the target company or the employee or contractor owns the intellectual property in technology or inventions that have been created or discovered.

As a general rule, employment and contractor agreements should ideally contain the following (although the absence of certain such provisions in employment agreements may not be an issue if ownership of the relevant IP rights has automatically vested in the employer by operation of law):

- an assignment of all rights in all work products and intellectual property created by the employee or contractor (ideally, there should also be a present assignment of future rights);
- a provision obliging the employee or contractor to perform all acts and execute and deliver all documents necessary to perfect the target company's ownership of all work products and intellectual property; and
- robust confidentiality provisions governing the use and disclosure of know-how and other confidential information.

Transferring licensed intellectual property

9 Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

Under English law, licences of intellectual property or other rights are generally treated as personal to the licensee, which means that they cannot be assigned without the consent of the licensor. This is because it is thought that the choice of a particular licensee may have been central to the licensor's decision to grant a licence at all, and therefore it is appropriate that the licensee should be prevented from assigning it to a third party at will. However, to clarify this, most IP or technology licences explicitly prohibit transfers of the licence by the licensee without the consent of the licensor. Frequently, this is qualified so that transfers are permitted without consent to other companies within the same group as the licensee, which will facilitate any intra-group reorganisation that the licensee may wish to carry out. Alternatively, or in addition, licences may provide that the licensor's consent to any assignment must be not unreasonably withheld or delayed, so as to permit more flexibility by the licensee in its choice of assignee. In general, exclusive licences are more likely to contain absolute prohibitions on assignment than non-exclusive licences.

The licensor's rights to assign are usually stated to be unfettered, so that it may assign the licence to any third party on notice to the licensee, but it does not need to acquire the licensee's consent to this.

If the licence is silent as to the party's rights to assign, it is generally accepted under English law that the licensor has the right to assign the licence at will, but the licensee may only do so with the consent of the licensor. This can vary depending on the facts surrounding each case, but this is the usual position in the absence of unusual circumstances. For the avoidance of doubt (and disputes), a well-drafted licence will explicitly set out each party's rights to assign and any limits to these.

It should be noted that English law only permits the assignment of the benefit of a licence (or any other form of contract) but not the burden of it. This means that the assignee would receive the rights granted, but would not be subject to any of the obligations set out in the licence. If it is intended that the entire licence, including the burden of fulfilling the obligations under it (such as payment of a licence fee), be taken on by the assignee then the licence must be novated, rather than assigned. A novation is a tripartite contract to which each of the licensor, the existing licensee and the assignee must be a party, under which the assignee formally agrees to assume the burden of the licence, along with the benefit of it, and the licensor acknowledges that the existing licensee is released from the licence entirely.

Software due diligence

10 What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

Software due diligence typically involves:

- identifying key proprietary software, if any, of the target group and how it has been developed;
- undertaking the due diligence steps in relation to employee or contractor-created intellectual property;
- ascertaining from the target, whether any of its key proprietary software products or systems contain any software that has been licensed from third parties and reviewing any related licences;
- determining whether and how proprietary software is licensed or distributed to third parties and reviewing any standard form licence agreements, and a sample of customer agreements that have been entered into, to identify any provisions that might unduly impact the business or its value; and
- ascertaining from the target:
  - whether any open source software has been incorporated into, distributed with, or used in connection with the development of, the target group's proprietary software; and
  - the licence terms under which each piece of open source software has been used.

It is necessary to review relevant open source software licences in light of the way in which the open source software has been deployed, and how the target company's resulting proprietary software is licensed or distributed, in order to determine whether the use of that open source software raises any material issues.

In the course of due diligence for technology M&A transactions in the United Kingdom, it is not customary for target companies to provide code scans for third-party or open source software code as a matter of course. However, it is not unusual for this to occur depending on the materiality of the software code at issue, the nature of the transaction and whether any potential open source issues have been identified.

Other due diligence

11 What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

Due diligence undertaken in relation to emerging technologies, such as artificial intelligence, the internet of things, block chain, crypto currency, autonomous driving and big data is fundamentally the same, from an IP perspective, as in relation to more established technologies because the underlying rights will be the same or similar and will need to be the subject of substantially the same diligence processes.

This will include establishing the owner of the relevant IP rights (primarily copyright in the software involved, database rights in the data being processed and any patents that have been granted or applied for in relation to any of the component parts) and examining the terms of any licences that have been granted to, or by, the target in relation to any of these.

Personal data and privacy issues are central to many emerging technologies and are, therefore, of increased significance in due diligence with respect to these technologies. One of the most vital areas of any emerging technology diligence process will be to seek to establish that appropriate security measures are in place as regards the data involved, and that the rights of the relevant individuals in relation to their personal data that is being processed are being appropriately safeguarded, in compliance with applicable data protection laws (including, in the United Kingdom, the UK GDPR and the DPA 18).

Given the reliance of most emerging technologies, in particular internet of things, block chain, crypto currency and autonomous driving, on connectivity (via the internet or telecommunication networks or other connection and data exchange technologies), cybersecurity is a further particular focus of due diligence with respect to such technologies.

A further area of concern is the problematic question of liability for damages resulting from malfunctions of complex and interconnected software, networks and IT devices and, in particular, from 'decisions' made by artificial intelligence systems.

PURCHASE AGREEMENT

Representations and warranties

12 In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

Buyers in technology M&A transactions typically require a wide range of warranties for intellectual property, technology, cybersecurity and data protection, although the scope of such warranties, as well as the applicable qualifiers and limitations, will depend both on the nature of the business and on the bargaining power of the parties. Warranties in transactions that are run as auctions tend to be limited. IP warranties are usually based on a broad definition of IP rights (which also includes rights that, at least under English law, are not technically IP rights, such as rights in know-how and confidential information, rights in goodwill and to sue for passing-off and rights in or to domain names).

Key IP warranties address such matters as:

- ownership, free from encumbrances, of all IP rights purportedly owned by the target group;
- full disclosure of material IP licences (in and out), which then customarily benefit from the 'material contracts' warranties;
- lack of infringement (usually knowledge qualified) by the target business of third-party IP rights or by third parties of material target-owned intellectual property;
- no challenges to the validity or enforceability of registered intellectual property;
- ownership of all rights in employee and contractor-created materials;
- protections afforded to confidential information and the circumstances in which it has been disclosed; and
- open source software usage and lack of disclosure of the source code of proprietary software.

Key themes of IT warranties are:

- the target group's ownership of, or continued rights to use, key IT systems;
- disclosure of all material IT agreements (together with covering them with material contracts protections); and
- comfort that all IT systems are in good working order and have not suffered significant security breaches or disruption.

Privacy warranties focus on compliance with the UK GDPR and other applicable privacy laws, including as regards collection of data, appointment of processors and cross-border data transfers, and lack of regulatory investigations or third-party allegations of non-compliance.

Customary ancillary agreements

13 What types of ancillary agreements are customary in a carveout or asset sale?

Customary ancillary agreements include the following:

- Short form deeds of assignment to transfer assets (including IP rights and technology). These deeds are then used for recording assignments of registered intellectual property.
- Transitional services agreements governing continued provision of support services (such as IT or back office functions) to facilitate the transition of shared functions from the seller's group to the buyer's group or vice versa.
- IP licences, such as a transitional trademark licence to allow the buyer to rebrand in a measured way and longer-term technology licences (in either direction) addressing 'shared' intellectual property.
- Depending on the specific features of the transaction, manufacturing and supply agreements, distribution agreements, research and development agreements, joint procurement agreements and long-term service agreements.

Conditions and covenants

14 What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

In the period between signing and closing, the responsibilities imposed on the seller may include a variety of housekeeping tasks, such as:

- obtaining third-party consent to change of control or assignment of IP licences;
- amending material IP or IT contracts as may be required to successfully integrate the target into the buyer's business;
- seeking out missing documents relevant to proof of chain of title;
- the execution of assignments from contractors or consultants, where the ownership of previously developed intellectual property is not clear from the existing documentation;
- tidying up material domain name registrations to ensure that they are held in the name of a target company; and
- remediation of open source issues.

Pre-closing, there are typically obligations on the seller to continue to maintain and protect the intellectual property that is being sold, not to dispose of any material intellectual property or let it lapse, not to enter into, amend or terminate any material IP licences and not to commence or settle any IP-related litigation.

Post-closing, there are likely to be obligations on the seller to assist the buyer in perfecting title to the intellectual property being sold (such as by lodging confirmatory assignments or forms required by relevant registries to enable the registers to be updated). Post-closing exclusivity or non-compete obligations may also be required, preventing the seller from using, for example, any technology or brands forming part of the sale in a way that is likely to infringe the buyer's rights or unfairly compete with the buyer in the future.

Survival period

15 Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

There is no hard and fast rule as regards the survival of IP warranties; this will vary case by case and depend largely on the significance of intellectual property to the transaction as a whole. It is not uncommon to have the warranties identified as fundamental survive longer than the business warranties. However, IP warranties will not normally form part of the fundamental warranties. Where there is no identified set of fundamental warranties, all warranties (including those relating to intellectual property) will typically be subject to the same survival period.

Breach of representations and warranties

16 Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

Any cap on liability will be the subject of negotiation a case-by-case basis. The cap may be higher, or indeed lower, for IP warranties depending on the value and significance of the intellectual property involved and also on the level of risk that has been identified in the diligence process. For example, there may be a known possibility of patent infringement that may significantly alter the value of the intellectual property being acquired.

Typically, liability for fundamental warranties is capped at 100 per cent of the consideration and non-fundamental warranties are capped at a much lower level (eg, between 5 and 25 per cent of the total consideration).

17 Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

In general, IP warranties are treated in the same way as the wider business warranties, unless there is a particular reason as to why such treatment should differ. If there is such a reason (eg, a significant risk has been identified in due diligence) then that risk is likely to be the subject of an indemnity.

Indemnities

18 Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

In English law, contractual indemnities are generally only provided in relation to a known risk which, if it crystallised, would give rise to a substantial loss or other material damage to the target business. This most commonly arises where there have been IP infringement allegations made against the target, but no formal litigation has been commenced. Also, given that the ICO is empowered to apply a maximum penalty of: (1) £17.5 million; or (2) 4 per cent of worldwide turnover (whichever is higher), and that there is a possibility of substantial damage to the business's reputation should any significant breach emerge, any known possibility of non-compliance is very likely to give rise to a request for an indemnity by the buyer. Liability for indemnities of any kind, including those that relate to intellectual property and data protection or cybersecurity, is often subject to a much higher cap than that which applies to the general warranties, or there may be no cap at all. Additionally, specific indemnities are not usually subject to de minimis thresholds, baskets or deductibles.

WHITE & CASE

Lindsey Canning
lindsey.canning@whitecase.com

Tom Matthews
tom.matthews@whitecase.com

Philip Trillmich
philip.trillmich@whitecase.com

5 Old Broad Street
London
EC2N 1DW
United Kingdom
Tel: +44 20 7532 1000
Fax: +44 20 7532 1001
www.whitecase.com

Walk rights

19 As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

In general, the only warranties that are likely to give rise to a right for the buyer to walk away at closing are those classified as fundamental warranties. As previously mentioned, IP warranties will not usually form part of the fundamental warranties, although this may vary depending on the significance of the intellectual property to the transaction, the length of the gap between signing and closing and any known risks associated with the intellectual property.

It would not be typical to introduce a general materiality qualifier for any warranties given at closing, but rather the original signing warranties would be repeated on the same basis as they were given originally.

UPDATES AND TRENDS

Key developments of the past year

20 What were the key cases, decisions, judgments and policy and legislative developments of the past year?

This last year has seen the end of the End of the Brexit Transitional Period and the passing of the Implementation Period Completion Day on

31 December 2020. From this date, certain Retained EU Laws continue to apply to the UK.

From an IP perspective, generally, holders of EU trademarks, registered community designs and community plant variety rights registered or granted before IP Completion Day will automatically become holders of comparable IP rights in the UK.

Trademarks

For any EUTM already granted and in force as of the IP Completion Day (31 December 2020), the UK IPO automatically granted an equivalent UK national trademark whereby the priority date filing date and renewal date of the EU registration are retained for such UK equivalent trademark. This registration was automatic and no fees were payable. Some holders of EUTMs may therefore now also have separate UK trademarks that they were not specifically aware of. Any EUTMs that were pending as of 31 December 2021, need to be filed as UK applications by 30 September 2021 in order to retain the same filing priority as the original EUTM. This conversion process is important as of the IP Completion Date, EUTMs are no longer effective in the UK.

Registered designs

Similarly, Registered Community Designs (RCDs) ceased to have effect or be enforceable in the UK after the IP Completion Date. Such EU RCDs were therefore automatically duplicated at no extra cost as an equivalent UK-registered design. These UK rights have the same application, registration and priority dates as the equivalent RCD. As with trademarks, RCDs that were pending registration on 31 December have the same nine-month period during which a UK design right can be registered, using the EU filing and priority dates.

Unregistered Community designs

Unregistered designs that came into being before 31 December 2020 have remained effective for the completion of the rest of their three-year term.

United States

Arlene Arin Hahn and Neeta Sahadev

White & Case LLP

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

1 What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

In the United States, the primary IP federal statutes implicated by technology M&A transactions are:

- the Patent Act (35 USC section 1 et seq);
- the Copyright Act (17 USC section 101, et seq);
- the Lanham (Trademark) Act (15 USC section 1051, et seq);
- the Defend Trade Secrets Act (18 USC section 1836, et seq); and
- the Semiconductor Chip Protection (Mask Works) Act (17 USC section 901, et seq).

State statutory and common law governing trademarks, trade secrets and contractual rights (including rights under invention assignment and confidentiality agreements and licences) are also typically implicated by technology M&A transactions.

Additionally, there are numerous US federal and state statutes that govern the collection, processing, use and disclosure of data in ways that are more likely to implicate technology M&A transactions than other types of transactions, including laws pertaining to:

- electronic surveillance (eg, the federal Electronic Communications Privacy Act);
- consumer privacy (eg, the California Consumer Privacy Act);
- data about children under the age of 13 (eg, the federal Children's Online Privacy Protection Act); and
- financial technology that requires secure development processes (eg, New York State Department of Financial Services Cybersecurity Regulation).

Further, cloud service providers (including data centres) that act as third-party processors often must be contractually bound to comply with regulatory requirements of their customers, which often include the Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, the Federal Acquisition Regulations and the Defense Federal Acquisition Regulations Supplement and the Family Educational Rights and Privacy Act of 1974.

Investments in US businesses that are involved with sensitive technologies by non-US parties may be subject to review by the Committee on Foreign Investment in the United States (CFIUS). CFIUS is a Treasury Department-led committee that conducts national security reviews of foreign direct investment into the United States. The CFIUS review process was overhauled with the passing of the Foreign Investment Risk Review Modernization Act (FIRRMA), in August 2018. On 13 February 2020, the US Department of Treasury issued the final regulations that implemented FIRRMA.

In evaluating transactions accepted for review, CFIUS conducts a risk-based analysis based on certain key factors:

- threat: whether the foreign investor has the capability or intent to exploit a vulnerability or cause harm;
- vulnerability: the national security risks associated with the US target, including the sensitivity of its technologies; and
- consequence: the consequences of the combination of the threat and vulnerability.

The review process may result in transactions being suspended, blocked or subject to mitigation even after closing. Parties to a transaction may file a fast-track declaration or a voluntary notice to obtain formal clearance of a transaction and prevent CFIUS from revisiting the transaction.

Government rights

2 Are there government march-in or step-in rights with respect to certain categories of technologies?

The US government has march-in rights with respect to inventions conceived or first actually reduced to practice in the performance of work under federally funded research and development contracts with small business firms or non-profit organisations (subject inventions) under the Bayh-Dole Act (35 USC sections 200-212). Under the Bayh-Dole Act, if the contracting organisation elects to retain title to a subject invention for which it has obtained assignment, it is subject to various obligations, including granting the applicable federal agency a non-exclusive, non-transferable, irrevocable and paid-up licence to practise or have practised any subject invention throughout the world. In addition, the federal agency under whose funding agreement the subject invention was made has the right to require that the contractor, assignee or exclusive licensee to a subject invention grant a licence to a third party in any field of use. If the party refuses to do so, the federal agency may grant the licence itself. The Act specifies that the US government may exercise such march-in rights if it determines that such action is necessary under the following circumstances:

- the contractor or assignee has not taken, or is not expected to take within a reasonable time, effective steps to achieve the practical application of the subject invention in such field of use;
- to alleviate public health or safety needs not reasonably satisfied by the contractor, assignee or licensee;
- to meet requirements for public use specified in federal regulations and such requirements are not reasonably satisfied by the contractor, assignee or licensee; or
- if the agreement required by 35 USC section 204 (preference for US industry) has not been obtained or waived or because an exclusive licensee of the subject invention in the United States is in breach of its obligation thereunder to manufacture substantially in

the United States any products embodying the subject invention or produced through the use of the subject invention.

The pharmaceutical and medical device industry faces greater susceptibility to the government exercising its march-in or step-in rights, as a result of the covid-19 pandemic. Specifically, given the severity of the covid-19 pandemic, the federal government could be prompted to invoke its march-in rights if a company in question is receiving federal funding for coronavirus-related research and development, and if such company does not make the resulting technology available for production. Though the possibility looms, the federal government has still not done so, to date.

Legal assets

3 | How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

Patents

Although US patent rights are protected under federal law, legal title in patents after the initial owner or owners is generally determined under applicable state law. For patent applications filed before 16 September 2012, ownership initially vests in the named inventors. For patent applications filed on or after 16 September 2012, the original applicant is presumed to be the initial owner. Ownership of a patent or patent application is assignable by written instrument, which is governed by applicable state contract law. Under the Patent Act, any assignment, grant or conveyance of a patent shall be void as against any subsequent purchaser or mortgagee for valuable consideration, without notice, unless it is recorded in the US Patent and Trademark Office (USPTO) within three months of its date or prior to the date of such subsequent purchase or mortgage.

Copyrights

Although US copyright is also protected under federal law, legal title in copyrights after the initial owner or owners is generally determined under applicable state law. Copyright in a work initially vests in the author or authors of the work. If the work is a 'work-made-for-hire', the employer or other person for whom the work was prepared is considered the author (and unless otherwise expressly agreed in a signed written instrument, owns the copyright in the work). Ownership of a copyright may be transferred in whole or in part by any means of conveyance or by operation of law. In addition, for works other than works made for hire, any assignments or licences of copyrights executed by the author on or after 1 January 1978 (other than by will) are subject to termination under certain conditions, including the death of the author. A transfer of copyright ownership, other than by operation of law, is not valid unless in writing and signed by the owner of the rights conveyed (or duly authorised agents). Although recording of any transfer of rights is not mandatory, proper recording of a document in the US Copyright Office provides constructive notice of such transfer. Between two conflicting transfers, the one executed first will prevail if it is properly recorded within one month after its execution in the United States (or within two months if outside of the United States), or at any time before the proper recording of the later transfer. Otherwise, the later transfer prevails if it is properly recorded first, taken in good faith, for valuable consideration or on the basis of a binding promise to pay royalties and without notice of the earlier transfer.

Trademarks

The United States is a 'first to use' jurisdiction and ownership of a trademark in the United States inures in the first party to use a trademark in commerce in connection with the relevant goods or services in the relevant geographic area. Although registration is not required, trademarks can be registered federally with the USPTO (if the mark is used in interstate commerce) or with state trademark registries. Federal trademark registration on the principal register provides various benefits, including evidence of validity and ownership of a mark, the ability to prevent others from using confusingly similar marks across the United States, the right to use the registered ® symbol, and statutory remedies for federal trademark infringement claims. Assignments of trademarks must be by written, duly executed instruments and any assignment of a trademark must include the goodwill of the business in which the mark is used. Moreover, intent-to-use trademark applications cannot be assigned before a statement or amendment to allege use has been filed with the USPTO, except to a successor to the applicant's business, or portion of the business to which the mark pertains, if that business is ongoing and existing.

A trademark assignment shall be void against any subsequent purchaser for valuable consideration without notice, unless the requisite assignment information is recorded in the USPTO within three months after the date of the assignment or prior to the subsequent purchase.

Trade secrets

Under the Defend Trade Secrets Act and most state laws, the owner of a trade secret is the person or entity in whom or in which rightful legal or equitable title to, or licence in, the trade secret is reposed. Thus, the trade secret owner is the person or entity who knows the trade secret information and has taken reasonable measures to keep such information secret. Transfer of ownership of a trade secret is subject to state contract law since the assignment of a trade secret technically requires both the transfer of the knowledge of the trade secret as well as obligations of the assignor not to use or disclose (or permit the use or disclosure of) the trade secret post-assignment.

Mask works

Unlike copyrights, registration of mask works in the Copyright Office is required for protection. Ownership of a mask work originally vests in the person who created the mask work, except that if a mask work is made within the scope of a person's employment, the owner of the mask work is the person's employer. Although US mask work rights are protected under federal law, legal title in mask works after the initial owner or owners is generally determined under applicable state law. The owner of exclusive rights in a mask work may transfer all of those rights by any written instrument signed by such owner or a duly authorised agent of the owner. A mask work transfer shall be void against a subsequent transfer that is made for a valuable consideration and without notice of the first transfer unless the first transfer is recorded in the Copyright Office within three months after the date on which it is executed, but in no case later than the day before the date of such subsequent transfer.

Domain names

Domain names are typically registered with accredited registrars or through registration services. Registrants typically provide the following information when registering a domain name: the domain name, registrant name, servers assigned to the domain name, and billing, administrative and technical contacts. Domain name registrars have different procedures for transferring ownership of domain names. Typically, domain name transfers involve terminating the existing registrant's contract with the registrar and creating a new contract between the new registrant and the registrar for the right to use the domain name being transferred. Parties may enter into agreements to memorialise the conditions of the domain name transfer.

DUE DILIGENCE

Typical areas

4 What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

Typical areas of intellectual property and technology due diligence undertaken in the United States with respect to technology M&A transactions include:

- identifying all registrations, issuances and applications for IP assets owned by the target and confirming the status, lien status, chain-of-title, expiration date (if applicable), scope of protection and ownership thereof;
- identifying all other IP assets owned or used by the target and confirming the ownership thereof, any restrictions thereon, and the target's scope of rights therein;
- reviewing and analysing the target's agreements with past and present employees, contractors and consultants with respect to the creation and ownership of IP assets and the use and disclosure of trade secrets and other confidential information;
- identifying and determining the scope of inbound and outbound grants of IP rights granted by or to the target;
- reviewing and analysing all other IP-related agreements (or IP provisions in agreements), including research and development agreements, consulting agreement, manufacturing, supply and distribution agreements, settlement agreements, and IP licensing and assignment agreements;
- determining and analysing the target's process for IP clearance, protection, and enforcement and for protecting trade secrets and confidential information;
- determining and analysing any past, present, or threatened IP-related claims or disputes involving the target company, such as infringement actions, cease-and-desist letters, requests for IP-related indemnification, disputes with past and present employees or contractors, and claims for remuneration for the creation of intellectual property;
- reviewing and analysing the target's processes and procedures for developing software code, including identifying open source or copyleft code, reviewing source code scans and identifying third-party access to the code;
- requesting and analysing agreements and rights with respect to information technology (IT) rights, assets and equipment;
- reviewing the target's implementation of commercially reasonable IT programs including IT security, for known material gaps and vulnerabilities to assess potential security flaws and alignment with industry standards;
- reviewing and analysing the target's practices with regard to the collection and processing of personal data to understand exposure to privacy and data security laws;
- reviewing the target's compliance with privacy and data security laws, contractual obligations and company policies;
- vetting the extent and ramifications of any data privacy breaches or security incidents; and
- determining whether and what rights to use personal data will transfer to the buyer.

Although the due diligence process for mergers, share acquisitions, carveouts and asset purchases are similar, there are several key differences. Because carveouts and asset purchase transactions require the assignment and transfer of IP rights from the seller to the buyer, the buyer should confirm that all desired IP assets may be transferred (and are properly transferred) under applicable law. For example, intent-to-use trademark applications may only be assigned under certain circumstances and assignments of trade secrets should be coupled with the covenants of the seller not to use or disclose such trade secrets post-closing. Moreover, the buyer should ensure that any shared rights in intellectual property are properly allocated or cross-licensed between the parties post-closing.

If source code or data is being transferred, the right of seller to transfer any third-party code (including open source) or third-party data (including personally identifiable information) should be properly vetted, the buyer should confirm that its intended uses of the data are permissible, as well as whether the data was rightfully collected by the seller.

The buyer should review material IP and IT contracts to determine whether they include change of control provisions or anti-assignment provisions triggered by the contemplated transaction. In the United States, the rules governing the transferability of IP licences where a contract is silent on transferability vary by applicable state law.

If a carveout or asset purchase transaction does not include all employees or IP assets relevant to the purchased business, the buyer should perform sufficient diligence to confirm that there is no 'key man' risk, whether the seller will need to give or receive any transition services, whether any IT systems or data will need to be migrated or separated, and whether the buyer will be able to use, maintain and exploit the purchased IP assets post-closing.

Customary searches

5 What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

Counsel for the buyer typically conducts:

- searches of publicly available databases (including the US Patent and Trademark Office (USPTO), the US Copyright Office, any relevant state trademark office databases and domain name registries) to identify and confirm the status, chain-of-title, expiration date (if applicable), scope of protection and ownership of the registered intellectual property purportedly owned by the seller;
- trademark clearance and availability searches may be performed to identify potential third-party trademark rights and 'freedom to operate' searches may be performed to identify potentially problematic patents;
- Uniform Commercial Code (UCC) lien searches and searches of the USPTO and the US Copyright Office assignment databases to determine if there are any active and unreleased liens or security interests recorded against the seller's IP assets;
- searches of public US court dockets to determine whether the seller has been involved in any IP-related litigation or any litigation related to its IP assets;
- searches of websites owned by the target to analyse privacy policies, terms of service and other publicly available information regarding the target;
- searches of public US federal and state regulator websites for data breach notifications or any enforcement actions related to data protection or data security; and
- if the target is a public company, searches for public filings of material contracts and other public disclosures, such as annual reports and filings with the Securities and Exchange Commission (eg, 10Ks, 10Qs, etc).

Registrable intellectual property

6 What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

In the United States:

- patents are registrable with the USPTO and issuance of a patent is required for patent protection;
- copyrights are registrable with the US Copyright Office, but registration of a copyright is not required;
- trademarks are registrable with the USPTO and with state or local trademark offices but registration of a trademark is not required;
- trade secrets are not registrable;
- mask works are registrable with the US Copyright Office and registration is required within two years after the date on which the mask work is first commercially exploited; and
- domain names are registrable with domain name registrars and registration is required.

With respect to registerable intellectual property, the buyer should conduct the following searches:

- searches of publicly available databases (including the US Patent and Trademark Office (USPTO), the US Copyright Office, any relevant state trademark office databases and domain name registries) to identify and confirm the status, chain-of-title, expiration date (if applicable), scope of protection and ownership of the registered intellectual property purportedly owned by the seller;
- trademark clearance and availability searches may be performed to identify potential third-party trademark rights and 'freedom to operate' searches may be performed to identify potentially problematic patents;
- Uniform Commercial Code (UCC) lien searches and searches of the USPTO and the US Copyright Office assignment databases to determine if there are any active and unreleased liens or security interests recorded against the seller's IP assets;
- searches of public US court dockets to determine whether the seller has been involved in any IP-related litigation or any litigation related to its IP assets; and
- if the target is a public company, searches for public filings of material contracts and other public disclosures, such as annual reports and filings with the Securities and Exchange Commission (eg, 10Ks, 10Qs, etc).

With respect to trade secrets, know-how and other unregistered intellectual property, the buyers should confirm ownership thereof by the seller and with respect to trade secrets, that the seller has taken reasonable steps necessary to maintain the confidentiality thereof.

Liens

7 Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

Liens and security interests can be granted on IP and technology assets in the US under article 9 of the UCC (as enacted by each state and the District of Columbia), which governs security interests in 'general intangibles' (including intellectual property), unless article 9 is pre-empted by US statute, regulation or treaty.

Because the Patent Act and the Lanham (Trademark) Act do not expressly pre-empt article 9 of the UCC, US courts have generally held that security interests in US patents and patent applications and federal trademark registrations and applications (as well as other unregistered intellectual property) are perfected by the filing of a UCC-1 financing statement with the applicable state where the owner of the IP asset is located and any release or termination of such security interest would be filed with such state. It is also prudent and considered good practice to file the security agreement (and any release or termination thereof) with the USPTO to ensure notice to subsequent good faith purchasers and mortgagees. In contrast, the Copyright Act pre-empts article 9 of the UCC. Accordingly, security interests in registered US copyrights (and applications therefor) are perfected by filing security agreements with the US Copyright Office. Any release or termination thereof should similarly be filed with the US Copyright Office. Turnaround time for UCC filings can vary by state and type of submission, but can be instantaneous (for electronic filings) or may take up to 30 days (for paper forms). Turnaround time for the USPTO and US Copyright Office depends on processing lag time, but a filing receipt is typically provided within a day for electronic filings.

Buyers typically conduct due diligence on liens or security interests by performing UCC lien searches as well as searches of the USPTO and the US Copyright Office databases to determine whether there are any active and unreleased liens or security interests recorded against the target's IP assets. Buyers will also require the target to disclose, through the due diligence process, all of the liens or security interests granted against the target's IP assets, and will verify such disclosures against the results of the buyer's searches. If a financing is being paid off in connection with the contemplated transaction, the parties typically agree that any security interests securing such financing would be released at closing.

Employee IP due diligence

8 What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

The due diligence typically undertaken with respect to employee-created and contractor-created intellectual property and technology in the context of US technology M&A transactions involves analysing employment or contractor-related agreements under applicable governing law to determine whether the target company or employee or contractor owns the employee or contractor-created intellectual property, and whether such intellectual property is material to the target company. The buyer should ensure that the agreements include:

- a provision stating that all copyrightable work created by the employee or contractor is a 'work made for hire' under the Copyright Act (and in the case of a contractor, specially ordered or commissioned for use) and an assignment or waiver of all moral rights and similar rights of attribution;
- a present assignment of (and future agreement to assign) all work product and intellectual property that does not qualify as a work made for hire;
- a provision obligating the employee or contractor to cooperate to perform all acts and execute and deliver all documents necessary to effect and perfect all work products and IP ownership;
- confidentiality provisions governing the use and disclosure of trade secrets and other confidential information;
- if any trade secrets are disclosed to the employee or contractor, the whistle-blower notice required under the Defend Trade Secrets Act for agreements executed on or after 12 May 2016;
- sufficient licences under any background intellectual property owned by the employee or contractor that is used or embodied in the work product or intellectual property created by such employee or contractor; and
- representations and warranties that all work product and intellectual property is original and does not infringe, misappropriate or otherwise violate any third-party IP rights.

In addition, the laws of several states (including California) restrict the scope of employee inventions that may be subject to assignment and require that certain statutory notices be included in agreements purporting to assign employee inventions.

Transferring licensed intellectual property

9 | Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

Under US law, the express language of the applicable IP licence agreement generally governs whether the licence is assignable. If the agreement is silent or ambiguous with respect to assignability, the analysis depends on governing law, the nature of the licensed intellectual property, whether the licence is exclusive or non-exclusive, whether the contemplated transaction constitutes an assignment under applicable law, and other considerations.

Typically, if an IP licence is silent or ambiguous with respect to assignability, then US courts have generally found that, absent countervailing circumstances that would result in material adverse consequences to the licensee (eg, the licence grant is coupled with various obligations of the licensor to provide assistance or other services or where the assignee is a competitor of the licensee), the licensor has the right to assign without the licensee's consent; and the licensee does not have the right to assign without the licensor's consent.

Non-exclusive licences that are silent regarding assignability have generally been found by US courts to be non-assignable by the licensee without the licensor's consent. However, courts are split on whether exclusive licences should be treated similarly. Although several courts have treated exclusive licences in the same manner as non-exclusive licences with respect to assignability, some courts have held that exclusive licensees should have rights commensurate to the owner of the intellectual property and therefore the right to assign without consent of the licensor because exclusive licences may be considered to be transfers of all rights (particularly with respect to copyrights).

Software due diligence

10 | What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

Software due diligence typically involves:

- identifying who created the source code (ie, employees or contractors) and reviewing any agreements governing the development of such source code;
- determining whether and how the software is used, accessed, stored, licensed or distributed to third parties (including whether it is subject to any source code escrow agreements), including reviewing any agreements governing the foregoing;
- confirming the confidentiality measures undertaken to protect any proprietary code and unauthorised access thereto or disclosure thereof; and
- reviewing or vetting any open source code policies and procedures (including reviewing source code scans).

Depending on the materiality of the software code at issue, the nature of the transaction and target industry, targets may provide code scans in the course of due diligence for technology M&A transactions in the United States.

Other due diligence

11 | What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

Artificial intelligence

Artificial intelligence (AI) algorithms typically 'learn' from broad and high-quality data sets, which may be subject to copyright protection. It is important to assess whether an AI system has the right to use, access or reproduce the copyrighted works within an input data set and whether any resulting technology could, therefore, be deemed to be an unauthorised 'derivative work'. Thus, when defining the legal relationship of the parties in terms of their respective rights, compensation and responsibilities, it is essential to understand and consider the:

- training set;
- algorithm or model;
- form of the input query; and
- form of the output result.

Because AI systems may be capable of producing more complex and innovative products and services, on the one hand, it is important to consider how inventorship and authorship will be determined where intellectual property results from an AI system. For example, US courts may decline to grant patent or copyright protection to inventions or works created by AI systems (rather than by humans). On the other hand, if a target uses an AI system that makes decisions resulting in damage or harm, it is unclear how liability would be allocated. Consequently, it is important to assess and allocate the risks associated with AI assets during transactions in which AI assets are a core piece of the potentially acquired business.

Additionally, with respect to privacy and data security, due diligence undertaken with respect to AI typically includes a review of the secure development lifecycle of hardware and software, including analysing implementation of privacy and security by design and by default, as well as legal considerations that may apply when AI drives automated individual decision making, the tracking and profiling of individuals, or the re-identification of previously anonymised personal data.

Regulatory change should also be a major area of focus in the course of due diligence taken with respect to AI. The five largest financial regulators in the US and the FTC have signalled incoming new guidance that will shape how companies can use AI. Assessing the rapidly evolving regulatory frameworks around the implementation of AI will serve a critical role in buyers' risk management assessment and post-closing integration plans.

Internet of things

Internet of things (IoT) relates to connected devices – the integration of industrial machine sensors and actuators with the internet – which are capable of collecting and analysing massive amounts of data and inherently gives rise to legal concerns around notice, consent, privacy, security and discrimination. It is important to consider whether the data collected by an IoT device is personal data and, if so, whether the persons about whom such data is collected have been given sufficient notice and consented to the collection, analysis and uses thereof, and whether any of the data or systems are subject to data privacy or data security regulatory requirements (as often is the case with healthcare or financial information).

Autonomous driving or advanced driver-assisted systems

Autonomous driving or advanced driver-assisted systems (ADAS) increasingly require sophisticated high-speed data systems and rely upon AI and connected devices (ie, IoT) technology; therefore, such systems may be subject to the same legal considerations discussed above with respect to IoT and AI. Moreover, such systems incorporate numerous other types of technologies, such as global positioning systems, radio or light detecting and ranging (RADOR or LIDAR), future human-machine interfaces, telecommunications, data analytics, heads-up displays and image processing. Accordingly, purchasers should conduct thorough due diligence to ensure that ADAS technology being acquired is not infringing or misappropriating third-party IP rights.

PURCHASE AGREEMENT

Representations and warranties

12 In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

Buyers of technology companies may require extensive IP representations and warranties, including:

- scheduling of all IP registrations and pending applications, and all material IP and IT contracts (typically included as part of the 'material contracts' representation);
- sole ownership of intellectual property purported to be owned by the target and ownership or the valid right to use all other intellectual property used in the target's business, in each case, free and clear of all encumbrances (other than permitted encumbrances);
- no infringement, misappropriation or other violation of third-party IP rights by the target (this representation may be qualified by knowledge) and of the target's IP rights by any third party (this representation is typically qualified by knowledge);
- validity, enforceability and subsistence of the target's intellectual property;
- no claims or actions asserted by or against the target alleging any infringement, misappropriation or other violation of IP rights, or challenging the ownership, use, validity or enforceability of the target's intellectual property;
- reasonable efforts to protect trade secrets and other confidential information;
- due execution of invention assignment and confidentiality agreements;
- sufficiency of IP assets;
- no adverse effect on IP rights arising from the consummation of the proposed transaction;
- no outstanding governmental orders affecting the target's intellectual property;
- no contribution of resources, facilities, funding or other matters by any governmental entity, university or similar public institution; and
- no unauthorised access to or disclosure of source code, compliance with all open source and other third-party code licences, and no problematic use of copyleft or viral code.

Standard IT, data security, and data privacy representations include:

- ownership and right to use all material IT assets;
- implementation of commercially reasonable information security programmes and reasonable efforts to protect the confidentiality, integrity and availability security of IT systems owned, leased or otherwise used by the company, and to protect the confidentiality, integrity and availability of the data (including personal information) on those systems;
- compliance with privacy, data security and data protection laws (including the California Consumer Privacy Act (CCPA), California Consumer Privacy Rights Act (CPRA), Colorado Privacy Act, Virginia Consumer Data Protection Act, HIPAA, New York SHIELD Act and the General Data Protection Regulation (GDPR)), contractual obligations (such as the Payment Card Industry Data Security Standard (PCI-DSS)), and company policies;
- adequate third-party vendor privacy and data security protections, to include the flow-down of any compliance requirements (for example, use restrictions, security measures and data breach notification requirements);
- continued ability to use personal data upon closing;
- sufficiency, good working order and good working condition of IT systems;
- no disabling codes, drop-dead devices, time bombs, Trojan horses, worms, trap doors, back doors or other contaminants in the target's products or IT systems;
- implementation of reasonable disaster recovery and business continuity plans;
- no failure, security breach, material interruption or disruption, loss or unauthorised access to or use of any IT systems or any business-sensitive information or personal data; and
- no data breach notifications required or provided, and no data breach claims or inquiries made against the target.

Customary ancillary agreements

13 What types of ancillary agreements are customary in a carveout or asset sale?

Ancillary agreements that are customary in a technology or IP-focused carveout or asset sale in the United States include IP assignments, transitional licences and transition services agreements. An asset sale is typically affected by means of a bill of sale and assignment and assumption agreement for the purchased assets, which generally transfers ownership in technology, products, equipment, other personal property, real property and agreements.

To the extent that assignments of any IP registrations or applications may be affected, short-form IP assignments are typically executed for purposes of recording such assignments.

Transitional trademark licences are typically executed if the seller will retain certain marks used by or in connection with the transferred business or assets and the buyer needs a period of time post-closing to wind down use of the seller's marks and transition to other marks.

Transition (or reverse transition) services agreements are commonly entered into where the parties need time to transition functions (such as IT systems and back-office functions) from seller to buyer (or buyer to seller).

Other post-closing licence agreements may be executed if one party acquires or retains intellectual property in which the other party will continue to have rights to use post-closing. The licence may take multiple forms, depending on how the transfer of intellectual property is structured. For example, instead of acquiring intellectual property outright, the buyer may take an exclusive licence from the seller (sometimes limited to a specific field of use). Where the buyer acquires the intellectual property outright, the seller may request a licence back from the buyer (for use other than in connection with the business being sold). In addition, if the purchased IP assets are transferred based on a 'used' or 'primarily used' standard, there may be post-closing cross-licences of intellectual property between the seller and buyer.

Conditions and covenants

14 What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

Pre-closing conditions or covenants of the seller may include:

- interim operating covenants, such as:
  - prohibitions on granting any licences, covenants not to assert or other rights in intellectual property to a third party, and on abandoning any IP rights or allowing IP rights to lapse (with negotiated carveouts); and
  - prohibitions on entering into, modifying or terminating any IP- or IT-related agreement (with negotiated carveouts);
  - requirements that the target obtain and provide:
  - third-party consents to change of control or assignment under material IP- or IT-related agreements with third parties;
  - amendments to material IP or IT contracts as may be required to successfully integrate the target into the buyer's business;
  - settlements or releases of outstanding adverse IP claims or actions; and
  - termination of certain IP contracts as may be requested by the buyer (in merger and stock purchase transactions);
- open-source remediation (updating or replacing software to ensure compliance with open-source licences and to eliminate potential inadvertent grants of open-source licences to third parties); and
- obtaining invention and IP assignments and confidentiality agreements from former and current employees and contractors (if such assignments were not previously obtained, if existing assignments were deficient or to correct chain-of-title issues).

Post-closing conditions or covenants of the seller may include:
- assisting the buyer with effecting and recording short-form IP assignments with the USPTO, US Copyright Office, relevant domain name registrars and any state IP offices;
- agreeing to 'wrong pockets' obligations (eg, whereby each party agrees to promptly and without any further consideration transfer to the other party any assets that were inadvertently improperly allocated to such party);
- granting post-closing transitional trademark licence agreements for any retained trademarks and licence (or cross-licence) agreements for any shared intellectual property; and
- providing transition services to help transition the business (including to the buyer's IT systems).

Survival period

15 Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

Acquirers of tech businesses may request the ability to sue for breach of IP representations for a period following closing (eg, three to six years). While there is no statute of limitations for filing a patent infringement suit in the United States, a six-year survival period would correspond to the time period for recovering monetary damages for patent infringement. Copyright infringement suits must typically be filed within three years after the infringement claim accrues. Federal trademark law does not specify a statute of limitations for filing trademark infringement suits so the time limit varies by state. The Defend Trade Secrets Act includes a three-year statute of limitations, but state laws vary. Ultimately, the survival period for IP representations depends on negotiations between the parties.

To provide some context, for general or non-fundamental representations (eg, financial statements or litigation), the survival period may be much shorter (eg, one or two years). For tax matters, the survival period may expire 30 to 90 days following the expiration of applicable statutes of limitations. For fundamental representations (eg, title to assets in an asset deal, title to shares in a share sale or due authorisation), buyers will generally request that the survival period last indefinitely, or 30 to 90 days following the expiration of the maximum period available under applicable law.

Breach of representations and warranties

16 Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

In a technology M&A transaction, buyers may request a liability cap for the breach of IP representations that exceeds the liability cap for non-fundamental representations (in a non-technology M&A transaction, this is less common). However, this may be the subject of heavy negotiations between the parties. Note that there is a growing trend in M&A transactions (including those in the technology sector) to rely on representation and warranty insurance (R&WI) for protection against liabilities instead of relying on the traditional indemnity structure. The terms and conditions of the R&WI (including any express exclusions from coverage) and whether it will be the sole mode of recourse for the buyer against liabilities may be the subject of heavy negotiations between the parties.

17 Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

This is also typically the subject of heavy negotiation. In some cases, the cap on liabilities for breach of IP representations may be subject to the same de minimis thresholds, baskets, deductibles or other limitations on recovery applicable to non-fundamental representations, but this point will be considered together with the other negotiated points described above.

Indemnities

18 Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

The parties may include specific indemnities for matters that were disclosed or discovered in due diligence (eg, potential claims by third parties related to patent infringement or trade secret misappropriation), including in transactions where all other liabilities are otherwise covered by the R&WI. Specific indemnities are typically not subject to de minimis thresholds, baskets or deductibles, but may be subject to a negotiated liability cap (eg, the purchase price or some other agreed amount).

In an asset purchase agreement, liability for retained liabilities is typically not subject to limitations on recovery. The same is true for liabilities related to matters arising prior to closing with respect to the transferred liabilities.

Walk rights

19 As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

Buyers and sellers will negotiate the extent to which IP representations are brought down subject to materiality qualifiers at closing.

In the most buyer-friendly formulation, a buyer may require that IP representations be true and correct in all respects as of the closing (without materiality qualifiers). Sellers may view this as reducing the certainty of closing, in particular where there are more than a few days between signing and closing and so a de minimis exception is sometimes provided.

An alternative formulation is for a limited subset of the IP representations and warranties (such as sufficiency of IP assets or non-infringement) to be brought down subject to a materiality qualifier, while the other IP representations are brought down subject to a no material adverse effect qualifier.

In the most seller-friendly formulation, all of the IP representations may be brought down at closing subject to a 'no material adverse effect' qualifier. 'Material adverse effect' (MAE) is typically a heavily negotiated term in an acquisition agreement, particularly the events that would not constitute an MAE. It is an exceedingly difficult threshold to meet and effectively requires the buyer to close even if material breaches are discovered between signing and closing (as they do not meet the MAE threshold).

In 2018, in a first-of-its-kind decision, the Delaware Chancery Court ruled in *Akorn Inc v Fresenius KABI AG* that Fresenius, as the acquirer, was released from its obligation to close the underlying acquisition due to an MAE suffered by Akorn, the target company. All prior Delaware court decisions had required the acquirer to close due to failure to establish a MAE, with courts typically finding that the acquirer was simply suffering from 'buyer's remorse'. In its decision in *Akorn Inc v Fresenius KABI AG*, the Delaware Chancery Court provided useful guidance on the significant burden that acquirers must meet when attempting to terminate an acquisition on the basis of an MAE (eg, an acquirer must establish that the applicable MAE event substantially threatens the overall earnings potential of the target in a durationally significant manner). At the same time, in reviewing and discussing specific financial metrics, the Delaware Chancery Court emphasised that it was not establishing any bright-line quantitative test for determining whether a MAE had occurred. While there have been no other findings of an MAE event by a Delaware court since the *Akorn* decision, the *Akorn* decision remains a useful resource for acquirers, target companies and practitioners going forward when drafting and negotiating MAE clauses in acquisition agreements.

UPDATES AND TRENDS

Key developments of the past year

20 What were the key cases, decisions, judgments and policy and legislative developments of the past year?

2020 and 2021 have seen a number of states following California's example and enacting consumer privacy legislation. Generally, these protections will come into effect in early 2023, and include the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and an overhaul to the CCPA, the California Privacy Rights Act.

In addition, the Biden Administration has heightened its scrutiny of M&A and SPAC activity in the technology sector.

Merger antitrust

On 9 July 2021, President Joe Biden signed the Executive Order on Promoting Competition in the American Economy. The Order calls on the Federal Trade Commission (FTC) and Department of Justice (DOJ) to enforce antitrust laws vigorously, with a particular focus on healthcare markets and the technology sector. Further, the Order calls on the FTC and DOJ to recognise the laws allowing them to challenge mergers that past Administrations did not previously challenge.

For the technology sector specifically, the Order criticises alleged 'killer acquisitions' meant to eliminate potential competitive threats, and announced greater scrutiny of mergers, especially by dominant internet platforms, with a particular focus on acquisition of 'nascent competitors, serial mergers, the accumulation of data, competition by 'free' products, and the effect on user privacy'. The Order encourages the FTC to establish rules related to the surveillance and accumulation of data, unfair competition in internet marketplaces, and restrictions on using independent repairs or do-it-yourself repairs of personal devices and equipment.

The same day the Order was signed, FTC Chair Lina Khan and the acting head of the US Justice Department Antitrust Division, Richard Powers, said that they would soon launch a review of merger guidelines to determine if they are 'overly permissive'. A White House Competition Council will be established to coordinate among federal agencies and to monitor progress on the Order's directives.

SPAC Review

In the early part of 2021, Securities and Exchange Commission (SEC) officials issued a string of pronouncements concerning the risks posed by the explosion of SPAC initial public offerings. A primary SEC concern is the potential misalignment of incentives between SPAC sponsors and public shareholders. The SEC has continued to announce enforcement actions against SPACs, SPAC sponsors, SPAC CEOs and proposed SPAC business combinations for misstatements in publicly filed documents (including with respect to the target's technology and business risks). Given that SPAC activity in the M&A market is expected to continue, parties should be prepared for additional scrutiny by the SEC of statements set forth in the SPAC's SEC filings made in connection with the proposed M&A transaction.

WHITE & CASE

Arlene Arin Hahn
arlene.hahn@whitecase.com

Neeta Sahadev
neeta.sahadev@whitecase.com

1221 Avenue of the Americas
New York, NY 10020-1095
United States
Tel: +1 212 819 8200
Fax: +1 212 354 8113
www.whitecase.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-727-0