Asia-Pacific Antitrust Review

2024

Asia-Pacific Antitrust Review

2024

GCR's *Asia-Pacific Antitrust Review 2024* delivers specialist intelligence to help readers – in-house counsel, government agencies and private practitioners – navigate increasingly complex competition regimes across the Asia-Pacific region.

Evolving legislation and enforcement tactics continue to transform the landscape, as highlighted by recent amendments to China's Anti-monopoly Law and an uptick in private antitrust cases in Japan; meanwhile, the Korea Fair Trade Commission has updated its Guidelines on Merger Filing to expedite the review process.

Generated: May 2, 2024

GCR Global Competition Review

Contents

Why competition law and data privacy are coming to a crossroads in the Asia-Pacific region

Sébastien Evrard, **Connell O'Neill**, **Nick Hay**, **Katie Cheung** and **Peter Chau**
Gibson Dunn & Crutcher LLP

Summary

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)

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. Recent years have been characterised by regulatory enforcement against 'Big Tech' companies, the introduction, expansion and gradual harmonisation of data privacy regimes across the Asia-Pacific region, and the significant investment made by enforcement agencies to better understand the digital economy and the role of competition and data privacy regimes in regulating this growing market.

In 2023, China published long-awaited measures on the use of standard contractual clauses for cross-border data transfers; Australia completed its multi-year review of the country's data privacy regime, with wholesale legislative amendments expected in 2024; Indonesia released draft regulations implementing its first comprehensive data privacy law enacted in 2023; while India managed to navigate various political obstacles to pass its equivalent after multiple prior attempts. 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, Japan, South Korea and Taiwan.

AUSTRALIA

Legislation

Since 2020, the Australian government has been undertaking a wholesale review of the Privacy Act 1988 (Privacy Act), with a view to reforming the country's data protection regime to align Australia's privacy regime more closely with global equivalents (such as the GDPR) and reflect recent developments in the digital economy. After nearly three years and multiple rounds of consultation, the Attorney-General released its final report on 16 February 2023. The report indicates the likely direction of travel – proposing wide-ranging reforms such as expanding the definition of personal information, increasing the enforcement and oversight powers of the regulator (including the maximum civil penalties for non-compliance), strengthening the rights of individuals to object to the collection, use and disclosure of their information and to require its erasure, as well as modifying the framework for international data transfers. Of the 116 proposals put forward in the report, the government has agreed to 38, agreed in-principle to a further 68 and noted the remaining – indicating a general consensus with the Attorney-General's findings.

The Attorney-General will now lead the next stage of reform, including progressing further advice to government in 2024 based on outcomes of additional consultation processes and legislative proposals. Changes to the Privacy Act in 2024 will also be complimented by other reforms that the government is progressing in this area, including the Digital ID, the National Strategy for Identity Resilience and Supporting Responsible AI in Australia.

On the antitrust side, companies that breach Australia's competition (and consumer) laws now face higher penalties under amendments introduced by the Treasury Laws Amendment (More Competition, Better Prices) Bill 2022 passed in late 2022. The changes consist of two parts:

- the introduction of penalties and other changes relating to unfair contract terms (representing the first ever penalties for unfair contract terms), which recently came into effect on 9 November 2023;
  and
- significant increases in maximum penalties for civil contraventions of the Competition and Consumer Act (CCA), which took effect on 10 November 2022.

The maximum penalties for companies that commit civil contraventions of the CCA have increased to the greater of A$50 million (approximately US$35 million) or three times the value derived from the relevant breach, or, if the value derived from the breach cannot be

determined, 30 per cent of the company's turnover during the period it engaged in the conduct.

Changes to Australia's antitrust framework for digital markets appear to be in the making. In November 2023, following the release of the Australian Competition and Consumer Commission's (ACCC) latest Digital Platform Services Inquiry 2020–2025 (DPSI) report (discussed further below), the ACCC announced that new competition laws were needed in response to the expansion of digital platforms, which the ACCC noted was exacerbating the risks of competitive harms and invasive data collection practices.

Market Studies

The issue of competition in digital markets has continued to be hot on Australia's regulatory agenda in recent years. Starting in 2017, the Australian Competition & Consumer Commission (ACCC) has conducted three inquiries into digital platforms: the Digital Platforms Inquiry 2017–2019 (which considered the impact of online search engines, social media and digital platforms on competition in the media and advertising services markets), the Digital Advertising Services Inquiry 2020–2021 (which considered the competition and efficiency in the supply of ad tech services) and the Digital Platform Services Inquiry 2020–2025 (DPSI) (which is still ongoing).

As part of the DPSI, the government directed the ACCC to examine competition in markets for the supply of digital platform services, including internet search engine services, social media services, online private messaging services, digital content aggregation platform services, media referral services and electronic marketplace services. Testament to the importance the government is placing on digital platforms, the ACCC is required to publish an interim report on the inquiry every six months until the final report is released in March 2025.

In 2023, the ACCC published its sixth and seventh interim reports (in April and November 2023, respectively) and passed the mid-point of the DPSI. The sixth interim report examined competition and consumer issues associated with social media services in Australia. In particular, the ACCC found a number of issues at the intersection of competition and data privacy, including data collection and use practices by social media service providers and a lack of advertising transparency. Meanwhile, the seventh interim report considered competition and consumer issues from the expanding of digital platforms providers in Australia, including how digital platform ecosystems may take advantage of increased data collection and lock-in practices to limit consumer choices. The ACCC concluded that new and strengthened laws are required to better protect Australian consumers and small businesses, who are increasingly reliant on digital platforms, and new measures to promote competition in the supply of digital platform services. The ACCC's recommendations include mandatory codes of conduct for specific digital services that address issues such as anticompetitive self-preferencing, tying and exclusive pre-installation arrangements.

Mergers

Proposed reforms to Australia's merger control regime have also been an important item on the ACCC's agenda. In addition to proposing a mandatory notification regime and other significant changes, the ACCC has recommended making 'increased access to or control of data, technology or other significant assets' a specific factor that must be considered when it assesses whether a merger could harm competition and raise barriers to entry. Further, the ACCC has specifically highlighted concerns that large digital platforms can reduce their

potential competition by acquiring competitors and their customer data, and by leveraging their data advantages to extend their market power into related markets.

The ACCC's concerns regarding data-related transactions are exemplified by its review of Google's acquisition of Fitbit, a producer of activity-tracking wearables that collect data including heart rate, steps and location.

The ACCC considered that the transaction raised concerns because of the aggregation of data: in particular, the ACCC considered that Google would be able to incorporate Fitbit data into its existing data set, which, when combined with Google's analytical capabilities, could lead to Google developing a strong position in the market for data-dependent health services. The ACCC was concerned that this could lessen competition in the market for data-dependent health services, and noted that Google would have faced strong competition if the transaction did not go ahead, given Fitbit's extensive data pool.

The ACCC also considered that the transaction could reduce competition in the supply of ad tech services. Given indications from third parties that certain data from wearables is unique and cannot be captured accurately (or at all) by other means, the ACCC concluded that 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'. The transaction could therefore eliminate an important source of potential competition for Google in the supply of certain ad tech services.

To address these concerns, Google offered commitments to the ACCC, but unlike its counterparts in the EU, Japan and South Africa, the ACCC rejected the proposed commitments. Nevertheless, Google completed its acquisition and the ACCC has continued its investigation into the transaction in the form of a post-completion review, which appears to be 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'. 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 argued that this newly combined information was used to improve Google's advertising business, and reduced the rights of account holders' without obtaining explicit consent. However, in December 2022, the Federal Court found that the notification and the changes to the privacy policy were not misleading because Google sought the informed consent of account holders to implement the changes and the Court also noted that account holders' rights were not reduced under the privacy policy.

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. In August 2022, the ACCC succeeded in its proceedings against Google to pay $60 million in penalties for the breach.

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, 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.

CHINA

Legislation

China's Personal Information Protection Law (PIPL) came into effect on 1 November 2021, but has continued to take shape in subsequent years as the Cyberspace Administration of China (CAC) has issued a wide range of implementing regulations to provide further colour to the law. The PIPL is the first comprehensive piece of Chinese legislation to protect the personal information rights of natural persons within China, and supplements data privacy-related legislation such as the Cybersecurity Law and the Data Security Law. In particular, 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. The PIPL gives agencies at different levels enforcement powers over its regulations.

Notably, in 2023, the CAC issued further guidance and regulations to facilitate data transfers outside China, including by establishing measures permitting applicable Chinese data exporters to utilise a standard contract akin to the GDPR's SCCs.

China's competition law regime did not reference data or explicitly recognize the relevance of data to competition assessment until the introduction of the Antitrust Guidelines in the Field of Platform Economy (the Platform Guidelines) in early 2021 and amendments to China's

Anti-Monopoly Law (AML), the main source of competition law in China, in mid-2022. This signalled that China's lawmakers are increasingly engaging with issues at the intersection of competition law and data, with a focus on the digital economy.

The AML amendments, among other things, prevent undertakings from 'us[ing] data and algorithms, technologies, capital advantages, platform rules, etc. to engage in monopolistic behaviour prohibited by this Law' (article 9), and state that undertakings 'with a dominant market position shall not use data, algorithms, technologies, platform rules, etc. to engage in the abuse of a dominant market position '. The relevance of data to China's antitrust regime was further highlighted by a number of the new implementing regulations for the AML that took effect in early 2023. These include:

- The Provisions on Prohibiting Abuse of Market Dominance, which establish that the ability to control, master and process data is a factor for determining market dominance, and provide that undertakings can invoke 'data security' as a justification for imposing exclusive or restricted dealing requirements;
- The Provisions on Prohibiting Monopoly Agreements, which prohibit competing undertakings from segmenting the market for data, and restrict undertakings from using data in any way to conclude a horizontal anticompetitive agreement or perpetrate resale price maintenance; and
- The Provisions on Merger Review, which stipulate that data divestiture is a structural remedy that can be imposed on a merged entity, and provide that the ability to master, process or control data is relevant to the determination of the degree of market control possessed by the parties to a merger, or the impact that a merged entity could have on barriers to entry.

The expansion of data privacy rules in China with the adoption of the PIPL, alongside the continuing updates of China's competition regime to tackle data issues, leaves no doubt that Chinese regulators will have to grapple with how these two regimes can be enforced side by side.

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).

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 to transfer such data.

Hence, the 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/enforcement

Article 22(5) of the AML prohibits undertakings in a dominant position from imposing unreasonable trading conditions, including through the use of data or algorithms, technology or platform rules, while the Platform Guidelines, referenced above, explicitly advise against 'compulsory collection of unnecessary user information.'
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).

Article 22(3) of the AML prohibits undertakings with a dominant position from refusing to deal without 'justified reason', including through the undertaking's use of data or algorithms, technology or platform rules, etc. However, in the context of a refusal to provide access to personal data, enforcing Article 22(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 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.

In July 2022, the CAC announced that it had fined the ride hailing platform Didi Chuxing 8 billion yuan for violations of the PIPL, Cyber Security Law and Data Security Law. Following an investigation, the CAC found that Didi had: (1) collected illegal and excessive personal information from users; (2) failed to clearly and accurately explain the processing purposes of personal information collected; and (3) failed to fulfil its obligations of cybersecurity, data security and personal information protection. While the CAC did not follow in 2023 with any enforcement action of a similar scale, the severity of the CAC's sanctions suggests that it is now prepared to utilise its broad investigatory and enforcement powers regardless of the potential business impact to companies, particularly those in the technology sector and with overseas operations. The classification of Didi as a 'critical information infrastructure operator' also indicates that the CAC and other Chinese regulators intend to adopt a broad interpretation of this defined concept under the Cyber Security Law, as well as to link mobility data, including location data, with national security.

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. On 26 January 2024, the revised merger notification thresholds came into effect, which introduced higher turnover thresholds. These are expected to reduce the volume of merger filings, and will hopefully help accelerate SAMR's case review.

The recent AML amendments have also confirmed SAMR's powers to review transactions that do not meet the notification threshold, in circumstances where the transaction nevertheless 'may have the effect of eliminating or restricting competition.' Indeed, in Sep 2023, SAMR granted conditional clearance to the proposed acquisition by Simcere of Tobishi, which was the first below-threshold case to have submitted a voluntary notification and received a conditional clearance.

However, there are unfortunately very few SAMR decisions to serve as precedent for SAMR's approach to transactions which raise anticompetitive concerns involving 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.

As noted above, in 2021, SAMR introduced the Platform Guidelines 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.

For now, SAMR is sending a clear message to tech companies that there will be consequences of failing to file in China. SAMR has issued penalties against a range of companies for failing to file, including tech companies Taobao, Baidu and Didi Chuxing. In July 2021, SAMR for the first time imposed remedies post-closing for failure to file, in particular, on Tencent for failing to notify its acquisition of a controlling stake in China Music Group. In Tencent/China Music Group, SAMR concluded not only that the transaction was reportable, but also identified anticompetitive effects.

INDIA

Legislation

After several years and multiple proposed bills, the Indian Government finally enacted a comprehensive data protection law in 2023. The Digital Personal Data Protection Act 2023 (the DPDP Act) received royal assent on 11 August 2023 and will come into force in phases (on dates to be notified), effecting wholesale changes to the treatment and protection of personal data in the world's most populous country.

The DPDP Act represents a more streamlined and focused approach to data protection regulation than prior iterations, departing from a 2022 draft which was criticised by commentators and industry groups as being overly prescriptive and compliance-heavy, and for providing undue access to data by state and law enforcement agencies. The DPDP Act includes provisions for its extraterritorial application, a notice and consent based regime for personal data processing (subject to a limited set of exceptions), restrictions on cross-border transfers to blacklisted countries and significant penalties (up to US$30 million) for non-compliance, however excludes data storage and localisation requirements contained in the 2022 draft. Despite this, many of the detailed requirements of the DPDP Act are pending the release of implementing regulations which the government plans to finalise in due course – so the full impact of the changes are yet to be seen.

On the antitrust side, the much-anticipated Competition Amendment Bill has been passed in April 2023, which will, among other things, expand the CCI's powers of merger review by introducing a deal value threshold. The Bill requires that deals with a transaction value of more than 20 billion rupees be notified and approved by the CCI.

Market Studies

Following the trend set by regulators around the world, the CCI has launched market studies into the telecom, pharmaceutical and e-commerce sectors in recent years. The Market Study Report on the telecom sector, released in January 2021, 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'.

The CCI acknowledged that India is yet to introduce its data protection law (the PDP Bill at the time), but concluded that the antitrust law framework is 'broad enough to address the exploitative and exclusionary behaviour arising out of privacy standards, of entities commanding market power'.

More recently, the CCI also initiated a new research paper on 'Data Protection and Anti-trust: Two sides of the same coin' to study the relationships and linkages between data privacy and protection and antitrust issues in the digital sector. This is an attempt to understand the issues involved in the interface of legal tools and to prepare an issue paper based on the research.

Litigation And Enforcement

The issue of dual enforcement reared its head in India in the WhatsApp case. The CCI ordered an investigation into changes to WhatsApp's privacy policy, alleging that WhatsApp's data collection regime was an abuse of dominance against its users. In addition to challenging the characterisation of its policy update, WhatsApp appealed the CCI's decision to open an

investigation on the basis that CCI should only be able to exercise jurisdiction after the judicial challenges are resolved. In October 2022, the Supreme Court dismissed the appeal, and the CCI's investigation remains ongoing.

The issue of data privacy arose in a different way in the CCI's action against Google in late 2022 for abuse of dominance in relation to the Play Store. Among other things, the CCI found that Google was able to collect significant amounts of personal and financial data by requiring users and app developers to use Google Play Store's billing system (GPBS) for app-related transactions.

The CCI observed that such data enabled Google to provide targeted offers to users of Google's own apps, and noted that Google's failure to share such data in a 'transparent and equitable' way with app developers had affected developers' ability to improve their competing offerings.

Notably, the CCI rejected Google's defence that it had to withhold certain personal data from app developers to protect privacy, and held that 'privacy concerns can be adequately protected by suitable measures through contractual stipulations rather than blanket denial of access to data of their users'. Following the CCI's fine of US$113 million, Google appealed to India's National Company Law Appellate Tribunal, and the substantive hearing is currently adjourned.

INDONESIA

Legislation

Indonesian data protection reform in 2023 was necessarily more muted than in 2022, which saw the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). Despite this, in August, the Ministry of Communications and Informatics (MOCI) publicly released the draft Government Regulation on the Implementation of the Personal Data Protection Law (PDP Regulation) for public consultation. The draft PDP Regulation further clarifies the provisions of the PDP Law, setting out binding obligations for covered entities. It is extensive (arguably unnecessarily so, comprising 245 articles over 180 pages), however notably broadens the scope of the definition of personal data, specifies the responsibilities of a newly formed data protection authority, mandates risk assessments prior to entities relying on the legitimate interest ground for processing and empowers the data protection authority to issue a white list for cross-border data transfers. Along with the PDP Law, the draft PDP Regulation consolidates the rules related to personal data protection in Indonesia and establishes data sovereignty and security as the keystone of Indonesia's data protection regime in order to align it more closely with international standards such as the GDPR.

On the antitrust end, the Competition Commission of Indonesia (KPPU) issued a new regulation on merger filings (Regulation No. 3 of 2023 on Assessments of Mergers or Consolidation of Business Entities, or Acquisitions of Company Shares Which May Result in Monopolistic Practices and/or Unfair Business Competition). One of the key amendments is the revised threshold for asset value, which is now limited to local asset value in Indonesia (as opposed to worldwide asset value). The new regulation also clarified that a foreign-to-foreign transaction is only notifiable to the KPPU if both parties (directly or indirectly) have asset or turnover in Indonesia.

An interesting intersection between data protection and antitrust concerns arose in the Ministry of Trade's Regulation No. 31 of 2023 (MOT 31/2023), which took effect on 26

September 2023. Among various provisions regulating the activities of business entities transacting through electronic systems, MOT 31/2023 effectively requires digital platforms to ensure that user data held by their e-commerce operations is segregated from other operations (such as social media), and prohibits any abuse of user data by their e-commerce operations.

Although the precise boundaries of these rules are unclear, the Indonesian government has emphasised that the purpose of the rule is to prevent monopolistic behaviour and advance data protection.

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.

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.

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.

Investigation

In Sep 2022, the KPPU launched an investigation against Google, with a focus on Google's requirement for certain applications to use the Play billing system and whether that amounted to an abuse of dominance. Pursuant to Indonesia's amended case-handling procedures published in April 2023, a company being investigated may apply for case dismissal by proposing a 'change in behaviour' integrity pact without admitting guilt. Google followed this path and offered behavioural commitments to the KPPU in late 2023, which were ultimately rejected by the KPPU on the basis that Google failed to fulfil two of the requirements in its application. The KPPU's investigation remains ongoing and may advance to the hearing stage soon.

JAPAN

Legislation

2023 saw limited domestic activity with regard to data protection in Japan. Despite this, Japanese government agencies announced various joint initiatives with foreign governments and data protection authorities in the second half of the year, including a memorandum of understanding with the UK that will facilitate sharing of information between data protection authorities in the respective countries, a deal on cross-border data flows with the EU that will remove certain data localisation requirements in each jurisdiction and a joint statement with the US regarding collaboration on cross-border data flows and effective privacy protections globally.

On the antitrust side, as a result of the JFTC's extensive market studies, the government has introduced a number of laws directed at regulating the digital economy, including the Act on

Improving Transparency and Fairness of Digital Platforms (TFDPA) (2021) and the Act for the Protection of Consumers who use Digital Platforms (PCDP) (2021). The TFDPA introduces obligations for certain digital platform providers to disclose terms and conditions, and prior notice of changes, to vendors of online marketplaces, as well as to submit annual reports to the Japanese government, which includes a self-assessment of their compliance with the TFDPA. The PCDP was introduced to regulate the relationship between consumers and digital platforms, and ensure that consumers are adequately protected. The PCDP seeks to introduce a non-prescriptive approach whereby digital platforms are encouraged to make voluntary efforts to protect the interests of consumers.

In accordance with the TFDPA, Japan's Ministry of Economy published the transparency evaluation reports of several tech companies like Google and Rakuten on 2 February 2024. In particular, the ministry noted that for cases where improvement requests from the previous evaluation report were not fulfilled, it would consider taking administrative actions if the issues remain.

Market Studies

The JFTC has undertaken a number of initiatives to better understand the digital economy in recent years. In Feb 2023, the JFTC published the 'Market Study Report on Mobile OS and Mobile App Distribution', in which the JFTC examined the mobile OS ecosystem as well as the app store platforms in Japan to assess the state of competition in these spaces. The JFTC recommended several measures for Apple and Google to consider, including refraining from using non-public data generated by other developers' apps for the purpose of developing competing apps.

In March 2023, the JFTC also launched the Study Group on Innovation and Competition Policy in order to attain a deeper understanding the interplay between innovation and competition in Japan. An interim report was published in June 2023, in which the study group set out preliminary thoughts on how mergers and acquisitions and joint research projects may affect innovation. In the next report, the study group will examine how innovation and competition could be translated into JFTC's practices and the application of Japan's Anti-Monopoly Act (AMA).

Mergers

On merger control, the JFTC has reviewed a number of mergers involving issues at the intersection of competition and data, including Google/Fitbit (2021) and salesforce.com/Slack Technologies (2021).

The JFTC's assessment of Google/Fitbit 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. 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.

In salesforce.com/Slack Technologies, part of the JFTC's investigation assessed whether the combined data collected by the two companies gave merged entity a competitive advantage. The JFTC found that Salesforce is mainly engaged in the business of providing

CRM software, and Slack, Inc. is engaged in the business of providing business chat services. Since all of these products and services are used for the common purpose of improving the efficiency of operations and communications by companies as users, there is a certain complementarity between each other. However, the JFTC concluded that due to the strict limits placed on the client data the two companies acquire or can access, the combined accumulation of user data posed no competitive advantage.

Investigation

In Oct 2023, the JFTC announced a preliminary investigation into Google's pre-installation of search and browser apps in the smartphone market, with a key focus to understand the effects of Google's policies on the search market and other rival search service providers to determine whether Google is in contravention with the AMA. This is also the first investigation where the JFTC invited third-party input at an early stage, as part of the JFTC's recent efforts to enhance information gathering to facilitate probes. It is expected that going forward, the JFTC will disclose the launch of new investigations at an early stage to encourage input from third-parties and expedite the information collection process.

SOUTH KOREA

Legislation

In February 2023, the Korean National Assembly adopted some of the most significant amendments to the Personal Information Protection Act (PIPA) since its enactment in 2011. The amendments took effect in September 2023 and are aimed at 'streamlining inconsistencies in data processing standards disparately applied to online and offline businesses' to help prepare the industry for a 'full-fledged digital transformation'.

Key amendments include streamlining privacy-related dispute resolution procedures for public institutions and private companies, aligning obligations applicable to online and offline businesses (including with respect to breach reporting, obtaining consent from minors and the application of administrative sanctions), and revising the conditions for cross-border data transfers and the associated penalties for non-compliance.

As of 12 January 2023, the KFTC has implemented new guidelines for digital platforms that define the screening criteria for abuse of dominance cases. As these platforms can generate revenue through, for example, targeted ad services using user data, the KFTC recognised that a market can be defined for zero-price services. In this case, a relevant market is the range of services that can be substituted as the amount of personal data collected grows. When evaluating market dominance, the new guidelines suggest looking at five factors: the presence of market entry barriers, whether platforms have significant influence as a gatekeeper to control access to major user groups, their ability to collect, store and use data, their research and development status and the potential of new services. The new guidelines highlight major types of competition-restraining practices adopted by platforms, including multi-homing restraints, most favoured nation treatment, self-preferencing and tying, with applicable provisions of the competition law attached to each conduct.

Notably, the KFTC has implemented guidelines, as opposed to regulations, as it recognises the nuance of 'platforms' multi-sided nature and other characteristics of digital markets, such as data concentration. Nonetheless, the KFTC also recognises that such characteristics can lead to 'tipping effects' of online platforms whereby several platforms with larger numbers of users (such as search engines, social media, video streaming services, mobile operating

systems, digital-ad services and others) raise barriers to new entrants. Going forward, the number of users, frequency of use and other variables could be assessed instead of market share for platforms that offer free services. Whether or not platforms' actions hinder competition may be determined, the new guidelines suggest, by weighing the competition restraints against efficiency gains or customer benefits.

The KFTC has also announced the initiative for a new legislation, the Act on the Promotion of Platform Market Competition, to prohibit unfair practices by designated dominant platforms. The initiative was first introduced in December 2023 and sparked controversy over the proposed pre-designation system, which critics argued would unfairly stigmatise the designated platforms and dampen innovation and growth in the digital platform ecosystem. The KFTC appeared to be reconsidering alternatives in light of the public feedback.

In addition, the KFTC is also introducing a reform of its merger-control regime after 40 years. The proposed changes include implementing a new system whereby merging companies can propose their own remedies and, if the regulator determines that these remedies are adequate to remove competition constraints, such mergers can be approved on a conditional basis.

Litigation

In September 2021, the KFTC fined Google 224.9 billion won and issued corrective orders against Google for its ban on 'Android forks' through the imposition of anti-fragmentation agreements (where rival smart-device makers cannot develop or adopt modified Android operating systems for their products). Google appealed this decision, but the appeal was dismissed in January 2024.

In December 2022, the Seoul High Court ruled in favour of the KFTC by determining that Naver, a Korean online market place, had indeed abused its dominant position by manipulating its search algorithms to self-preference its own platform, Smart Store, over competitors, and that the KFTC had succeeded in issuing its antitrust fine of 26.6 billion won. The KFTC alleged that Naver regularly monitored the effect of its search algorithm changes on the visibility of Smart Store items and adjusted its strategy accordingly. As a result, the KFTC found that Naver's exposure of items hosted on its own market place at the top of search results, in order to entice customers, was an unfair trade practice as it went against consumer expectations that searches would provide the most relevant results.

TAIWAN

Legislation

In May 2023, the Taiwan Legislative Yan passed an amendment to the Personal Data Protection Act 2015 (PDPA) to address public concerns about increasingly frequent data breaches affecting large numbers of data subjects. The amendment increases fines for covered entities that fail to adequately protect their data subjects' personal data and designates the establishment of the Personal Data Protection Commission (PDPC) as the exclusive (and independent) data protection authority in the country. Taiwan also remains in continued discussions with the EU in relation to obtaining an adequacy decision for cross-border data transfers. Relevant to these efforts, the Executive Yuan revealed that it has approved draft regulations for the PDPC, which would empower the authority to draft further amendments to amendments to the PDPA, and start planning how it would provide

oversight over personal data protection affairs for both government and non-government agencies.

On the antitrust side, the Taiwan Fair Trade Commission (TFTC) has announced revisions to the Rules for Relevant Market Definition in July 2023. In particular, the proposed revisions will provide clarifications to the factors for consideration when defining relevant product and geographic markets in relation to the digital economy. The revised rules were published for public consultation last year.

Market Studies

In 2021, Taiwan's Digital Economy Committee published the issues for consideration in its White Paper on Competition Policy in the Digital Economy, which focused in part on the development of national data strategies to facilitate healthy market competition. The Committee suggested that the government provide the newly established Ministry of Digital Development 'with a mandate to promote a more open, less restrictive digital economy'. It noted that the new ministry was set up to encourage 'reasonable market competition', and argued that the recommended mandate would further support digitalisation. Since, the TFTC has published its own White Paper on Competition Policy in the Digital Economy (the TFTC White Paper) in December 2022, following public consultation on an earlier draft.

The TFTC White Paper summarises 14 competition issues in the digital economy and provides its position and guiding principles of enforcement for enterprises' reference. These issues include challenges to data privacy and market competition and algorithms. The TFTC indicated that the TFTC White Paper also provides suggestions of possible regulatory amendments, such as to review the guidelines of market definition so as to adapt to the market features of digital economy. Moreover, in the future, the TFTC will progressively introduce information technology in the course of case analysis and improve its technological enforcement capability by employing digital tools.

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.

GIBSON DUNN

Sébastien Evrard sevrard@gibsondunn.com
Connell O'Neill coneill@gibsondunn.com
Nick Hay nhay@gibsondunn.com
Katie Cheung kcheung@gibsondunn.com
Peter Chau PChau@gibsondunn.com

75008 Paris, France

Tel: +33 1 56 43 13 00

http://www.gibsondunn.com/