The Chinese Journal of Comparative Law, 2025, **13**, 1–16
https://doi.org/10.1093/cjcl/cxae018
Article

OXFORD

Excessive Data Collection and (Mis)use of Data: A Comparative Law and Economics Study on the Chinese Didi Case and the German Facebook Case

Qian Li *

*Law and Tech Lab, Faculty of Law, Maastricht University, Bouillonstraat 1-3, 6211LH, Maastricht, The Netherlands. Email: q.li@maastrihctuniversity.nl

ABSTRACT

The excessive data collection and (mis)use of data can result in the coexistence of two market failures—namely, market dominance and information asymmetry—which in turn interact with each other in digital markets and trigger simultaneous concerns about competition law and data protection law. This article establishes a law and economics framework to study the divergence in response to the concerns caused by excessive data collection and (mis)use of data by dominant technology undertakings in the European Union and China. The German competition authority, the Bundeskartellamt, found that Facebook, a dominant social network platform, abused its dominant position by excessively collecting and misusing user data without consent, whereas the Cyberspace Administration of China addressed similar concerns caused by Didi, a dominant ride-hailing undertaking, via data protection law. Based on the comparative analysis of the German Facebook case and the Chinese Didi case, a competition law approach to deal with excessive data collection and the (mis)use of data by a dominant technology undertaking results in high enforcement costs due to the prerequisites of market definition and dominance determination under abuse of dominance, while contributing to minimizing error costs, especially false negatives in the absence of data protection enforcement. In contrast, a data protection approach would be a cost-effective way to intervene in the market *ex-ante* by decreasing the likelihood of excessive collection and misuse of data, reducing the exclusionary and/or exploitative effects of competition and lowering the market entry barrier that benefits from the collection and processing of significant amounts of data.

This research was supported by the China Scholarship Council under the project 'AI-enabled Price Discrimination: A Competition Law Perspective' (Grant No. 202009370093) and the RegTech4AI AiNed Fellowship Grant, funded by the Dutch National Growth Fund (File No. NGF.1607.22.028).

INTRODUCTION

In digital markets, competition and data protection questions are often intertwined. These markets are typically dominated by a handful of large gatekeepers whose business models are contingent on the large-scale collection of data. In the European Union (EU), Facebook, a social media undertaking, is one of the largest technology undertakings and is known for its large-scale collection of data about its users. It uses this to better target its users with advertising—the core of Facebook's business model. In China, Didi is the largest ride-hailing undertaking and it, too, collects very detailed data about its customers. It, too, uses this data to show its users better advertising and also to improve the pricing of any taxi rides booked through the Didi app. The extent of this data collection, for both undertakings, has long been criticized and deemed as being in violation of both competition and data protection rules.

Facebook exploited its dominant position by requiring users to allow the unrestricted collection of all data generated through third-party websites and combining it with their Facebook account as a condition for using its social network.[1] The German competition authority, the Bundeskartellamt, ordered the undertaking to seek proper consent before data collection and not to abuse its market power in seeking such consent. In the Didi case, the undertaking was met with a fine of $1.2 billion for its data protection violation due to its extremely excessive collection and processing of user data and was ordered to revise its data practices.[2] Both rulings were arguably unprecedented since they posed novel challenges at the intersection of competition and data protection law and attracted wide coverage in the news.

Interestingly, the German Facebook case and the Chinese Didi case share many important characteristics: both involve highly influential technology undertakings that excessively collected and misused data. However, the two cases were addressed using different legal frameworks. The Bundeskartellamt applied traditional competition law in the Facebook case, while the Cyberspace Administration of China determined that Didi's excessive data collection violated data protection law. What prompted the different regulatory treatment was that, in the Chinese case, regulators identified threats to national security and saw a need to act swiftly. This is despite the fact that China's competition and data protection law regime was similar—in many ways—to that of Germany and the EU.[3] This motivates a comparative analysis of the two cases in this article. Admittedly, one might argue that the Digital Markets Act (DMA) would come into play in the EU nowadays.[4] Nevertheless, this article aims to compare the traditional competition law approach and the data protection law approach when addressing the issue in question.

As such, the research question in this article is, therefore, how should competent authorities respond to the concerns caused by the excessive data collection and (mis)use of those data conducted by dominant technology undertakings? To answer the research question, this article will explore the economics of excessive data collection and (mis)use of data after this introduction, then discuss current legal regimes to tackle concerns caused by excessive

[1] Bundeskartellamt, 'Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing, Sector: Social Networks' (6 February 2019) <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3> accessed 30 July 2024.

[2] Cyberspace Administration of China, 'A Spokesperson from the Cyberspace Administration of China Responded to Questions from Journalists Regarding the Decision to Impose Administrative Penalties on Didi Global Inc. Through Network Security Reviews'[国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问] <http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm> accessed 30 July 2024.

[3] Lars Hornuf, Sonja Mangold and Yayun Yang, 'Data Protection Law in Germany, the United States, and China' in Lars Hornuf, Sonja Mangold and Yayun Yang, *Data Privacy and Crowdsourcing* (Springer 2023) 19–79. See also Anja Geller, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective' (2020) 69 GRUR Intl 1191.

[4] EU Regulation 2022/1925 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)(2022, OJ L 265).

data collection and (mis)use of data in China and the EU. After that, this article will delve into different approaches taken in the Chinese Didi case and the German Facebook case. Next, a theoretical framework measured by cost-benefit analysis will be established to evaluate the effectiveness of the two approaches. Further, this article will apply the theoretical framework to assess the effectiveness of the two approaches and observations come afterwards.

ECONOMICS OF EXCESSIVE COLLECTION AND (MIS)USE OF DATA

The expansion of business models centred on collecting and processing consumer data has changed the modern world. In general, employing consumer data helps businesses enhance production efficiency, predict market trends, and optimize decision-making, which may lead to positive gains for businesses and consumers.[5] Under these circumstances, businesses will increasingly undertake strategies to obtain and sustain their advantages to maximize profits in data-equipped competition, including, *inter alia*, excessive data collection and misuse of those data, which may enhance consumer segmentation through targeted advertising and personalized recommendations.[6]

However, information asymmetry between online retailers and consumers during digital transactions places consumers in a more vulnerable position. Since there is a lack of transparency regarding the excessive collection and (mis)use of data, misleading information, and behavioural manipulation, consumers seem to be overwhelmed and unable to make rational, well informed decisions concerning their personal data.[7] It would enhance the exploitative effects on consumers in the digital markets, in particular, with the lock-in effects in the platform economy.

What makes it even worse is that, once consumer data is controlled by a few large market participants, it can grant them a significant competitive edge, enabling them to block new entrants and exclude competition. Therefore, it may lead to competition concerns of exclusionary effects in digital markets due to the dominant market positions of large technology companies. The stronger the market power, the greater the possibility of hindering market access by potential competitors, which results in an even stronger position of dominance.[8] As such, a few large profit-driven market players equipped with excessive consumer data may exclude rivals[9] and thereby derogate effective competition. Therefore, the excessive data collection and (mis)use of those data conducted by dominant technology undertakings lead to the coexistence of two market failures (market dominance and information asymmetry). The interaction effects between the two market failures make the relationship more complicated in digital markets.[10] As such, economic concerns caused by competition and data protection are deeply intertwined, and the division of the two legal regimes of competition law and data protection law has been blurred in the digital platform.

Although the collection and control of substantial amounts of data are not illegal, the (mis)use of consumer data to gain or maintain market power and conduct abusive conduct might amount to a violation of competition law that requires the intervention of competition authorities.[11] In the meantime, it may also fall into the scope of data protection law. This

[5] Organisation for Economic Co-operation and Development (OECD), *Big Data: Bringing Competition Policy to the Digital Era* (2016) 8 <https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf> accessed 1 August 2024.

[6] OECD, 'Price Discrimination: Background Note by the Secretariat' (2016) <https://one.oecd.org/document/DAF/COMP(2016)15/en/pdf> accessed 1 August 2024.

[7] Wolfgang Kerber and Karsten Zolna, 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law' (2022) 54 Eur JL & Economics 217.

[8] Qian Li and Niels Philipsen, Why AI enabled Price Discrimination is not Always Undesirable: Lessons from Law and Economics, Maastricht University Law Blog (2022) <https://www.maastrichtuniversity.nl/blog/2022/06/why-ai-enabled-price-discrimination-not-always-undesirable-lessons-law-and-economics> accessed 12 November 2024.

[9] OECD (n 5) 2 .

[10] Kerber and Zolna (n 7) 222.

[11] OECD (n 5) 20.

raises the question of how to deal with the relationship between competition law and data protection law regarding the excessive data collection and (mis)use of data by dominant technology undertakings.

LEGAL REGIMES TO TACKLE EXCESSIVE DATA COLLECTION AND THE (MIS)USE OF DATA IN CHINA AND THE EU

In China, excessive data collection and (mis)use of data by dominant undertakings may amount to an abuse of dominance in digital markets within the meaning of Article 22 of the Anti-Monopoly Law of the People's Republic of China.[12] Apart from competition law, Articles 41, 64, and 74 of the Cyber Security Law[13] provide the principles and methods to collect personal data. Articles 24, 66, 67, and 69 of the Personal Information Protection Law (PIPL)[14] and Articles 10, 29, 50, 56, and 57 of the Consumer Protection Law[15] also deal with the collection and processing of personal data.

In the EU, the excessive data collection and (mis)use of data conducted by dominant undertakings would trigger competition concerns and could fall within the scope of Article 102 of the Treaty on the Functioning of the European Union (TFEU)[16] in the manner of price discrimination, unfair pricing, predatory pricing, and so on. If the data of natural persons would be collected and/or processed without a legal ground (normally, their consent), the Directive on Privacy and Electronic Communications[17] and the General Data Protection Regulation (GDPR)[18] come into play. The application of the GDPR also triggers numerous other obligations, such as transparency requirements, that need to be respected. In specific circumstances, the Unfair Commercial Practices Directive,[19] the Services Directive,[20] the P2B Regulation,[21] the Digital Services Act,[22] the Digital Markets Act (DMA), and even the Directive on the Supply of Digital Content and Digital Services[23] may be relevant.

As such, the comprehensive legal regimes established in China and the EU provide theoretical possibilities to deal with the concerns brought about by excessive data collection and

[12] Anti-Monopoly Law of the People's Republic of China [中华人民共和国反垄断法] (Order no 68 of the President of the People's Republic of China, promulgated by the Standing Committee of the National People's Congress on 30 August 2007, effected on 1 August 2008, amended and released on 24 June 2022 and enacted on 1 August 2022 (AML)).

[13] Cyber Security Law of the People's Republic of China [中华人民共和国网络安全法] (Order no 53 of the President on 11 July 2016, effected on 6 January 2017 (Cyber Security Law)).

[14] Personal Information Protection Law of the People's Republic of China [中华人民共和国个人信息保护法] (Adopted at the 30th meeting of the Standing Committee of the 13th National People's Congress on 20 August 2022, effected on 1 December 2021).

[15] Consumer Protection Law of the People's Republic of China [中华人民共和国消费者权益保护法] (Order no 92 of the President on 31 October 1993, effected on 1 January 1994, amended on 25 October 2013).

[16] Treaty on the Functioning of the European Union, as adopted by the Treaty of Lisbon (2010, OJ C83/49).

[17] EC Directive 2002/58 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (2002, OJ L 201). See, in particular, art 13 requiring the prior consent of subscribers or users for the use of automatic calling machines, faxes, or email for direct marketing.

[18] EU Regulation 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR) (2016, OJ L 119). See, in particular, art 21 concerning the individual's right to object to the use of its personal data for direct marketing, arts 12–14 containing information obligations and art 22 granting the individual the right not to be subject to a decision that produces legal effects concerning them or significantly affects them and that is based solely on automated processing of data, including profiling.

[19] EC Directive 2005/29 Concerning Unfair Business-to-consumer Commercial Practices in the Internal Market (2005, OJ L 149).

[20] EC Directive 2006/123 on Services in the Internal Market (2006, OJ L 376).

[21] EU Regulation 2019/1150 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services (2019, OJ L 186).

[22] EU Regulation 2022/2065 on a Single Market For Digital Services (2022, OJ L 277).

[23] EU Directive 2019/770 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services (2019, OJ L 136).

(mis)use of data. The question arises as to the advantages and disadvantages of the use of any of these legal instruments (or a combination thereof).

DIFFERENT APPROACHES TAKEN IN THE CHINESE DIDI CASE AND THE GERMAN FACEBOOK CASE

Reviewing recent cases, China and the EU responded differently to the concerns of excessive data collection and (mis)use of data by dominant technology undertakings. This section will look into two typical cases—the Chinese Didi Case and the German Facebook Case—as examples to explore the advantages and disadvantages of the approaches used.

Case analysis of the Chinese Didi case

In its initial public offering prospectus, Didi identified itself as 'the world's largest mobility technology platform' in ride-hailing service.[24] Didi disclosed that it and more than 30 other Chinese Internet companies had met with regulators, including the State Administration for Market Regulation (SAMR) (competition authority in China) and the Cyberspace Administration of China, in April 2021. They were instructed to carry out a 'self-inspection' to identify and rectify any potential infringements under anti-monopoly, anti-unfair competition, tax and other related laws and regulations, and submit compliance commitments.[25] As disclosed, the SAMR recently imposed administrative penalties on Didi for 'failing to duly make filings as to transactions subject to merger control review' and fined Didi for 'certain transactions where it did not obtain prior merger control clearance' in the past.[26] This demonstrates that Didi has violated competition law due to, among others, its significant market power in ride-hailing service. Moreover, Didi also identified the compliance requirements on the security of information collected and used by mobile apps provided in recent regulatory instruments (such as the Methods of Identifying Illegal Acts of Apps to Collect and Use Personal Information) jointly adopted by, *inter alia*, the SAMR and the Cyberspace Administration of China.[27] It is reasonable to conclude, on a *prima facie* basis, that Didi's practices have raised both competition and data protection concerns, given the vast amount of data collected and used by the world's largest mobility technology platform.

According to an industry report, Didi Chuxing held approximately 90 per cent of the market share in 2022,[28] which further demonstrates its significant market position in the ride-

[24] DiDi Global Inc Registration Statement under the Securities Act of 1933, as filed with the Securities and Exchange Commission on 28 June 2021, Registration no 333-256977 <https://www.sec.gov/Archives/edgar/data/1764757/000104746921001221/a2243298zf-1a.htm#ca10201_prospectus_summary> accessed 1 August 2024.

[25] See China's initial public offering (IPO)-bound Didi probed for antitrust violations by Julie Zhu and Pei Li, 17 June 2021 <https://www.reuters.com/business/autos-transportation/exclusive-chinas-ipo-bound-didi-probed-antitrust-violations-sources-2021-06-17/> accessed 1 August 2024.

[26] DiDi Global Inc Registration Statement (n 24).

[27] As stated in Didi's IPO prospectus, 'pursuant to the Announcement of Conducting Special Supervision against the Illegal Collection and Use of Personal Information by Apps, which was issued by the Cyberspace Administration of China, the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security and the State Administration for Market Regulation on 23 January 2019, app operators shall collect and use personal information in compliance with the Cyber Security Law and shall be responsible for the security of personal information obtained from users and take effective measures to strengthen personal information protection. Furthermore, app operators shall not force their users to make authorization by means of default settings, bundling, suspending installation or use of the app or other similar means and shall not collect personal information in violation of laws, regulations, or breach of user agreements. Such regulatory requirements were emphasized by the Notice on the Special Rectification of Apps Infringing upon User's Personal Rights and Interests, which was issued by MIIT on 31 October 2019. On 28 November 2019, the Cyberspace Administration of China, the MIIT, the Ministry of Public Security and the State Administration for Market Regulation jointly issued the Methods of Identifying Illegal Acts of Apps to Collect and Use Personal Information. This regulation further illustrates certain commonly seen illegal practices of app operators in terms of personal information protection and specifies acts of app operators that will be considered as 'collection and use of personal information without users' consent''.

[28] According to an industry report, the app, Didi Chuxing [滴滴出行] holds around 90% of the market share, as observed from indicators of daily orders and monthly active users in 2022. See Qianji Investment Bank, *2023 Online Car Hailing*

hailing market. Based on the investigation, the Cyberspace Administration of China mainly provides the reasoning in the following aspects: (i) regarding the nature of the violations, Didi failed to fulfil its obligations regarding network security, data security, and personal information protection as required by relevant laws, regulations, and regulatory authorities; (ii) considering the duration of the violations, Didi's relevant illegal behaviours began as early as June 2015 and have persisted for seven years, continuously violating the Cyber Security Law implemented in June 2017, the Data Security Law implemented in September 2021, and the PIPL implemented in November 2021; (iii) regarding the harm caused by the violations, Didi collected personal information such as clipboard data, screenshot information from photo albums, and family relationship information through illegal means, severely infringing upon users' privacy rights and personal information; (iv) regarding the quantity of illegally processed personal information, Didi has processed approximately 64.709 billion pieces of personal information, including sensitive data such as facial recognition information, precise location information, and identification card numbers; and (v) examining the circumstances of the illegal handling of personal information, Didi's violations involve multiple apps and encompass various situations, including the excessive collection of personal information, compulsory collection of sensitive personal information, frequent requests for unnecessary permissions, failure to fulfil obligations regarding personal information handling notifications, and neglect of network security and data security protection obligations.[29]

Therefore, the Cyberspace Administration of China imposed the following penalties on Didi Global: (i) a fine of 8.026 billion yuan (approximately US $1.2 billion) imposed on Didi Global, accounting for 4.6 per cent of its total revenue of 173.827 billion yuan in the previous business year. This fine is close to the upper limit specified in the PIPL, which is 5 per cent of the previous year's revenue; (ii) a fine of 1 million yuan was imposed on the chief executive officer and the president of Didi Global, respectively. This is the maximum penalty for company executives who violate the Chinese PIPL; and (iii) During the investigation (July 2021–July 2022), all of Didi Global's apps were removed from app stores. Didi Global's app was prohibited from accepting new users.

Case analysis of the German Facebook case

Germany employed a competition law approach in the Facebook case. The German Competition Authority, the Bundeskartellamt, found that 'Facebook is abusing this dominant position by making the use of its social network conditional on its being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account'.[30] First, applying the concept of demand-side substitutability, the Bundeskartellamt defined 'the product market as a private social network market with private users as the relevant opposite market side. The relevant geographic market is Germany'.[31]

Second, Facebook is the dominant undertaking in the national market for social networks for private users pursuant to Section 18(1) in conjunction with (3) and (3a) of the German Competition Act (GWB),[32] with full consideration of all factors of market power. The Bundeskartellamt examined the user-based market share of Facebook. The Bundeskartellamt

Industry Research Report <https://www.21jingji.com/article/20230410/herald/1eb153f7e2ae7c03a619b290ad077263.html> accessed 1 August 2024.

[29] Cyberspace Administration of China (n 2).

[30] Bundeskartellamt (n 1).

[31] Bundeskartellamt (n 1).

[32] Competition Act (Gesetz gegen Wettbewerbsbeschränkungen—GWB) Competition Act in the version published on 26 June 2013, Bundesgesetzblatt (Federal Law Gazette I) (2013) 1750, 3245, as last amended by art 1 of the Act of 25 October 2023 (Federal Law Gazette I) 294.

considered the number of daily active users as the key indicator to evaluate the network's competitiveness. In this case, the Bundeskartellamt mainly examined the amount of time spent intensively using the network when assessing the market share. The market dominance test highlights Facebook's strong direct and indirect network effects, the difficulty of switching to other networks, and its superior access to competitively valuable data, which enhances personalized advertising and raises significant barriers to market entry.

Third, Facebook's data policy, which allows the collection and merging of user and device data from both Facebook and external sources, constitutes an abuse of its dominant position in the social network market under Section 19(1) GWB. This data exploitation, in violation of GDPR requirements, harms both users and competitors. Facebook's processing of personal data through its services breaches European data protection laws and requires user consent. This policy grants Facebook an unfair competitive advantage, raises market entry barriers, and strengthens its market power over end customers.

Therefore, the Bundeskartellamt prohibited Facebook's data processing policy and its implementation under Section 19(1) GWB, requiring the undertaking to provide users with an additional consent option. Facebook filed an appeal against the ruling to the Düsseldorf Higher Regional Court, which dismissed the decision made by the Bundeskartellamt. Nevertheless, the German Federal Court of Justice overturned the ruling of the Düsseldorf Higher Regional Court and upheld the Bundeskartellamt's decision, albeit on different grounds. The German Federal Court of Justice employed the German constitutionally fundamental right to informational self-determination to reconcile the opposing positions of the contractual parties. This case returned to the Düsseldorf Higher Regional Court, which subsequently requested the Court of Justice of the European Union (CJEU) for a preliminary ruling under Article 267 of the TFEU.[33] The CJEU ruling on the Facebook case explicitly holds that a national competition authority can find, in the context of the examination of the abuse of a dominant position, that the GDPR has been infringed.[34] If dominant digital undertakings use the very personal data of consumers, this usage can also be considered abusive under competition law.[35] The Bundeskartellamt finally concluded its Facebook proceeding on 10 October 2024, which resulted in a bundle of measures that gives users of the social network Facebook significantly improved options regarding the combination of their data.[36]

Germany uses competition law as a weapon to deal with the excessive collection and (mis)use of user data by dominant technology undertakings, while China tackles a similar problem via an information protection approach under the Cyber Security Law, the Data Security Law, and the PIPL. The question that arises is: is one approach more effective than the other? To answer this question, this research will establish economic benchmarks to evaluate the two approaches.

[33] Case C-252/21, *Meta Platforms and Others v the Bundeskartellamt* [2023] ECLI:EU:C:2023:537.

This request for a preliminary ruling concerns the interpretation of art 4(3) of the Treaty on European Union (2010, OJ C83/13) and of art 6(1), art 9(1), and (2), art 51(1) and art 56(1) of the GDPR (n 17). 'The request has been made in proceedings between Meta Platforms Inc, formerly Facebook Inc, Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, and Facebook Deutschland GmbH, on the one hand, and the Bundeskartellamt (Federal Cartel Office, Germany), on the other, concerning the decision by which the latter prohibited those companies from processing certain personal data as provided for in the general terms of use of the social network Facebook'.

[34] Ibid.

[35] Bundeskartellamt, 'CJEU Decision in Facebook Proceeding: Bundeskartellamt May Take Data Protection Rules into Consideration' (4 July 2023) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/04_07_2023_EuGH.html> accessed 30 July 2024.

[36] Measures include: (i) introducing an Accounts Centre to keep data collected from Meta's different services separate; (ii) introducing 'cookie' settings that allow Facebook data to be separated from other data; (iii) special exception for Facebook Login; (iv) concise customer information; (v) user navigation; and (vi) limited combination of data for security purposes. Bundeskartellamt, 'Facebook Proceeding Concluded' (10 October 2024) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html?nn=49114> accessed 18 October 2024.

A THEORETICAL FRAMEWORK TO EVALUATE THE TWO APPROACHES

In order to assess which approach is more effective in dealing with excessive collection and (mis)use of data by dominant technology undertakings in China and the EU, an economic theoretical framework of optimal deterrence measured by a model of cost-benefit analysis will be employed. Following Roger Van den Bergh, in economic terms, the enforcement of legal regimes may be qualified as *optimal* if anti-competitive practices are properly punished and deterred, while enforcement errors and enforcement costs are minimized.[37] In other words, the goal of competition law is not to achieve full deterrence but rather optimal deterrence, taking into account welfare loss in the form of error costs and enforcement costs. Besides these inter-related economic considerations, retributive justice and data protection will also be considered.

Optimal deterrence

According to Nobel prize winner Gary Becker,[38] a crime 'will be committed if the expected benefits exceed the expected costs, which equal the statutory fine discounted by the probability of detection and punishment'.[39] Becker's model of the rational criminal seems referable in competition law and data protection law. This is predicated on the assumption that undertakings are likely to engage in unlawful anti-competitive behaviours if the gains/benefits derived from such an activity exceed the costs, both adjusted according to the probability that they will materialize in case of detection and punishment.[40]

In the context of excessive data collection and misuse of data, the costs of dominant undertakings consist of fines (F) imposed by competent authorities multiplied by the probability of detection and punishment (p). The costs expected by the dominant undertakings must be higher than the gains (G) expected by those undertakings.[41] Becker's model can be formulated as:

$$G < p.\ F$$

Achieving deterrence requires the determination of an efficient fine (F). The harm caused by excessive data collection and misuse of data is difficult to assess since it is not simply equal to the 'consumer surplus transferred to the producer' but also includes the 'additional loss of consumer welfare (deadweight loss), the harm in terms of productive and dynamic efficiency, as well as the costs of rent-seeking'.[42] As an alternative, scholars proposed to measure the size of the gains/benefits since this amount, multiplied in inverse proportion to the probability of detection and punishment, enables law enforcers to set the fine above the expected profit.[43] Furthermore, the amount of gains is easier to access compared with the above-mentioned harm.

Besides the size of the fines, the calculation of efficient fines requires the rate of detection and punishment—that is, (p)—as well. Since the 1980s, there have been several empirical studies published that estimate the percentage of detected and punished anti-competitive

[37] Roger Van den Bergh, *Comparative Competition Law and Economics* (Edward Elgar 2017) 382.

[38] Gary Becker introduced the model in criminal law and this model was then extended to administrative law and even civil law.

[39] Gary Becker, 'Crime and Punishment: An Economic Approach' (1968) 76 J Political Economy 169.

[40] Van den Bergh (n 37) 398.

[41] It takes the analysis about hard-core cartel as a reference. See Roger Van den Bergh (n 37) 398.

[42] Van den Bergh (n 37) 399.

[43] Mitchell Polinsky and Steven Shavell, 'Should Liability Be Based on the Harm to the Victim or the Gain to the Injurer?' (1994) 10 JL Economics, Organization 427.

Table 1. Accumulative condition for optimal deterrence on anti-competitive practice

***Optimal* Deterrence on Anticompetitive Practice Requires:**	
1.	Deterrence of Anticompetitive Practice
2.	Minimizing Error Costs ↓
3.	Minimizing Enforcement Costs ↓

behaviours conducted by dominant undertakings, which ranges between 10 per cent and 17 per cent.[44] Van den Bergh presents an example in which he calculates the efficient fine that is needed to deter an undertaking from participating in a cartel, based on estimates in the economic literature on the size of the overcharge and the rate of detection. In this scenario, if a price increase of 10 per cent leads to an increase in profits of 5 per cent of turnover, the observed behaviour lasts five years and the probability of detection and punishment is 16 per cent, a fine of no less than 150 per cent of the annual turnover would be needed to reach full deterrence based on the formula, $G < p.\ F$.[45] Whether the fines imposed in the Didi case and the Facebook case can reach effective deterrence requires further examination in the next section (Table 1).

A cost-benefit approach compares the costs and benefits to determine effective enforcement. To conduct this comparison, benefits refer to the reduction of social costs arising from the excessive data collection and misuse of data conducted by tech undertakings, while costs refer to the error costs and enforcement costs. Generally speaking, it appears to be difficult to qualify benefits and costs in practice.[46] With respect to benefits, it is necessary to ascertain the beneficial impact (B) in terms of achieving compliance with the different enforcement policy options.[47] Regarding costs, there are error costs (C_e) arising from the imperfect procedure, institutions, or inappropriate decisions, and administrative costs (C_a) associated with the enforcement regimes (that is, enforcement costs). As for the cost-effectiveness approach, it takes a high enforcement level as the goal and aims to achieve it at the least cost.[48] It thereby requires considering whether the benefits outweigh the costs—that is:

$$B > C_e + C_a$$

The cost-benefit approach enables us to hypothesize how decisions on different enforcement options are likely to impact benefits and costs—that is, (B) and ($C_e + C_a$). To do so, the administrative and error costs incurred in applying the possible options must be compared with the benefits. The benefits here are social benefits to be measured by the increase in consumer welfare and the reduction of social deadweight loss. In order to achieve effective deterrence, the benefits must exceed the costs.

Error costs (C_e) may 'occur when practices that do not harm economic welfare are falsely prohibited (type I errors/false positives) or harmful practices are allowed (type II errors/

[44] Peter Bryant and Edwin Eckard, 'Price-fixing: The Probability of Getting Caught' (1991) 73 Rev Economics & Statistics 531 (probability between 13 per cent and 17 per cent); Emmanuel Combe and Constance Monnier, 'Fines against Hard Core Cartels in Europe: The Myth of Overenforcement' (2011) 56 Antitrust Bulletin 235 (probability of 15 per cent). See also Van den Bergh (n 37) 400.

[45] See Van den Bergh (n 37) 401 (and the economic studies quoted therein). It should be noted that the economic studies used by Van den Bergh focused on cartels rather than excessive data collection and misuse of data, but it seems safe to assume that the deterrence mechanism works to a large extent similarly for all undertakings engaged in anti-competitive behaviour.

[46] George Stigler, 'The Optimum Enforcement of Laws' (1970) 78 J Political Economy 526.

[47] Michael Faure, Anthony Ogus and Niels Philipsen, 'Curbing Consumer Financial Losses: The Economics of Regulatory Enforcement' (2009) 31 L & Policy 161.

[48] Ibid 167.

false negatives)'.[49] More specifically, false positives refer to decisions that hold exclusionary conduct by a monopolist unlawful when it should not be so held,[50] whereas false negatives refer to decisions that fail to find violations where the conduct unreasonably and unnecessarily excludes either new or existing competition.[51] Since both types of errors give rise to welfare losses, the optimal enforcement regime requires avoiding false negatives and false positives,[52] or at least striking a balance between minimizing the likelihood of false negatives and false positives.

Deterrence is deemed efficient if the administrative costs—that is, (C_a)—are lower than the benefits resulting from prohibiting the anti-competitive practice.[53] Administrative costs are deemed sufficiently low when the 'benefits of the competitive process' that are preserved outweigh the 'administrative costs of detection (information costs) and sanctioning violations' of the competition rules and/or data protection rules.[54] Achieving optimal deterrence of the enforcement system requires minimizing 'the sum of social costs resulting from the infringement and the costs of enforcement'.[55] As such, it requires minimizing the administrative costs (the resources spent on the detection, prosecution and punishment) and costs of the legal and economic support for the competent authorities and undertakings (which are purely social deadweight loss).

Non-economic considerations

Retributive justice 'requires that offenders get a punishment that adequately reflects the societal disapproval of their behaviour'.[56] For example, in China and the EU, the upper ceiling fine of 10 per cent of the turnover of the undertaking in the previous business year[57] imposed for a violation of competition rules seems inappropriate to achieve deterrence. Instead, the fine seems to reflect the requirements of retributive justice—that is, 'the maximum fine reflects the degree of disapproval of the behaviour'.[58] As discussed under Becker's model, achieving full deterrence requires a fine of at least 150 per cent of the annual turnover of the products concerned by the violation. However, the involved parties enjoy the autonomy to engage in economic activities in markets, and competition law intervenes in case anticompetitive effects are created; therefore, infringement of competition law seems less serious than other forms of disproved conduct sanctioned by criminal laws in jurisdictions of China and the EU. As such, fines are more likely to serve as punishment for undertakings that violate competition law, which is in line with the requirements of retributive justice and proportionality. This rationale also applies to data protection law.

Data protection is another important factor to be considered in this theoretical framework. There seems to be some overlap between data protection and privacy. Some scholars consider privacy as part of consumer welfare[59] as a non-price parameter and propose to use

[49] Van den Bergh (n 37) 382.

[50] Peter Carstensen, 'False Positives in Identifying Liability for Exclusionary Conduct: Conceptual Error, Business Reality, and Aspen' (2008) 2 Wisconsin L Rev 296.

[51] Ibid 321.

[52] Peter van Wijck, 'Loyalty Rebates and the More Economic Approach to EU Competition Law' 17 (2021) Eur Competition J 1.

[53] Van den Bergh (n 37) 382.

[54] Ibid.

[55] Ibid.

[56] Ibid 383.

[57] Art 57 of the AML (n 11). EC Regulation no 1/2003 on the Implementation of the Rules on Competition Laid Down in arts 81 and 82 of the Treaty, art 23.

[58] Van den Bergh (n 37) 403.

[59] Privacy harms can reduce consumer welfare. See Peter Swire, 'Protecting Consumers: Privacy Matters in Antitrust Analysis' *CAP20* (19 October 2007) <https://www.americanprogress.org/article/protecting-consumers-privacy-matters-in-antitrust-analysis/> accessed 30 July 2024.

traditional approaches to tackle concerns caused by exploitative abuse—in particular, unfair terms to deal with excessive data collection and misuse of data in Article 102 of the TFEU.[60] Some take data protection law directly into account in the enforcement of competition law.[61] This is the approach of the Bundeskartellamt, which considers the violation of GDPR as the benchmark of abuse of dominance. This would lead to the critique that competition authorities might become enforcers of data protection law. Furthermore, it is also possible to take privacy as a fundamental value in broader reasoning about abuse.[62] This is in line with the approach of the German Federal Court of Justice, which uses the German constitutional right of information self-determination. Nevertheless, data protection is an inherent objective of data protection law, which enables data protection law to serve as an appropriate instrument to directly protect data. This is the approach of the Didi case, which tackles data protection concerns caused by dominant undertakings in the data protection approach.

Undertakings can make enormous profits if there is no restriction on the collection and use of personal data. It would lead to an increase in social output and thereby promote static efficiency. Under the standard of social welfare, the economic gains go to the undertakings. However, this does not apply under the consumer welfare standard. Privacy/personal data protection is considered a non-economic parameter of consumer welfare. The excessive collection and misuse of data seems to be a detriment to data protection and would lead consumers to be worse off. However, in oligopolies, the collection and use of data may benefit consumers through intensified competition and thereby raise consumer surplus at the expense of industry profits.[63] By contrast, in monopolies, consumers are placed in a vulnerable position with an information disadvantage, which would result in the exploitation of consumers.[64]

Therefore, whether competent authorities have to make trade-offs when intervening in the market to deal with excessive data collection and misuse of data by dominant undertakings depends on the welfare standards and the specific market conditions. Under the social welfare standard, competent authorities only need to take the benefits of undertakings into account. Under the consumer welfare standards, it depends on the market conditions. In oligopolies, the collection and use of data may benefit consumers through intensified competition. In monopolies, competent authorities should take a more stringent approach to excessive data collection because it will ultimately harm consumers.

THE EVALUATION OF THE TWO APPROACHES

The theoretical framework will be applied to assess and compare the effectiveness of the competition law approach and data protection law approach employed in the Chinese Didi case and the German Facebook case. In the meantime, the holistic overview of different considerations and trade-offs will be further examined in this section. To determine whether the two cases achieve effective deterrence, we measure the two decisions under Becker's model, $G < p.F$. In the German Facebook case, the Bundeskartellamt did not impose any fines on

[60] Marco Botta and Klaus Wiedemann, 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (2019) 64 Antitrust Bulletin 428. See also Erika Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy', Temple University Legal Studies Research Paper no 2021-40 (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737> accessed 30 July 2024.

[61] Maximilian Volmar and Katharina Helmdach, 'Protecting Consumers and Their Data through Competition Law? Rethinking Abuse of Dominance in Light of the Federal Cartel Office's Facebook Investigation' (2018) 14 Eur Competition J 195. See also Giulia Schneider, 'Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's investigation against Facebook' (2018) 9 J Eur Competition L & Practice 213.

[62] Kerber and Zolna (n 7) 222.

[63] Qian Li, Niels Philipsen and Caroline Cauffman, 'AI-enabled Price Discrimination as an Abuse of Dominance: A Law and Economics Analysis' (2023) 9 China–EU LJ 51, 58.

[64] Ibid 57.

Facebook. In contrast, the Chinese Didi case imposed a fine of 8.026 billion yuan on Didi, accounting for 4.6 per cent of its total turnover in the previous business year. This fine is close to the maximum fine specified in the PIPL, which is 5 per cent of the previous year's revenue.

In addition, a fine of 1 million yuan was imposed on the chief executive officer and president of Didi, respectively, which is the maximum fine on company executives of the PIPL. By comparing the sanctions of the two cases, the amount of fines seemingly indicates the stronger deterrence of the Chinese Didi case than no fines at all in the German Facebook case. As discussed earlier in this article, a fine of no less than 150 per cent of the annual turnover would be needed to reach full deterrence based on the formula, $G < p.F$. Although competition law does not aim for full deterrence, the fines imposed are minimal compared to the substantial profits gained from illegal activities, rendering them ineffective as a deterrent. Notably, this was the first instance in which the Bundeskartellamt applied data protection law to identify an abuse of dominant position under competition law, and it was not certain whether the authority had the legal power to do so. This may provide further explanation as to why no fine was imposed, especially since under German law, imposing fines requires a far more rigorous assessment of the case compared to decisions made without financial penalties.

The optimal enforcement requires that the error costs (C_e) and administrative costs (C_a) are minimized. The Facebook decision has triggered an intensive debate on the procedure and substance of its decisions. The debate involves the competence of the Bundeskartellamt to apply data protection law, the appropriateness of the decision, the relationship between data protection law and competition law, and so on. There is no doubt that Facebook abused its dominant position by making use of its social network conditional on it being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account. The harm to competition and consumer privacy should be corrected. Therefore, the debate is whether the methods are appropriate but not whether the behaviour *per se* should be prohibited. In other words, the Bundeskartellamt was trying to avoid false negatives but triggered concerns about the competence of competition law and the potentially false positives via explicitly applying data protection law in a competition case. It turns out that this decision has been supported by the CJEU, leading to overarching effects to correct the potential error costs—in particular, false negatives when tackling concerns brought about by excessive data collection and misuse of data by Facebook.

What is worth mentioning is that the administrative costs seem to be high in the Facebook case. In order to reach a decent and persuasive decision, the Bundeskartellamt conducted a market definition, a market dominance test, and the assessment of abusive data policy, which requires vast amounts of resources spent on investigation, detection, and punishment. In the meantime, it also leads to high expenses on legal and economic support for the competition authorities and undertakings, which is purely social deadweight loss. The court proceedings involve the two instances of the Dusseldorf Higher Regional Court and the German Federal Court of Justice, and the further proceedings of the Dusseldorf Higher Regional Court and the CJEU have resulted in similar costly situations. After five years of effort, the Bundeskartellamt ultimately wrapped up the proceedings on 10 October 2024.[65] The long-lasting administrative and judicial proceedings consume human resources and the budget of the administrative and judicial system as well as the economic and legal expenses of Facebook in the proceedings. In this sense, the German Facebook case seems to amount to high enforcement costs and social deadweight loss.

Interestingly, the Bundeskartellamt acknowledged that its decision to close the case against Facebook does not imply that all competition concerns have been entirely

[65] Bundeskartellamt, 'Facebook proceeding concluded' (10 October 2024) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html?nn=49114> accessed 18 October 2024.

addressed.[66] This conclusion is based not only on the fact that the measures implemented by Facebook were deemed a sufficiently suitable package to justify discontinuing its enforcement action but also on the availability of effective and appropriate tools from other authorities (such as the DMA and GDPR) to facilitate further improvements for users of Facebook services in the EU, if necessary. However, this closure does not imply any findings regarding Facebook's compliance with the obligations arising from these tools. As a result, there remain possibilities to trigger the enforcement actions of other authorities (such as the European Commission), which could lead to additional enforcement costs.[67]

However, the enforcement costs seem to be properly justified, which can be attributed to the responses of the parties involved and the inherent requirements of EU judicial systems aiming to guarantee legal certainty and legal predictability. Facebook disagreed with the Bundeskartellamt's decision and brought the dispute before the competent courts for judicial review, which would incur expenses and resources in terms of economic, legal, and technical support. Nevertheless, Facebook might contest this decision since it was not certain whether the Bundeskartellamt had the jurisdiction to apply data protection law to act against it. There is still a possibility to reverse this case even when facing a tough regulator in Germany. This is different from the compliance in the Didi case.

Furthermore, the costs associated with a preliminary reference in Germany do not stem directly from the competition law but rather from the data protection approach, due to the fact that the decision was taken by an EU court that may—and, if deciding in the last instance, must—refer to the CJEU when the interpretation of EU law is uncertain and critical to the case's outcome. The costs of two instances of judicial review in Germany lie in the institution design, which aims to guarantee legal certainty and justice; putting it in the context of other controversial and significant cases, the expenses may incur as well. To this end, the enforcement costs and social deadweight costs can be justified to a large extent as they demonstrate how judicial systems work in practice rather than simply due to the application of competition law to address the concerns caused by excessive data collection and misuse of data in the Facebook case. Moreover, given a certain degree of similarity between the issues raised by competition law and data protection law, the Bundeskartellamt regularly exchanged views with the data protection authorities during the proceeding, which might reduce the error costs.[68] This demonstrates the Bundeskartellamt's efforts to strike a balance between minimizing the risks of both false negatives and false positives. Additionally, the Facebook case went to a higher level of courts resulting in a persuasive precedent for the future case. In this sense, it creates a positive externality, which, in return, compensates for the high enforcement costs, although this is outside the scope of analysis in this article.

Unlike Facebook, Didi swiftly released a statement expressing its firm commitment to comply with the penalty decision and actively carrying out rectification measures after the investigation and publication of the administrative penalty by the Cyberspace Administration of China. It was Didi's deliberate choice that it did not bring this decision before the competent court or seek administrative review before the State Council, although the Administrative Law offered the possibility for Didi to do so. Didi might have recognized that there was little to be gained from an appeal as the decision was well-articulated and likely to be upheld. In any case, Didi's compliance with the penalty decision saved the administrative costs to further detect and punish the infringement, as well as the expenses of legal and technological support. The maximum fine imposed on Didi appears to mitigate false negatives and uphold the overall value of data protection. Therefore, compared with the German

[66] Ibid.
[67] Ibid.
[68] Ibid.

Facebook case, the administrative costs seem to be low, and the error costs seem to be minimized.

As for the achievement of retributive justice, this is reflected by the remedy of an additional option for the consent of users of Facebook as imposed by the Bundeskartellamt. The order given to require additional consent forced Facebook to revise its customer terms and provide consumer choices, which can adjust the unbalanced position of the two contractual parties. To correct the misbehaviour conducted by Facebook, this behavioural remedy required compliance scrutiny and supervision checks, which inevitably led to additional administrative costs, but also minimized the potential error costs, especially false negatives carrying more benefits to parties involved in the long run.

In contrast, the punishment of Didi also demonstrated the goal of retributive justice. As already discussed, Didi was imposed an almost up-ceiling fine as provided by the PIPL of approximately 5 per cent of its turnover in 2021. Beyond that, during the investigation between July 2021 and July 2022, all of Didi's apps were removed from app stores and prohibited from accepting new users, which led to the decrease of its market share from 90 per cent to 70 per cent. This behavioural remedy allowed Didi's competitors to enter the ride-hailing market, thereby enriching consumer choices and imposing competition restrictions on Didi to carve up its monopoly market share. In other words, this behavioural remedy can guarantee consumer welfare and drive competition on the merits. In this sense, this remedy can also contribute to minimizing the error costs—in particular, false negatives to address concerns brought about by excessive data collection and misuse of data by Didi.

Data protection is of great importance in the excessive data collection and misuse of data. Both the competition law approach and the data protection law approach in the two cases demonstrate the proactive attitudes of regulators to personal data protection in the scenarios of excessive data collection and misuse of data conducted by dominant undertakings. In the German Facebook case, consumers' personal data was exploited by Facebook due to the imbalanced contractual positions of the two parties, and the investigation was launched within the framework of abuse of dominant position under competition law. Exploitative abuse of dominance requires the assessment of the harm to consumer welfare. Even if the protection of consumer welfare is an objective of competition law, it is protected indirectly, but it is premised on the definition of relevant markets and the determination of market dominance. In addition, the Bundeskartellamt's explicit application of the GDPR when determining abuse of dominance has sparked heated discussions and calls for responses from the judiciary regarding the competence of competition authorities and the separation of labour from competition and data protection laws. Potential confrontations between parties and contentious judicial responses create resource and expense costs that are incompatible with efficiency to a certain extent.

Notably, data protection law pursues to protect data in an explicit manner. In the Didi case, there seems to be no doubt about the competence of the Cyberspace Administration of China. The investigation, detection, and punishment of Didi's excessive data collection and misuse of data are a response to the achievement of the objective data protection law. As far as Didi is concerned, the implementation of the data protection law contributes to, on the one hand, correcting market failures in the form of market dominance and information asymmetry, and, on the other hand, promoting legal certainty and legal predictability. In this sense, data protection law seems a more suitable and direct instrument to tackle data protection concerns caused by excessive data collection and misuse of data by dominant technology undertakings.

Based on the comparative analysis of the two cases, the potential conflict between efficiency and data protection requires the competent authorities to make trade-offs when

Table 2. Evaluation of the two cases

		Facebook Case	Didi Case
Components of Optimal Deterrence			
1	Deterrence	Low	Low
2	Error Costs	Low	Low
3	Enforcement Costs	High	Low
Non-economic Considerations			
1	Retributive Justice	High	High
2	Data Protection	High	High

dealing with excessive data collection and misuse of data. Both Facebook and Didi would make massive amounts of profits if they had unlimited access to consumer data, which would lead to an increase in social output and thereby promote static efficiency under the social welfare standard. However, consumers would be worse off with unlimited data collection facing the tech giants, Facebook and Didi.

Under consumer welfare standards, especially in oligopolies, the collection and use of data may benefit consumers through intensified competition and thereby raise consumer surplus at the expense of industry profits. However, Facebook and Didi are monopolists with overwhelming market power in the relevant markets. Consumers are placed in a vulnerable position, which results in the exploitation of consumers, as demonstrated in the two cases. Consumer perception of unfairness makes the situation worse, in particular, given the unbalanced information advantage between the consumers and the dominant undertakings, Facebook and Didi. Therefore, it makes sense for competent authorities to take a more stringent approach to deal with excessive data collection and misuse of data considering the severe exploitation of consumers (Table 2).

OBSERVATION

The excessive data collection and (mis)use of data can result in the coexistence of two market failures: namely, market dominance and information asymmetry, which in turn interact with each other in digital markets and trigger simultaneous concerns about competition law and data protection law. The German competition authority employs a competition law approach to deal with excessive data collection and (mis)use of data by dominant technology undertakings, which can be observed in the Facebook case. Chinese data protection authorities tackle similar concerns via a data protection law approach under the PIPL and the Cyber Security Law.

To answer the question of whether one approach is preferred over the other, this article conducted a comparative law and economics study on the Chinese Didi Case and the German Facebook Case to examine the effectiveness of the data protection law approach and the competition law approach. Compared with no fine in the Facebook case, the huge number of fines imposed on Didi seemingly demonstrates a stronger deterrent effect. Nevertheless, although competition law does not pursue full deterrence, the fines imposed are minimal in relation to the substantial profits generated from illegal activities, making them an ineffective deterrent. The enforcement costs in the Facebook case seem to be higher than that of the Didi case. However, these costs seem to be justifiable due to (i) the responses of the parties involved (regarding compliance and appeal options); (ii) the fact of the two instances of judicial proceedings initiated by Facebook; and (iii) the preliminary

ruling as required in the proceeding when the interpretation of EU law is uncertain and critical to the case's outcome.

Admittedly, the prerequisites of market definition and dominance determination under abuse of dominance in competition law require more expenses and resources on legal and economic support compared with the direct assessment of the infringement of excessive data collection and misuse of data in data protection law. This would lead to higher enforcement costs under the competition law approach, especially in addressing concerns brought about by the excessive data collection and misuse of data by dominant technology undertakings such as Facebook and Didi. Nevertheless, the investigation and punishment of the two cases aim to minimize the error costs, especially false negatives, to address concerns caused by excessive data collection and misuse of data conducted by the two dominant technology undertakings. In addition, the behavioural remedies in the two cases both demonstrate the pursuit of retributive justice and data protection, although they were imposed by competition authorities and data protection authorities separately.

In terms of how competent authorities should respond to concerns caused by the excessive collection and (mis)use of data by dominant technology undertakings, the potential conflict between efficiency and data protection requires the competent authorities to take different considerations into account and even make trade-offs on a case-by-case basis. Dominant undertakings like Facebook and Didi would make massive amounts of profit if they had unlimited access to consumer data, which would increase social output and thereby promote static efficiency under the social welfare standard, despite the fact that consumers would be worse off. Under consumer welfare standards, especially in oligopolies, the collection and use of data may benefit consumers through intensified competition and thereby raise consumer surplus. However, in monopolies, consumers are placed in a vulnerable position, which results in the exploitation of consumers given the unbalanced information advantage between the consumers and the dominant undertakings. Therefore, it makes sense for competent authorities to take a more stringent approach to deal with excessive data collection and misuse of data by dominant technology undertakings.

It is worth noting that the data protection approach would be cost-effective to intervene in the market *ex-ante* to address concerns brought about by excessive data collection and misuse of data conducted by dominant undertakings, since its main objective is to guarantee data protection. If data protection law intervenes at an early stage of the collection and processing of data, it can decrease the likelihood of excessive collection and misuse of data. Meanwhile, it can also reduce the exclusionary and/or exploitative effects of competition and lower the market entry barrier that benefits from the collection and processing of significant amounts of data. Therefore, the *ex-ante* intervention of data protection law can effectively tackle concerns caused by market dominance and information asymmetry. In contrast, competition law aims to protect competition on the merits and indirectly protect consumer welfare. The controversy surrounding the application of data protection law by competition authorities has been clarified by the CJEU but might still lead to additional information costs and error costs in enforcement. Nevertheless, there is no doubt that close cooperation between the competition authorities and data protection authorities would contribute to achieving effective deterrence when tackling concerns arising from excessive data collection and misuse of data.

The Chinese Journal of Comparative Law, 2024, 13, 1–16
https://doi.org/10.1093/cjcl/cxae018
Article