



ASIA-PACIFIC ANTITRUST REVIEW 2022

Asia-Pacific Antitrust Review 2022

Reproduced with permission from Law Business Research Ltd
This article was first published in March 2022
For further information please contact insight@globalcompetitionreview.com

Published in the United Kingdom
by Global Competition Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL
© 2022 Law Business Research Ltd
www.globalcompetitionreview.com

To subscribe please contact subscriptions@globalcompetitionreview.com

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at March 2022, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the Publisher – clare.bolton@globalcompetitionreview.com

© 2022 Law Business Research Limited

ISBN: 978-1-83862-858-1

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

Contents

OVERVIEW

Cartels and Abuse 1
Adelaide Luke, Patrick Gay and Joel Rheuben
Herbert Smith Freehills

The Intersection of Competition Law and Data Privacy in APAC..... 20
Sébastien Evrard, Connell O'Neill, Hayley Smith, Katherine Tomsett and Nick Hay
Gibson, Dunn & Crutcher LLP

Pharmaceuticals 39
Susan Jones
Gilbert + Tobin

AUSTRALIA

Overview 57
Linda Evans and Patrick Gay
Herbert Smith Freehills

CHINA

Overview 79
Yong Bai, Dayu Man and Nan Lan
Clifford Chance LLP

Merger Control..... 100
Susan Ning, Zhifeng Chai and Weimin Wu
King & Wood Mallesons

INDIA

Overview..... 114
Manas Kumar Chaudhuri, Anisha Chand, Tanveer Verma and Armaan Gupta
Khaitan & Co

Cartels..... 132
Ram Kumar Poornachandran, Shreya Singh and Dhruv Chadha
AZB & Partners

Leniency..... 153
Dinoo Muthappa and Dhruv Dikshit
Talwar Thakore & Associates

Merger Control..... 165
Avaantika Kakkar and Vijay Pratap Singh Chauhan
Cyril Amarchand Mangaldas

JAPAN

Overview..... 182
Junya Ae, Ryo Yamaguchi and Masayuki Shinoura
Baker & McKenzie (Gaikokuho Joint Enterprise)

Antitrust Litigation 197
Kentaro Hirayama
Hirayama Law Offices

Cartels..... 207
Hideto Ishida and Atsushi Yamada
Anderson Mōri & Tomotsune

Merger Control..... 223

Hideto Ishida and Takeshi Suzuki

Anderson Mōri & Tomotsune

Settlements 236

Kentaro Hirayama

Hirayama Law Offices

VIETNAM

Merger Control..... 247

Nguyen Anh Tuan, Tran Hai Thinh and Tran Hoang My

LNT & Partners

Preface

Global Competition Review is a leading source of news and insight on national and cross-border competition law and practice, with a readership that includes top international lawyers, corporate counsel, academics, economists and government agencies. GCR delivers daily news, surveys and features for its subscribers, enabling them to stay apprised of the most important developments in competition law worldwide.

Complementing our news coverage, the *Asia-Pacific Antitrust Review 2021* provides an in-depth and exclusive look at the region. Pre-eminent practitioners have written about antitrust issues in five key jurisdictions, with this edition including new chapters on merger control in China, leniency proceedings in India and a broad take on the intersection of data privacy and antitrust throughout the region. In addition, we have expanded the scope of the country overviews to encompass cartels and abuse, and pharmaceuticals.

This annual review expands its remit each year, especially as the Asia-Pacific region gains even more significance in the global antitrust landscape. It has some of the world's most developed enforcers – in Australia and Japan, for example – as well as some of the world's newest competition regimes.

The authors are, unquestionably, among the experts in their field within both their own jurisdictions and the region as a whole. Their knowledge and experience, and, in particular, their ability to contextualise both law and policy, give this report special value.

Although every effort has been made to ensure that all the matters of concern to readers are covered, competition law is a complex and fast-changing field of practice, and therefore specific legal advice should always be sought. Subscribers to Global Competition Review will receive regular updates on any changes to relevant laws during the coming year.

If you have a suggestion for a topic to cover or would like to find out how to contribute, please contact insight@globalcompetitionreview.com.

GCR thanks all of the contributors for their time and efforts.

Global Competition Review

London

March 2022

The Intersection of Competition Law and Data Privacy in APAC

Sébastien Evrard, Connell O'Neill, Hayley Smith, Katherine Tomsett and Nick Hay

Gibson, Dunn & Crutcher LLP

IN SUMMARY

This chapter explores the interplay between competition law and data privacy law in the Asia-Pacific region, covering key developments in legislation, enforcement, litigation and mergers.

DISCUSSION POINTS

- Latest developments at the intersection of competition and data privacy law in the Asia-Pacific region.
- The competing interests of competition and data privacy regimes and the issues this may cause for data handlers and enforcement agencies, in particular with respect to dual enforcement.
- The direction of travel for legal frameworks in the region to address these challenges and regulate data markets fairly and effectively.

REFERENCED IN THIS ARTICLE

- Australian Competition and Consumer Commission (ACCC)
- Competition Commission of India (CCI)
- Indonesian Competition Commission (KPPU)
- Japan Fair Trade Commission (JFTC)
- China's State Administration for Market Regulation (SAMR), Anti-Monopoly Law (AML) and Personal Information Protection Law (PIPL)
- Taiwan Fair Trade Commission (TFTC)
- India's Draft Data Protection Bill

Introduction

This contribution explores the interplay between competition law and data privacy law in the Asia-Pacific region. In an age defined by data monetisation and fierce competition for users and their valuable behavioural data among technology's biggest players, issues at the intersection of these two legal areas are coming into sharp focus. Broad regulatory enforcement against 'Big Tech' companies in China, the introduction, expansion and gradual harmonisation of data privacy regimes across the Asia-Pacific region, and the significant investment made by enforcement agencies in Asia to better understand how competition and data privacy issues interact, particularly in the context of the digital economy, are all reflective of the region's increasing cognisance of the complexities at the intersect of competition and data privacy law.

In 2021, China introduced one of the world's strictest data protection regimes, Australia began consulting on a proposal to expand its data privacy laws, and India's legislature considered its first data protection bill, which it looks likely to pass in 2022. The strengthening of data protection regimes has an obvious benefit to consumers, but it creates a risk for companies that both competition and data privacy laws will be enforced against the same conduct, such that companies could face punishment twice. Dual enforcement is not an efficient use of scarce regulatory resources; in the near future, policymakers must align on whether abuses concerning data better fit in the realm of protecting competitive markets, or protecting consumer privacy. Stricter criteria for handling personal information may also have the unintended effect of raising barriers to entry and entrenching a dominant player's position. For instance, a dominant market player may legitimately decline to share its dataset of personal information with new entrants, and regulators may be restricted from ordering a transfer of data to address the potential anticompetitive effects of a merger or an abuse of dominance.

This article considers the latest developments at the intersect of competition and data privacy law in Australia, China, India, Indonesia, South Korea, Taiwan and Japan.

Australia

Legislation

Australia's data protection regime is currently governed by the Privacy Act 1988 and associated Australian Privacy Principles (together, the Privacy Act). However, commencing in 2020, the Attorney-General is undertaking a wholesale review of the Privacy Act with a view to aligning the country's regime more closely to international standards, such as the European Union's General Data Protection Regulation

(GDPR), and reflecting recent developments in the digital economy. The review is due to conclude in 2022, and a final report and proposed amendments to the Privacy Act will be submitted to government in due course.¹

This review has been conducted concurrently with a public consultation on the exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Online Privacy Bill), which was released in October 2021. The Online Privacy Bill relevantly proposes to establish a binding privacy code for social media platforms, data brokerage services and large online platforms, in addition to expanding the enforcement options available to the regulator for non-compliance. Public submissions collected in 2021 will inform further development of the Online Privacy Bill before its introduction to Parliament in 2022.²

Market studies

The issue of competition in digital markets was hot on Australia's regulatory agenda in 2021. The Australian Competition & Consumer Commission (ACCC) conducted the Digital Advertising Services Inquiry 2020–2021, which analyses competition and efficiency in the supply of ad tech services.³ In addition, the ACCC is conducting the ongoing Digital Platform Services Inquiry 2020–2025, which examines, inter alia, 'the intensity of competition in markets for the supply of digital platform services, with particular regard to the concentration of power, the behaviour of suppliers, mergers and acquisitions, barriers to entry or expansion and changes in the range of services offered by suppliers of digital platform services'.⁴ In the former, the ACCC concluded that competition for ad tech services in Australia is ineffective, with Google dominating the market. The ACCC considered that Google's access to data contributed to its dominance in the ad tech services market, and found that the company engaged in self-preferencing conduct. In the latter, the ACCC's investigation continues into the operation of markets in a range of digital platform services, including search engine, social media, online private messaging and electronic marketplace services.

1 See <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/>.

2 See <https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/>.

3 See <https://www.accc.gov.au/focus-areas/inquiries-finalised/digital-advertising-services-inquiry/final-report>.

4 See <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025>.

Mergers

The ACCC is one of the many antitrust agencies that reviewed Google's acquisition of Fitbit, a maker of wearables such as the Fitbit watch, which collects data including heart rate, steps, calories and location.⁵ The ACCC considered that the transaction raised concerns because of the aggregation of data:⁶ post-transaction, Google will be able to (1) incorporate Fitbit data into its existing user profiles, likely enabling improved ad targeting, and (2) use the data at the aggregate level to draw broader insights about groups of people with specific attributes, for use across different parts of the business such as in the supply of data-dependent health services.⁷

The ACCC was concerned that the transaction could lessen competition in the supply of data-dependent health services. It noted that Google would have faced stronger competition had the transaction not gone ahead, given Fitbit's extensive pool of data. In addition, the ACCC expressed concern that the combination of Google's analytical capabilities, its existing data and the data it will acquire via Fitbit, could result in Google developing a strong foothold in the market for data-dependent health services. The ACCC considered that the transaction could also reduce competition in the supply of ad tech services. Third parties indicated to the ACCC that certain data from wearables is unique and cannot be captured accurately (or at all) by other means, including data related to heart rate, sleep activity and oxygen saturation.⁸ Therefore, combining Fitbit data with Google's existing dataset may enable Google to 'even more effectively target advertising to consumers with health-related issues, or interests in particular fitness products'.⁹ The transaction could therefore eliminate an important source of potential competition for Google in the supply of certain ad tech services.

5 See Statement of Issues, available at: <https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20Statement%20of%20Issues%20-%202018%20June%202020.pdf>.

6 The ACCC also considered that the transaction raised vertical concerns, as it could give Google the incentive and ability (1) to foreclose competition on the market for wearables by restricting access for rival wearable suppliers to WearOS, Google Maps, the Google Play Store, or (2) to limit the interoperability of rival wearables with the Android phone software.

7 Statement of Issues, para. 86.

8 Statement of Issues, para. 111.

9 Statement of Issues, para. 114.

To address these concerns, Google offered commitments to the ACCC under section 87B of the Australia Competition and Consumer Act.¹⁰ However, unlike its counterparts in the EU, Japan and South Africa,¹¹ the ACCC rejected the proposed commitments.¹² Google subsequently completed its acquisition and the ACCC's investigation into the transaction is ongoing.

Litigation

Google has also come under fire in Australia in recent years due to alleged breaches of data privacy laws. In July 2020, the ACCC announced that it had launched Federal Court proceedings against Google, alleging that the company had 'misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers' internet activity, for use by Google, including for targeted advertising'.¹³

In particular, Google combined user data from Google accounts with user data on non-Google sites that used Google technology, formerly DoubleClick technology, to display ads. The ACCC cleared Google's acquisition of DoubleClick in 2008. Notably, at that time, Google made submissions to the US Federal Trade Commission and European Commission (EC) that it would not combine Google's and DoubleClick's data on consumer internet activity post-merger. However, the regulators did not rely on these statements to approve the transaction.

10 See <https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20s.87B%20consultation%20letter.pdf>.

11 See the European Commission's conditional approval at https://ec.europa.eu/competition/mergers/cases1/202120/m9660_3314_3.pdf; the Japan Fair Trade Commission's conditional approval at <https://www.jftc.go.jp/en/pressreleases/yearly-2021/January/210114r.pdf> and <https://www.jftc.go.jp/en/pressreleases/yearly-2021/January/210114r.pdf>; and the South African Competition Commissioner's conditional approval at <http://www.compcom.co.za/wp-content/uploads/2020/12/Competition-Commission-conditionally-approves-the-Google-Fitbit-merger.pdf>.

12 See <https://www.accc.gov.au/media-release/accc-rejects-google-behavioural-undertakings-for-fitbit-acquisition>. However, similar conditions were accepted by the European Commission at https://ec.europa.eu/competition/mergers/cases1/202120/m9660_3314_3.pdf; the Japan Fair Trade Commission at <https://www.jftc.go.jp/en/pressreleases/yearly-2021/January/210114r.pdf>; and the South African Competition Commissioner at <http://www.compcom.co.za/wp-content/uploads/2020/12/Competition-Commission-conditionally-approves-the-Google-Fitbit-merger.pdf>.

13 See <https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data>.

More recently, Australia's Federal Court ruled in April 2021 that Google misled consumers about personal location data collected through Android mobile devices between January 2017 and December 2018, in a world-first enforcement action brought by the ACCC. The court ruled that when consumers created new Google Accounts during the initial set-up process of their Android devices, Google misrepresented that the 'Location History' setting was the only Google Account setting affecting whether Google collected, kept or used personally identifiable data about their location. In fact, another Google Account setting (Web & App Activity) also enabled Google to collect, store and use personally identifiable location data when turned on, and the setting was turned on by default. The ACCC is seeking declarations, pecuniary penalties, publications orders and compliance orders.

Interaction of privacy and consumer laws

These recent proceedings demonstrate that there is a significant risk of dual enforcement under privacy and consumer laws in Australia. While data subjects in Australia do not have a personal cause of action under the Privacy Act, the Privacy Commissioner has demonstrated a willingness to take enforcement action for significant privacy breaches. The ACCC's proceedings against Google demonstrate a growing propensity to bring actions citing breaches of competition and consumer laws against major platform companies for their use of consumer personal information. While we have not yet seen coordination in enforcement between the Privacy Commissioner and the ACCC, we expect coordinated proceedings in the future given the general focus on curtailing the market power of major platform companies and their data collection and use.

While the criminal codes of Australia's states and territories include provisions against double jeopardy,¹⁴ these are unlikely to prevent dual enforcement by the Privacy Commissioner and the ACCC, particularly in relation to the range of administrative remedies and civil penalties available to each regulator. Criminal penalties do exist for certain breaches of the Privacy Act and Australian competition and consumer law; however, they are available in more limited circumstances in relation to particularly severe violations of each law. As also explained in the Chinese context below, it is not certain that the provisions preventing double jeopardy for criminal offences would apply when the same act violates two different laws.

14 See, section 17, Criminal Code Act 1899 (Qld), section 100, Crimes (Appeal and Review) Act 2001 (NSW) and section 46 Criminal Appeals Act 2004 (WA).

China

Legislation

China's Personal Information Protection Law (PIPL) came into effect on 1 November 2021. It is the first comprehensive piece of Chinese legislation to protect the personal information rights of natural persons within China, and it supplements data privacy-related legislation such as the Cybersecurity Law and the Data Security Law. The PIPL creates new rights of action for individuals whose personal information rights are violated, and sets requirements and penalties for personal information handlers (PIH) that violate the law. It shares many similarities with the GDPR, including its extraterritorial effect, the creation of personal information rights, and the inclusion of penalties for PIH in cases of breach.¹⁵ The PIPL gives agencies at different levels enforcement powers over its regulations.¹⁶

The PIPL's adoption will have an impact on the enforcement of China's Anti-Monopoly Law (AML), the main source of competition law in China. The AML prohibits anticompetitive agreements between competitors, including price-fixing, output restrictions, market allocation and boycotts.¹⁷ It also prohibits vertical agreements that restrict or eliminate competition,¹⁸ and abuses of a dominant position.¹⁹ The AML includes a presumption of dominance where a single undertaking's market share exceeds 50 per cent.²⁰ The State Administration for Market Regulation (SAMR) enforces the AML, and may impose a fine of between 1 and 10 per cent of a company's turnover in case of a breach of the prohibition on anticompetitive agreements or abuses of dominance.

15 There are also many differences between the GDPR and the PIPL. See <https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/>.

16 PIPL, article 60. See <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml> (in Chinese); and <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> (unofficial English translation).

17 AML, article 13. See <http://www.lawinfochina.com/display.aspx?id=6351&lib=law&EncodingName=big5> (English and Chinese).

18 AML, article 14.

19 AML, article 17.

20 See article 19, AML. The presumption of dominance also applies where two undertakings have a combined market share in excess of 66 per cent, or three undertakings have a combined market share in excess of 75 per cent. These presumptions based on combined market shares do not apply to an undertaking that has a market share below 10 per cent.

Interaction of privacy and competition laws

There is a significant risk of dual enforcement against anticompetitive conduct involving breaches of the PIPL, in that both SAMR and the enforcement agencies responsible for enforcing the PIPL can investigate (and potentially impose fines for) conduct that breaches both the PIPL and the AML. In the absence of a memorandum of understanding between the two agencies, it is unclear whether and how they will coordinate their enforcement actions, which creates the risk that companies may be fined twice for the same conduct. While China's Administrative Penalty Law includes a provision against double jeopardy, it is unlikely to provide meaningful protection against dual enforcement as on a literal reading of this provision, double jeopardy only applies in the case of two violations of the same law. This would mean that double jeopardy does not apply when the same act violates two different laws, such as the PIPL and the AML.

Additionally, the PIPL may curtail SAMR's ability to order remedies involving personal information. For example, when investigating an alleged refusal to grant access to personal data by a dominant firm, SAMR may wish to order the dominant firm to 'cease and desist' such conduct, which practically means that the dominant firm must grant access to the data. However, pursuant to the PIPL, a PIH can only transfer personal data to a third party in a limited set of circumstances listed in article 13. The most relevant legal grounds for transferring data are article 13(1) of the PIPL (consent) and article 13(3) of the PIPL (which authorises data processing 'where necessary to fulfil statutory duties and responsibilities or statutory obligations', and which does not require consent from the individual).²¹ It is unlikely that the dominant firm will have the individuals' consent to transfer their personal information to a competitor. The other possible ground is article 13(3), but it is not obvious that a SAMR decision to cease and desist a specific conduct will constitute a valid 'statutory duty and responsibility' or a 'statutory obligation'²² to transfer such data.²³ Hence, the

21 It seems that article 22 of the PIPL, which requires PIH to inform users and obtain their consent in case of a transfer to another PIH, would not apply in the case of a statutory obligation to transfer data because article 13(7) explicitly provides that consent is not required.

22 The term used by the PIPL is "法定义务", which we have translated as 'statutory obligation'. The term 'statutory obligation' appears to suggest a prerequisite statutory law, order or regulation that would give rise to an obligation to comply. In the present case, a cease-and-desist decision appears to fall short of this requirement.

23 Under article 6.1(c) of the GDPR, data can be processed where it is "necessary for compliance with a legal obligation to which the controller is subject". It is debatable whether this would be a sufficient ground for allowing access to data under article 102 TFEU (which prohibits abuses of

dominant firm will therefore need to obtain such consent in accordance with article 23 of the PIPL, unless guidance is issued to the effect that a ‘cease and desist’ order from SAMR constitutes a statutory duty or obligation pursuant to article 13(3) of the PIPL.

Litigation

Article 17(5) of the AML prohibits undertakings in a dominant position from imposing unreasonable trading conditions, while the Antitrust Guidelines in the Field of Platform Economy (Platform Guidelines), introduced by SAMR in 2021, also advise against ‘compulsory collection of unnecessary user information.’²⁴ A PIH in a dominant position that requires users to provide ‘unnecessary information’ (or to consent to a transfer of personal information to a third party) as a condition for using its services could therefore be in breach of both the PIPL and the AML. There is no guidance on the term ‘unnecessary information’, but a narrow interpretation would mean that a PIH can only collect information that is strictly necessary to use its services (or, where relevant, to deliver its products). In July 2021, a local court in Zhejiang province found that Ctrip, China’s largest online travel agent, was liable for collecting personal data from users that was used to personalise price offering, likely resulting in higher prices for consumers. The court ordered Ctrip to either (1) allow users to use its services without agreeing to the platform’s privacy policy and service agreement, or (2) stop collecting unnecessary personal information.²⁵

Article 17(3) of the AML prohibits undertakings with a dominant position from refusing to deal without ‘justified reason’. However, in the context of a refusal to provide access to personal data, enforcing article 17(3) is likely to prove difficult. From a competition law perspective, a plaintiff will have to demonstrate that a defendant PIH holds a dominant position, which is onerous as market shares are often difficult to calculate in data-related markets. Additionally, if the plaintiff claims that the data is an essential facility, it will have to demonstrate that such data is necessary or indispensable to compete. Given that data is non-exclusive and non-rivalrous, it is likely that

dominance). Indeed, according to recital 41 of the GDPR ‘such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it’.

See V Kathuria and J Globonick, Exclusionary conduct in data-driven markets: limitation of data sharing remedies, Max Planck Institute for Innovation and Competition, Research paper No. 19-04, p. 23.

24 Platform Guidelines, article 16(5). See https://gkml.samr.gov.cn/nsjg/fldj/202102/t20210207_325967.html.

25 See <https://www.scmp.com/tech/policy/article/3141264/tripcom-ordered-make-exception-privacy-policy-lawsuit-could-open-door>.

such a claim will fail. Even if these competition law issues are surmounted, the PIPL may provide the PIH with a justified reason for refusing access to personal data, as a PIH can only transfer personal data to a third party in the limited set of circumstances listed in article 13 of the PIPL.

The courts may soon have a first opportunity to opine on a case involving a refusal of access to personal data. In November 2021, the Changsha Intermediate People's Court accepted an antitrust complaint brought by Eefung Software, a data analytics company based in Hunan province. After Sina Weibo allegedly terminated its cooperation with Eefung Software, the latter company unsuccessfully attempted to reconnect with the former. Eefung Software alleges that its business model was destroyed by the termination, and alleges abuse of dominance by virtue of Sina Weibo's refusal to deal. It seeks the use of Sina Weibo's data under reasonable conditions, as well as compensation for economic loss and reasonable legal costs. This case will likely set a precedent for future cases involving the intersection of antitrust and data access.

Mergers

The AML includes a prohibition on anticompetitive mergers, with a focus on concentrations that result or that may result in the elimination or restriction of market competition. However, there are unfortunately very few SAMR decisions to serve as precedent for SAMR's approach to such transactions when they involve personal data. While SAMR and its predecessors have never expressly stated that transactions involving variable interest entities (the corporate structure used by virtually all Chinese big tech companies (VIEs)), do not need to be notified, in practice these transactions have generally gone unreported.²⁶ As noted above, in 2021, SAMR introduced the Platform Guidelines²⁷ which made it clear that transactions involving VIEs ought to be notified if the thresholds for compulsory notification are met. This could lead to an influx of SAMR decisions involving tech companies and personal data issues in the near future. Notably, the Platform Guidelines state that when evaluating a concentration, SAMR may consider, inter alia, (1) the difficulties faced by market participants

26 See F Jiang, S Yu and J Jiang, '*China signals VIE no longer an obstacle in merger filing*', Competition Policy International, available at: <https://www.competitionpolicyinternational.com/china-signals-vie-no-longer-an-obstacle-in-merger-filing/>.

27 See the full text of the Platform Guidelines in Chinese at: https://gkml.samr.gov.cn/nsjg/ftdj/202102/t20210207_325967.html.

in obtaining necessary resources and essential facilities such as data, and the scale of capital investment necessary to enter the market,²⁸ and (2) the merger party's ability to improperly use consumer data post-transaction.²⁹

India

Legislation

While India as yet has no omnibus data protection laws, a final draft of its Data Protection Bill was submitted by the Indian Joint Parliamentary Committee (the Committee) in December 2021. The Bill is largely in line with the GDPR. The Committee's report on the Bill recommended a phased approach to implementation after the law takes force, likely in the first half of 2022. Once the Bill comes into force, there is a risk that the same conduct will breach both competition and data protection laws in India, increasing the risk of dual enforcement.

Market studies

The interplay between data privacy and competition regulation was further explored by the CCI in its Market Study Report on the Telecom Sector in India, released in January 2021.³⁰ The Report examined, inter alia, data competition in the digital communications market, and the inherent conflict between allowing user access and protecting consumer privacy. The CCI considered that there is a conflict between allowing access and protecting consumer privacy in the context of data in the digital communications market. It noted that while privacy can take the form of non-price competition, competition analysis must also focus on 'the extent to which a consumer can 'freely consent' to action by a dominant player'.³¹ The CCI acknowledged that India is yet to introduce its Data Protection Law, but concluded that the antitrust law framework is 'broad enough to address the exploitative and exclusionary behavior arising out of privacy standards, of entities commanding market power'.³²

28 See the Platform Guidelines, article 20(4).

29 See the Platform Guidelines, article 20(6).

30 See https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-Study-on-the-Telecom-Sector-In-India.pdf.

31 *id.*, para 70.

32 *ibid.*

Litigation and enforcement

The issue of dual enforcement has already reared its head in India in the case of *In re: updated terms of service and privacy policy for WhatsApp users*. The CCI ordered a *suo moto* investigation into changes to WhatsApp's privacy policy while the same issue was 'sub judice before various courts and other fora in India'.³³ Prior to conducting any investigation, the CCI took the prima facie position that the changes constituted the imposition of unfair terms. WhatsApp challenged the characterisation of its policy update and argued that the CCI should only be able to exercise jurisdiction after the judicial challenges are resolved, and appealed the CCI's decision to open an investigation. The jurisdictional challenge is currently pending before the courts.

Indonesia

Legislation

There is currently no single law governing data protection in Indonesia; the applicable regime is enshrined in various different sector-specific laws and regulations. To address this, a draft of the Personal Data Protection Act (PDP Bill)³⁴ was introduced in the Indonesian parliament in January 2020, to consolidate rules related to data protection and align Indonesia more closely with international standards like the GDPR, including by introducing concepts such as data controllers and data processors and imposing administrative and criminal sanctions for non-compliance. However, despite the ongoing efforts of Indonesian legislators, the PDP Bill is yet to pass into law.

Law No. 5 of 1999 on the Prohibition of Monopolistic Practices and Unfair Business Competition is the main source of competition law in Indonesia. In November 2020, Law No. 11/2020 on Jobs Creation came into force (the Omnibus Law), which amended various provisions of Law No. 5 of 1999. Most significantly, the Omnibus Law removed the 25 billion rupees (approximately US\$1.7 million) cap on fines for competition law infringements. In May 2021, the Indonesian Competition Commission (KPPU) issued its implementing regulation for the Omnibus Law³⁵

33 Para. 11, *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users*, *Suo Moto Case No. 01 of 202*, available at: https://www.cci.gov.in/sites/default/files/SM01of2021_0.pdf.

34 Press release (in Indonesian) available at https://www.kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-presiden-serahkan-naskah-ruu-pdp-ke-dpr-ri/0/siaran_pers; the PDP Bill (in Indonesian) is available at <https://web.kominfo.go.id/sites/default/files/users/4752/Rancangan%20UU%20PDP%20Final%20%28Setneg%20061219%29.pdf>.

35 Regulation No. 2 of the Guidelines for Imposing Administrative Fines.

which granted the CCI has the power to impose fines of up to (1) 50 per cent of relevant net profits, or (2) 10 per cent of relevant turnover during the infringement period, for companies that violate competition laws.³⁶

Mergers

In May 2021, Gojek, a leading mobile on-demand services and payments platform in Southeast Asia, and Tokopedia, a leading online marketplace in Indonesia, announced a merger of their businesses to form the largest technology group in Indonesia, GoTo Group. According to Tokopedia, the GoTo Group encompasses 2 per cent of Indonesia's GDP.³⁷

The KPPU has announced that it continues to monitor the GoTo Group post-transaction. According to the KPPU, it is yet to receive any notification of the merger in accordance with domestic regulations. However, the KPPU has stated that it will use the studies it has conducted into the digital sector to oversee the merger.³⁸ In its 2020 study into the digital economy, the KPPU found that market power in the digital economy depends largely on the control of data and network effects, meaning that these factors should be considered when assessing a concentration's competitive (or anticompetitive) effects.³⁹

South Korea

Data protection in South Korea is currently governed by the Personal Information Protection Act (PIPA). In January 2020, the Korean National Assembly adopted amendments to the PIPA and other data protection laws, to implement a more streamlined approach to personal data protection in South Korea and align the PIPA with international standards. The amendments were also aimed at facilitating an adequacy decision from the EC, which was subsequently received in December 2021 and promotes the transfer of personal data between South Korea and the EU without

36 See <https://content.mlex.com/#/content/1269482>.

37 See <https://www.tokopedia.com/blog/gojek-and-tokopedia-combine-to-form-goto-the-largest-technology-group-in-indonesia-and-the-go-to-ecosystem-for-daily-life/>.

38 See <https://eng.kppu.go.id/icc-watch-over-potential-violation-in-post-establishment-of-goto-group/>.

39 See https://content.mlex.com/Attachments/2021-02-10_1LE2TGMJR61NY77Y/Digital-2020-Ringkasan-Eksekutif.pdf.

additional mechanisms or authorisations for data transfers.⁴⁰ The Personal Information Protection Commission is the exclusive supervisory authority in South Korea and has the competency to impose fines similar to those provided for under the GDPR.

In November 2021, the Korean National Assembly adopted amendments (the Amendments) to the Unfair Competition Prevention and Trade Secret Protection Act (the UCPA), which are due to come into force on 20 April 2022. The Amendments expand the scope of data protection and the definition of unfair competition. In particular, the Amended UCPA now covers data defined under the Framework Act on the Promotion of Data Industry and Promotion of Utilization, defined as ‘technical or business information provided to a specific person or a large number of specific persons for business, accumulated and managed in a substantial amount by electronic means, and not managed as confidential’.⁴¹ The Amendments also clarify the categories of data use that will constitute unfair competition.

Taiwan Legislation

The Personal Data Protection Act 2015 (PDPA) and its related Enforcement Rules govern data protection in Taiwan. As in South Korea, Taiwanese legislators have sought to align the country’s data protection regime more closely with the GDPR to obtain an adequacy decision from the EC. Taiwan is in continued discussions with the EU in relation to the adequacy decision and may implement additional amendments to the PDPA to achieve a favourable outcome.

Market studies

Taiwan’s Digital Economy Committee has published the issues for consideration in its 2021 White Paper, which focuses in part on the development of national data strategies to facilitate healthy market competition.⁴² The Committee suggests that the government provides the newly established Ministry of Digital Development ‘with a

40 The adequacy decision between South Korea and the European Union is available at <https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-republic-korea-annexes_en>.

41 Framework Act on the Promotion of Data Industry and Promotion of Utilization, Article 2(1). See <https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EB%8D%B0%EC%9D%B4%ED%84%B0%EC%82%B0%EC%97%85%EC%A7%84%ED%9D%A5%EB%B0%8F%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EC%97%90%EA%B4%80%ED%95%9C%EA%B8%B0%EB%B3%B8%EB%B2%95/18475,20211019> (in Korean).

42 See <https://amcham.com.tw/2021/06/2021-digital-economy-position-paper/>.

mandate to promote a more open, less restrictive digital economy'. It notes that the new ministry was set up to encourage 'reasonable market competition', and argues that the recommended mandate would further support digitalisation.

Taiwan's Fair Trade Commission (TFTC), is currently conducting a market inquiry to explore antitrust issues in digital markets,⁴³ with the aim of establishing whether there is a need to investigate specific market players. The inquiry is expected to conclude by the end of 2022. This comes after the TFTC closed an investigation into Google's Android operating system in May 2021, finding a lack of sufficient evidence of wrongdoing following allegations of abuse of market dominance.⁴⁴ Although the investigation has been dropped, the moves suggest that data processors will face increasing scrutiny in Taiwan with respect to competition law issues.

Japan

Legislation

The Act on the Protection of Personal Information (APPI) sets out the general data protection regime in Japan and reflects significant reforms implemented in 2015. Despite this, data protection reform in Japan has been ongoing and in June 2020 the Japanese parliament adopted an amending bill to better align the APPI with the GDPR and strengthen Japan's data protection regime.⁴⁵ The bill will take force on 1 April 2022 and expand the rights of data subjects, in addition to increasing the applicable criminal penalties for both individuals and entities.

Market studies

In June 2021, the Japan Fair Trade Commission (JFTC) published its Report of the Study Group on Competition Policy for Data Markets (the Report).⁴⁶ The Report notes that data is increasingly seen as a source of competitiveness, and that businesses have started to utilise data in physical spaces (eg, automatic driving, medical care and agriculture) as well as in cyber spaces (eg, search engines and social networking services). The Report discusses the various challenges involved with drafting effective competition policy in data markets, and recommends, inter alia (1) involving a wide range of stakeholders when establishing frameworks to ensure individuals' security and

43 See <https://content.mlex.com/#/content/1325781>.

44 See https://content.mlex.com/#/content/1294483?referrer=content_seehereview.

45 English version of the of APPI available at https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

46 See <https://www.jftc.go.jp/en/pressreleases/yearly-2021/June/210625.html>.

trust; (2) providing free and easy access to data to limit competition concerns, and (3) ensuring data portability and interoperability to enable users to switch without obstacles or to use multiple different platforms (multi-homing).⁴⁷ Significantly, the JFTC makes clear that when addressing personal data issues, competition, data privacy and consumer protection should not be discussed separately, but rather regulators should adopt a holistic approach considering the three areas together.

Merger

In January 2021, the JFTC, like many other regulators, reviewed Google's acquisition of Fitbit. The JFTC's assessment paid close attention to the potentially anticompetitive effects of Google combining its own dataset with that of Fitbit's, for use in its advertising business. However, on the basis of the commitments offered by Google, the JFTC ultimately concluded that the acquisition would not substantially restrain competition.⁴⁸ Google undertook, for a period of 10 years, to (1) supply operating systems for smart phones and healthcare databases on a non-discriminatory basis; (2) segregate the parties' healthcare database from Google's other datasets and restrict the use of such database for Google's digital ads, and (3) report to the JFTC every six months via a monitoring trustee.

Conclusion

The legislation, enforcement, litigation and mergers examined in this contribution demonstrate the increasing significance of issues at the intersection of data privacy and competition law in the Asia-Pacific region. Legislators, regulators and lawyers are working to define how modern legal issues concerning the digital economy can or should be framed under existing competition, data privacy and consumer laws, or otherwise, how these legal frameworks should be developed to tackle nascent data privacy issues. Evidently, the answer is not simple, and challenges remain: most notably, coordination between enforcement agencies is needed to prevent dual enforcement under different regimes for the same conduct.

47 See <https://www.jftc.go.jp/en/pressreleases/yearly-2021/June/210812.pdf>.

48 See <https://www.jftc.go.jp/en/pressreleases/yearly-2021/January/210114.pdf>.



SÉBASTIEN EVRARD

Gibson, Dunn & Crutcher LLP

Sébastien Evrard is a partner in the Hong Kong office of Gibson, Dunn & Crutcher LLP. He is a member of the firm’s antitrust and competition practice group. Based in Asia since 2010, Mr Evrard handles complex antitrust matters in Asia and the European Union, including merger control, non-merger investigations, and litigation. His practice also focuses on the antitrust aspects of intellectual property rights, and the interplay between data privacy and antitrust. Mr. Evrard’s experience spans a wide range of industries including aviation/shipping, banking, energy/mining, media/entertainment, software/hardware, telecommunications, pharmaceuticals, automotive, and fast moving consumer goods.



CONNELL O'NEILL

Gibson, Dunn & Crutcher LLP

Connell O'Neill is a partner of Gibson, Dunn & Crutcher LLP. He is head of the firm’s technology practice in Asia, advises clients throughout APAC and the Middle East on corporate and commercial transactions, privacy and cybersecurity, product counselling, and commercial intellectual property matters in the information technology, media and telecommunications sectors. Mr O'Neill has been a key adviser on many major matters across APAC and the Middle East, including in China, Hong Kong, the Philippines, Myanmar, Thailand, Indonesia, UAE and elsewhere, and has provided strategic commercially sensitive advice to clients on a range of complex and emerging topics.



HAYLEY SMITH

Gibson, Dunn & Crutcher LLP

Hayley Smith is an associate in the Hong Kong office of Gibson, Dunn & Crutcher LLP. Ms Smith has broad experience of internal and regulatory investigations, commercial litigation and competition and antitrust matters.



KATHERINE TOMSETT

Gibson, Dunn & Crutcher LLP

Katherine Tomsett is a trainee solicitor currently on secondment to the Hong Kong office of Gibson, Dunn & Crutcher LLP.



NICK HAY

Gibson, Dunn & Crutcher LLP

Nick Hay is an associate in the Hong Kong office of Gibson, Dunn & Crutcher LLP. Mr. Hay advises clients throughout the Asia-Pacific region on technology, data and IP-driven corporate and commercial transactions, with a particular focus on the information technology, telecommunications, FMCG and financial services sectors.

GIBSON DUNN

Gibson, Dunn & Crutcher is a global law firm with more than 1,600 lawyers located in 20 offices in major cities throughout the United States, Europe, the Middle East, Asia and South America. Gibson Dunn's Antitrust and Competition Practice Group is repeatedly recognised by Chambers and other publications as one of the top antitrust practices in the world. The Group comprises over 150 lawyers worldwide that include former high-ranking officials from the US Department of Justice (DOJ), the US Federal Trade Commission (FTC), the US Solicitor General's Office and the European Commission, as well as Fellows of the American College of Trial Lawyers. Gibson Dunn's privacy, cybersecurity and data innovation practice group has a demonstrated history of helping companies successfully navigate the complex and rapidly evolving laws, regulations, and industry best practices relating to privacy, cybersecurity and data innovation. The firm's global and interdisciplinary team advises clients across a broad range of industries in high-stakes matters on the full spectrum of issues in these areas.

32/F, Gloucester Tower
The Landmark
15 Queen's Road Central
Hong Kong
Tel: +852 2214 3700
Fax: +852 2214 3710
www.gibsondunn.com

Sébastien Evrard
sevrard@gibsondunn.com

Connell O'Neill
coneill@gibsondunn.com

Hayley Smith
hsmith@gibsondunn.com

Katherine Tomsett
ktomsett@gibsondunn.com

Nick Hay
nhay@gibsondunn.com

The *Asia-Pacific Antitrust Review 2022* edition of Global Competition Review Insight is one of a series of publications that also covers the Americas and Europe, Africa and the Middle East. Each one delivers specialist intelligence and research designed to help readers – general counsel, government agencies and private practitioners – successfully navigate the world's increasingly complex competition regimes. GCR has worked exclusively with the region's leading competition practitioners, and it is their wealth of experience and knowledge – enabling them not only to explain law and policy, but also put it into context – that makes this review particularly valuable to anyone doing business in the Asia-Pacific region today.

Visit globalcompetitionreview.com
Follow @GCR_alerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-858-1