International Competition Network

Competition law enforcement at the intersection between competition and privacy: *Agency considerations*

2024

ICN Steering Group Project

WHAT IS THE PURPOSE OF THIS HANDBOOK?

This handbook offers a list of issues for agencies to assess when privacy and competition concerns intersect, to help them navigate their decision-making processes. The aim here is for policymakers to recognize the potential tensions between competition and privacy regulation, take steps to minimize these tensions where possible, and align incentives so that firms compete to promote privacy and data protection. At times, however, conflicts will arise despite the alignment of privacy and competition policies. So, this handbook also discusses some principles to consider in deciding these trade-offs, including standards that align with rule-of-law principles.

When does privacy intersect with competition? Often enforcement cases and mergers involving digital platform markets come to mind. But in practice, competition agencies may see this issue in many businesses across the economy (including in the health, transport, and agriculture industries) that use digital technologies. And it may arise in different contexts, whether in conduct enforcement, merger review, proposing remedies, market inquiries, or proposing regulations. Thus, this handbook is intended to have a broad application.

What happens, however, when privacy and competition clash? There is no "one-size-fits-all" solution in addressing this trade-off. After all, these trade-offs might vary among jurisdictions. Different jurisdictions may have different laws and policy approaches to competition and privacy; the laws and policies are also in flux in many jurisdictions. Moreover, the trade-offs may depend on, among other things, the agencies enforcing the competition and privacy regulation (whether they fall within one agency or are handled by different agencies), the agencies' missions, and the extent to which the type of harm falls within their jurisdiction. Keeping this in mind may help the respective agencies (or divisions within the agency) determine when they should intervene and when they should yield to other authorities. For example, not every privacy issue overlaps with an antitrust concern (such as a landlord hiding a surveillance camera in a tenant's bedroom), just as not every competition concern (such as bid rigging among commodity producers) raises a privacy issue. These simple examples illustrate how the underlying policy concerns involved in competition and privacy enforcement differ and the problems that those policies aim to solve.

This handbook is the outcome of the ICN Project "Competition law enforcement at the intersection between competition, consumer protection, and privacy," launched in 2020. It has been informed by a significant amount of work including an *Issues Paper* and a *Summary of ICN Members actions and policy responses.*[1] Of course, as our experience and understanding of these issues deepen, we expect the frameworks outlined herein to be updated.

STRUCTURE

Part I presents four possible relationships between privacy and competition, in an academic-style context.

[1] Such documents can be downloaded from the dedicated "intersection" web page on the ICN website: https://www.internationalcompetitionnetwork.org/working-groups/icn-operations/intersection-project/.

Part II provides a checklist of of practical issues and questions for competition agencies to consider in assessing the privacy/antitrust relationships in any conduct enforcement, merger, remedy, or policy matter.

When privacy and competition policies conflict, jurisdictions may weigh these values differently in assessing the trade-offs. While recognizing those differences, Part III provides several principles for jurisdictions to consider, including a checklist to foster inter-agency coordination.

I. WHAT IS "INTERSECTION" AND THE DATA-DRIVEN REASONS FOR IT?

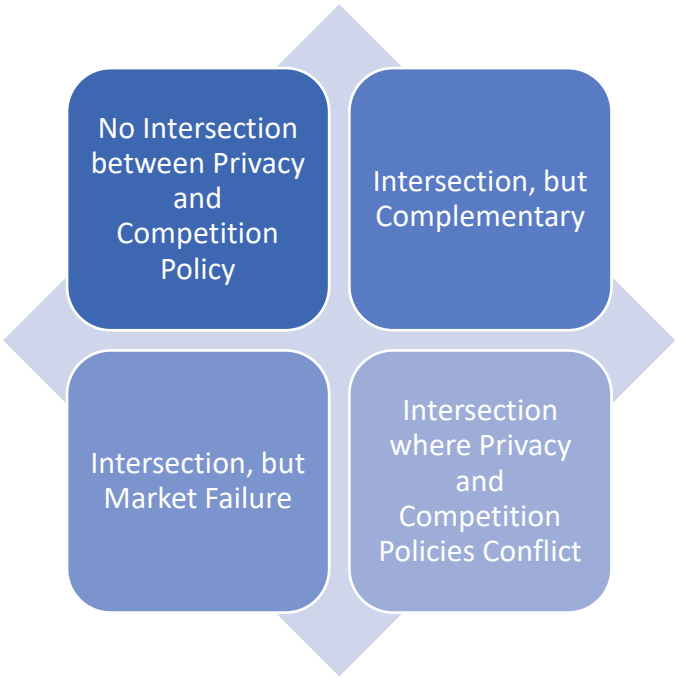
Competition agencies, as of 2024, recognize privacy as a potentially important parameter of competition, especially in the digital platform economy. A consensus among agencies has emerged on, among other things:

- The features of the digital platform economy (e.g., the importance of economies of scale, network effects, and high entry barriers) can lead to winner-take-most markets;
- Personal data can play a key role in attaining and sustaining market power[2];
- Excessive collection of personal data can be seen as the equivalent of charging an excessive price, and how firms can exploit their market power by extracting an excessive amount of personal data from consumers;
- Extracting an excssive amount of personal data can raise entry barriers and depress privacy levels; and
- The need for cooperation among privacy and antitrust agencies and the need for increased cooperation globally.

But there has been less discussion (and consensus) on the relationship between competition and privacy regulation. One can see at least four possible relationships, as Figure 1 reflects below, and as this Part discusses in greater detail.

[2] Non-personal data can also play a key role to compete, but is not discussed here, as it typically does not raise privacy issues.

Figure 1



While the focus of this handbook is on the intersection between privacy and competition policies, it is important to note that other policy concerns, such as consumer protection concerns, can raise both privacy and competition concerns. This can include, for example,

1) deceptive privacy statements to trick users to adopt their products or deceptive statements about their cost (with the aim of dominance in markets with strong network effects) (see Italy's Facebook case),[3] and

2) use of dark patterns and choice architecture to nudge users to opt for less privacy-friendly options.[4]

[3] For example, in its 2018 Facebook case, the Italian Competition Authority ("AGCM") ascertained that the promotions of "apparent gratuity" of the services offered by the Facebook social network platforms (e.g., "FB is free and it will be free forever") was deceptive in that, at the moment of creating an account, it omitted information about the mandatory transfer of the right to exploit one's personal data (often also shared with third parties/business partners unknown to users). Even in the absence of a "monetary transaction" (exchange of currency), the AGCM was able to identify an "economic transaction" and, therefore, a "commercial practice" for the purpose of applying consumer protection law, by recognizing users' personal data exploitation rights as the new "digital currency" in the context of the so-called "zero price"/data driven economy. See press release in English: https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes. In November 2021, the AGCM fined Google ten million euros for some unfair and aggressive commercial practices related to the utilization of user data, such as the omission of information about the collection and use of personal data and the set-up of an opt-in as default option for data sharing consent. See press release: https://en.agcm.it/en/media/press-releases/2021/11/PS11147-PS11150.

[4] See, for example, Bringing Dark Patterns to Light, FTC Staff Report, September 2022, https://www.ftc.gov/reports/bringing-dark-patterns-light; Forbrukerrådet, *Deceived by Design: How tech companies use dark patterns to discourage us for exercising our privacy rights* (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

For both examples, it is also worth noting that consumer protection concerns may raise privacy concerns even if the practice does not increase market concentration, lessen competition, or enable the firms to gain market power. Thus, the cause of the problem at hand or its solution, at times, may necessitate looking at other policies, including consumer protection.

A. First Category: Where Privacy And Competition Policies Do Not Intersect

While the goals of competition and privacy laws may vary by jurisdiction, in every jurisdiction, there are large swaths of competition concerns that do not raise any privacy or data protection issues and vice versa.

One simple example from the US illustrates this point. In *Hamberger v. Eastman*,[5] a couple sued their landlord for invading their privacy, after learning that the defendant installed and concealed "a listening and recording device" in their apartment. Here, their "injury to personality" – the quality of being a person – was central to their privacy claim, but far afield from competition concerns (especially when there was no allegation that the landlord possessed (and abused) a dominant position in the rental market). Indeed, these types of privacy cases typically never reach the competition agency.

Likewise, many competition cases do not raise any privacy concerns. Examples include bid rigging among suppliers and price-fixing cartels.

B. Second Category: Where Privacy and Competition Policies Intersect but Are Complementary

The underlying assumption of this category is that privacy and data protection are important non-price parameters of competition.[6] Competitive pressure causes firms to improve their privacy policies and data protection measures to comport with consumers' demands. The lack of competition can potentially reduce privacy protections below competitive levels and may increase the collection of personal data above competitive levels.[7]

---

[5] 106 N.H. 107 (New Hampshire 1964).

[6] A recent survey by the Office of the Australian Information Commissioner found that privacy is the third most important factor when choosing a product or service, coming only after quality and price. See Australian Community Attitudes to Privacy Survey 2023.

[7] *See, e.g.*, UK Competition & Markets Authority, *Online Platforms and Digital Advertising: Market Study Final Report* ¶¶ 2.84, 3.151 (2020) [hereinafter *CMA Final Report*]; Australian Competition & Consumer Commission (ACCC), *Digital Platforms Inquiry—Final Report*, at 374 (2019) [hereinafter *ACCC Final Report*]; *Organisation for Economic Co-operation and Development Secretariat*, DAF/COMP(2020)1, *Consumer Data Rights and Competition–Background Note* ¶¶ 69, 99, 100 (2020) [hereinafter OECD Consumer Data Rights and Competition]; Jason Furman et al., *Unlocking Digital Competition - Report of the UK Digital Competition Expert Panel,* at 49 (March 2019), https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [hereinafter *Furman Report*]; *Organisation for Economic Co-operation and Development,* DAF/COMP/WD(2020)51, *Consumer Data Rights and Competition–Note by the United Kingdom* ¶ 25 (June 2, 2020) (noting how privacy and data protection rights "may constitute an aspect of service quality on which firms can differentiate themselves from their competitors" and a merger's "reduction in privacy protection . . . may . . . be interpreted as a reduction in quality"); *Organisation for Economic Co-operation and Development*, DAF/COMP/WD(2020)40, *Consumer Data Rights and Competition—Note by the European Union* ¶ 51 (2020) ("Market investigations in specific cases, such as *Microsoft/LinkedIn*, have further supported the view that data protection standards can be an important parameter of competition, particularly in markets characterised by zero-price platform services where the undertaking has an incentive to collect as much data as possible in order to better monetise it on the other side of the platform."); Furman

Possible anticompetitive conduct

Competition agencies have identified several possible anticompetitive actions that can harm privacy, including:

1. Exploitative abuses of dominance

Subject to the privacy and competition laws in the relevant jurisdiction, this exploitation could be considered (i) a degradation of privacy protection, (ii) excessive collection of personal data, or (iii) an infringement of obligations set by other regulations, such as data protection or privacy.[8] Germany's Bundeskartellamt, for example, found that Facebook abused its dominant position by "collect[ing] an almost unlimited amount of any type of user data from third party sources, allocat[ing] these to the users' Facebook accounts and us[ing] them for numerous data processing processes."[9] Facebook extracted data even when individuals were not using the company's services.[10] In affirming, the European Court of Justice recognized that the competition authority, in cooperating with the relevant privacy authority, can consider whether a dominant firm's collection and processing of personal data is consistent with the jurisdiction's other rules (including its privacy regulation) in assessing whether that conduct constitutes an abuse.[11]

The Competition Commission of India raised similar concerns when Meta's dominant messaging app WhatsApp changed its privacy policy to integrate its users' data with the other personal data it collected across its platforms. This amounted to a "degradation of non-price parameters of competition, viz., quality which results in objective detriment to consumers, without any acceptable justification, and that such conduct prima facie amounts to the

Report at 50 ("A small number of large digital companies occupy strategically important gateway positions in digital markets, wielding significant bargaining power over their business users as a result… these market dynamics will lead to business users of platforms accepting worse terms than they would face if multiple platforms were competing with one another in each market.").

[8] See Bundeskartellamt Facebook decision; see also World Bank, Antitrust and Digital Platforms: An analysis of global patterns and approaches by competition authorities. EFI Insight-Trade, Investment and Competitiveness, at 37 (Washington, DC: World Bank 2021) [hereinafter World Bank 2021 Digital Platforms Report] (finding that issues of data protection and privacy are more prevalent in the evaluations of competition authorities in high-income jurisdictions relative to middle- or low-income jurisdictions).

[9] *See, e.g.*, Press Release, Bundeskartellamt at 3, Bundeskartellamt prohibits Facebook from combining user data from different sources (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2; Case B6-22/16 – Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing; Facebook Inc. v, Bundeskartellamt, KVR 69/19 German Federal Court of Justice (June 23, 2020).

[10] Ibid. Facebook is not alone. See, for instance, World Bank, World Development Report 2021: Data for Better Lives at 109 (Washington, DC: World Bank. 2021), doi:10.1596/978-1-4648-1600-0 (noting how a major part of Google's data collection occurs when a user is not directly engaged with any of its products). In the meantime, based on Sec. 19a GWB which was established in 2021, the Bundeskartellamt took a commitment decision concerning Google's data processing practices. The commitments require Google to give users better choice as to how Google processes their data, see Press Release at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/05_10_2023_Google_Data.html (October 3, 2023).

[11] Meta Platforms (Case C-252/21) [2023].

imposition of unfair terms and conditions upon the users of the WhatsApp messaging app."[12] India's Supreme Court held that this inquiry was within the competition authority's jurisdiction.

2. Anticompetitive exclusionary conduct that can foreclose privacy-friendly rivals and entrants.

A dominant firm may also seek to degrade the superior privacy protections offered by rivals. Consider the European Commission's Google Android case. Google imposed restraints on original equipment manufacturers and mobile network operators to ensure that traffic on Google Android devices would be directed to Google's search engine. This had, in the Commission's view, the anticompetitive effect of "depriving Google's competitors – such as Qwant or Seznam – of the possibility of competing with it on their own merits, and EU consumers of the advantages of effective competition, such as the possibility of using a search engine that prioritises the protection of privacy, is adapted to particular linguistic features or focuses on value-added content, particularly in the field of information."[13]

3. Data-driven mergers that can help firms attain or maintain their dominance.

Mergers may lessen privacy protection in markets where (i) privacy protection is an important non-price parameter of competition; (ii) the acquired firm distinguished itself by offering better privacy protections than the acquiring firm; and (iii) the dominant firm has the incentive and ability post-merger to degrade privacy protections for the acquired firm's customers. (See the Google/Fitbit case note below.)

4. Mergers that eliminate a potential threat that offers superior privacy protections.

Consider Meta's acquisition of WhatsApp. As the FTC alleged in its complaint, Meta viewed WhatsApp as a potential threat to its dominance in social networks, and degraded WhatsApp's privacy policies after acquiring it. (The FTC's litigation against Meta remains ongoing, as of 2023.)

5. Sharing personal data to foster collusion (and colluding to depress privacy standards).

Consider, for example, litigation in the United States where many landlords allegedly shared with a third-party pricing algorithm "real-time, competitively sensitive, non-public data" which included "non-public information regarding inventory, prices of actual leases, concessions offered, and detailed information about amenities and rental unit value."[14] The defendant landlords allegedly colluded to raise rents by sharing sensitive company data and delegating their rent-setting authority to the third-party pricing algorithm. Privacy concerns were not

---

[12] OECD, Annual Report on Competition Policy Developments in India, 2022 (September 5, 2023), https://one.oecd.org/document/DAF/COMP/AR(2023)45/en/pdf.

[13] *See, e.g.*, EC Google Android case para 65.

[14] Complaint ¶ 100, filed in District of Columbia v. RealPage Inc. (D.C. Superior Ct. Nov. 1. 2023), https://oag.dc.gov/release/attorney-general-schwalb-sues-realpage-residential. See also Statement of Interest of the United States, filed in In Re: RealPage, Rental Software Antitrust Litigation (No. II), 3:23-md-03071 (M.D. Tenn. filed Nov. 15, 2023).

raised in that litigation. But one can imagine in the future other cases where rivals share users' personally sensitive information to a third-party algorithm, which, as a result, can harm both competition and privacy.

6. Using market power to extract personal data to harm competition.

For example, a dominant firm may condition interoperability with its platform on the condition that firms share with it the personal data of their users. (Consider the FTC's complaint against Meta.[15])

7. Frustrating the right to data portability by denying interoperability of the dominant firm's platform with competing operators that offer superior privacy policies.

This tactic can prevent the development of innovative and potentially more privacy friendly alternatives. Alternatively, it can prevent less-privacy concerned users from trading and monetizing their personal data via intermediaries (see Italy's Google/Hoda case[16]).

This anticompetitive behavior also gives rise to concerns about users being "locked in", lacking information on viable outside options, or being unaware of the full scale of the collection and subsequent use of their personal data.

Indeed, this anticompetitive behavior can be far worse than when a monopoly charges higher prices. When a monopoly sets an excessive price in markets where the prices are transparent, consumers, especially price-sensitive ones, are often aware of this abuse of dominance. The monopoly pricing might eventually attract entrants or disruptive innovators eager to serve the monopoly's dissatisfied customers. With data, however, consumers may be unaware of the amount and scope of personal information that is being collected and the toll it has on their privacy and well-being.[17] They simply do not know the price. In addition, consumers may be unaware of the extent to which they are being exploited.

---

[15] Complaint ¶¶ 88-89, United States v. Facebook, Inc., No. 1:19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

[16] In July 2022, the Italian Competition Authority opened an investigation for alleged abuse of dominant position, following Google's refusal in sharing data on its platform with other platforms and, in particular, with the Weople App, managed by Hoda. The latter has developed new services through its innovative data investment bank: by signing up to its App Weople, users authorize Hoda, pursuant to article 20 of the GDPR, to collect, process and sell personal data on their behalf to businesses requesting them for client targeting, data collection and other purposes. Hoda receives a fee for this service. In the Authority's view, Google's conduct could compress the right to portability of personal data, established by Article 20 of the GDPR, and could constrain the economic benefits that consumers can derive from their data. At the same time, the alleged abuse could restrict competition because it limits the ability of alternative operators to develop innovative data-based services. See press release: https://en.agcm.it/en/media/press-releases/2022/7/A552. This investigation was closed in July 2023, by accepting Google's commitments. Two of the three commitments are aimed at providing solutions to Takeout (the service Google makes available to end users for taking up their data) to facilitate the export of data to third-party operators. Under the third commitment, Google will make available a test version of a tool that will enable other digital services operators to access personal data users generate through their activity on Google's services like YouTube and Search. See press release: https://en.agcm.it/en/media/press-releases/2023/7/A552.

[17] Furman Report at 22 (finding that many platforms operating in the attention market "provide valued services in exchange for their users' time and attention, while selling access to this time to companies for targeted advertising," but many consumers "are typically not consciously participating in this exchange, or do not appreciate the value of the attention they are providing") & 23 (noting that many consumers "are not aware

Implications for authorities

When privacy and competition are complementary, a decrease in competition and market contestability can harm individuals' privacy. In addition to antitrust tools, some jurisdictions may have comprehensive privacy and data protection laws to which enforcers and courts at times can turn to remediate and deter the anticompetitive measure. At other times, under this complementary perspective, competition agencies and courts can use privacy laws and corporate privacy and data protection policies to inform competition policy, including:

1. Substantive benchmarks

Competition enforcers and courts can turn to privacy laws to assess whether the collection and use of data were excessive and exploitative. Consider the Bundeskartellamt's Facebook case, where the competition agency considered the European data protection provisions as a standard for examining exploitative abuse. In determining whether Facebook's terms of service and the manner and extent to which it collected and used data violated European data protection rules to the detriment of users, the Bundeskartellamt closely cooperated with leading data protection authorities in clarifying the data protection issues involved.[18] As the European Court of Justice noted, "the compliance or non-compliance of that conduct with the provisions of the GDPR may, depending on the circumstances, be a vital clue among the relevant circumstances of the case in order to establish whether that conduct entails resorting to methods governing normal competition and to assess the consequences of a certain practice in the market or for consumers."[19]

2. Market definition

Competition enforcers and courts can turn to changes to corporate or industry-wide privacy policies to help define relevant antitrust markets. For example, they can use privacy degradation as part of a SSNDQ ("small, but significant, non-transitory decrease in quality") test, rather than the price centric SSNIP test (see, for example, the EU Android case[20]). When

---

of the extent or value of their data which they are providing nor do they usually read terms and conditions for online platforms"); CMA Final Report at ¶¶ 4.61–62.

[18] Under Europe's legal framework, a competition authority of a member state has a duty of "sincere cooperation" with the relevant privacy supervisory authority, and in view of this duty, "the national competition authority cannot depart from a decision by the competent national supervisory authority or the competent lead supervisory authority concerning those general terms or similar general terms." Where it has doubts as to the scope of such a privacy decision, the national competition authority must consult and seek the cooperation of those privacy supervisory authorities "in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment." Meta Platforms (Case C-252/21) [2023].

[19] Ibid.

[20] The competition agencies have applied a "quality degradation" or "SSNDQ test" in other non-privacy contexts. In the Google Android case, for example, the European Commission considered whether Apple's and BlackBerry's non-licensable operating systems were in the same market as licensable operating systems. To assess whether Google's dominant position on the market for licensable OSs was affected by the competitive constraint exerted on that market by the non-licensable OSs of Apple and BlackBerry, the Commission, inter alia, applied a "quality degradation" or "SSNDQ test." That test examined the reaction of users and app developers to a small but significant non-transitory decrease in quality of Android, i.e., "whether Google could refrain from developing and financing Android without its users and app developers responding by favouring an alternative." The General Court upheld the use of the SSNDQ test, noting how the product did

the instant product or service is ostensibly free and where privacy is an important parameter of competition, competition officials can assess the extent to which consumers would shift to alternatives, if a hypothetical monopolist depressed privacy protection by a small, but significant, level.

3. Assessing competitive effects

Competition enforcers and courts may be able to consider privacy laws and corporate privacy policies to inform their perspective when assessing competitive effects, such as assessing a merger's or restraint's likely impact on privacy. Consider the FTC's case against Meta. Even though Meta's acquisitions of Instagram and WhatsApp did not lead to higher prices, the FTC alleged "a decrease in service quality, lack of innovation, decreased privacy and data protection, excessive advertisements and decreased choice and control with regard to ads, and a general lack of consumer choice in the market for such services."[21] The FTC specifically alleged that "the lack of 'meaningful competition' has allowed Facebook to 'provide lower levels of service quality on privacy and data protection than it would have to provide in a competitive market.'"[22]

Thus, firms post-merger can exercise market power by decreasing privacy and data protection below current or competitive levels. (That leaves the issue of whether the privacy law will be a sufficient check on the exercise of market power, or whether the risk of harm and circumvention necessitates antitrust action.)

4. Designing remedies

Competition enforcers and courts may be able to consider privacy policies to inform the design of antitrust remedies. The Bundeskartellamt's Facebook case, for example, included as part of its remedy the requirement of free and informed consent to prevent the exploitation of users. This is in line with Article 4 no. 11 of Europe's privacy law, the GDPR, which provides that consent must be voluntary. Considering the monopoly position of Facebook in terms of its being an unavoidable gateway of social network services, the German agency ordered Facebook to combine personal data only under the user's voluntary consent, and that, in absence of consent, consumers shall remain free to use the service without Facebook data being combined with personal data from other sources.[23]

---

not lend itself to the classic hypothetical monopolist test aimed at verifying the market's response to a small but significant and non-transitory increase in the price of an asset. Moreover, defining a precise quantitative standard of degradation of quality of the target product cannot be a prerequisite for the application of the SSNDQ test. The hypothesis of a small deterioration in the quality of Android did not require – as in the case of the classic hypothetical monopolist test for which a small but significant and non-transitory increase in price can be more easily quantified – a precise standard of degradation to be set beforehand. All that matters is that the quality degradation remains small, albeit significant and non-transitory." Google Android para 180.

[21] Fed. Trade Comm'n v. Facebook, Inc., 581 F. Supp. 3d 34, 55 (D.D.C. 2022).

[22] Ibid.

[23] Bundeskartellamt, Press Release, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources, Feb. 7, 2019 (head of the German competition agency stating "Voluntary consent means that the use of Facebook's services must not be subject to the users' consent to their data being collected and combined in this way. If users do not consent, Facebook may not exclude them from its services and must refrain from collecting and merging data from different sources"); see also Meta Platforms (Case C-252/21)

Case study – Google/Fitbit

The European Commission's review of the proposed Google/Fitbit merger in 2020 considered the relationship between competition and data protection law.[24]

In its merger review, the Commission outlined a new theory of harm where the acquisition of complementary datasets can strengthen an entity's market power in downstream markets or give rise to foreclosure concerns. In particular, the Commission assessed concerns that Google's acquisition of complementary health and wellness data from Fitbit would strengthen Google's market power in the supply of (i) online search, display advertising, and ad tech services, (ii) general search services, or (iii) digital healthcare services, thereby impeding competition in these markets.[25]

The Commission found that Google's acquisition of Fitbit, by combining Google's already vast data collection with Fitbit's health and location data, could enable Google to hinder expansion by competitors in online advertising markets where Google already had very substantial market power pre-transaction. This even though the Commission found that the Fitbit data, although valuable, in particular for online advertising services, was not "unique" when compared to the databases of other players.

Data-driven mergers, like this, can often fall outside the traditional horizontal, vertical, and conglomerate theories of harm. For example, according to the Commission, its theory of harm in Google/Fitbit did not constitute a classical "vertical" concern, since Fitbit's data was not traded and could therefore not be regarded as an input for a firm active in online advertising. Moreover, the transaction did not present a traditional "horizontal" concern since Fitbit was not active in any online advertising market, and Google did not directly compete with its own smartwatches. Nor was Google a perceived or actual potential competitor in Fitbit's market.

But the fact that the data-driven merger fell outside these three categories did not mean it wasn't of concern. The Commission concluded that the transaction would allow Google to combine its existing datasets with those of Fitbit, thus strengthening its ability to supply services in online advertising markets and foreclose competitors' entry and ability to expand in such markets.

The European Commission specifically considered concerns that the merger would reduce competition along non-price parameters including privacy. It found that "in data intensive digital markets characterised by increased corporate concentration" such as search and digital advertising, Google already had very little incentive to adopt practices that enhance consumers' privacy.[26] In addition, data protection rules set out in the General Data Protection Regulation in the European Union provide a high standard of privacy and data protection that leaves little room for privacy to operate as a parameter for competition.[27]

[2023] (the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Europe's privacy regulation, to the processing of their personal data by that operator, but that such dominance is an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove).

[24] Google/Fitbit (Case M.9660) [2020] OJ C 194/7.

[25] Ibid, para 413.

[26] Ibid, para 452.

[27] Ibid, para 452, footnote 300.

Ultimately, the European Commission approved the merger in December 2020 conditional on a suite of commitments made by Google regarding how Google can use the data collected for advertising purposes, how interoperability between competing devices will be safeguarded, and how users can continue to share health and fitness data if they choose to.[28]

C. Third Category: Intersection But Market Failure – The role of Privacy and Other Policies to Align Incentives

In the second category, the underlying assumption is that privacy and data protection are important non-price parameters of competition. Competitive pressure causes firms to improve their privacy policies and data protection measures to comport with consumers' demands.

At times, however, consumers may value privacy, but market forces fail to deliver. Instead, firms degrade individuals' privacy, extract personal data, and use it to better exploit or manipulate their behavior (such as through neuro- and emotional marketing[29]).

Thus, the competition agency must assess the source of the market failure. Is it due to:

- the absence of meaningful competition (e.g., collective or individual market power) or
- a more fundamental problem of misaligned incentives beyond market power?

For the former, current or more advanced antitrust tools may address the problem. For the latter, privacy and other policies will likely be required to align incentives, which might be beyond the scope of many competition agencies' authority.

But even when beyond the competition agency's purview, it is important for the agency to recognize that promoting transparency of the companies' privacy practices, lowering entry barriers, making the markets more contestable, and increasing the number of rivals will not necessarily improve privacy protection, when the market participants' incentives are not aligned with the consumers' interests. Competition will increase, but not privacy. When the incentives are misaligned, firms will collect and use personal data about individuals, but not necessarily for their benefit.

---

[28] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

[29] The concern is that in using emotional marketing to trigger desires, whether to buy a particular car, endorse it to friends, or create a community around the brand, advertisers can compete to manipulate consumer demand. Emotional marketing, as one industry participant noted, is a gamechanger for advertising, whereby powerful platforms can use personal data "to exploit to the emotions of users in ways that increase the likelihood that they purchase a specific model of car or vote in a certain way." Roger McNamee, Zucked: Waking Up to the Facebook Catastrophe 69 (2019); for more on the risks posed by emotional marketing and manipulating behavior, and its potential toll on well-being, governance, and democratic institutions, see, e.g., Maurice E. Stucke, Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy 83-85, 121-24, 222-44 (Oxford University Press 2022); Ariel Ezrachi & Maurice E. Stucke, How Big Tech Barons Smash Innovation and How to Strike Back 108-20, 123-39 (HarperCollins 2022). Forty-two state attorneys general in the US sued Meta in 2023 for exploiting "young users of its Social Media Platforms" by among things "creating a business model focused on maximizing young users' time on its Platforms," and monetizing "young users' attention through data harvesting and targeted [behavioral] advertising." Complaint, filed in Arizona v. Meta, 4:23-cv-05448 (N.D. Cal. filed Oct. 24, 2023).

One example of misaligned incentives is when firms profit more from degrading privacy (rather than promoting it). Such may be the case in markets that rely primary on behavioral advertising.[30] Although the product or service is ostensibly free, individuals often pay with their attention and personal data. Nor is the focus necessarily providing individuals with more relevant ads; instead, they may use the personal data to better predict and manipulate consumer behavior.[31] Here ethical advertisers and publishers may find it difficult to unilaterally opt out of this competition since they will receive far less (if any) profits.[32] Besides behavioral advertising, firms in other industries (such as insurance, healthcare, and financial services) may also compete in ways to collect and use more sensitive personal data that harm individuals' privacy interests.[33]

Policy measures

It is important for agencies to recognize this intersection since promoting competition, without addressing the fundamentally misaligned incentives, will not benefit consumers, but might actually hurt them.

Jurisdictions can use consumer protection and privacy measures to align incentives and help ensure that the competition is a race to the top rather than the bottom. These measures are often determined by other laws, or the decisions, policies, and rules created by data privacy and/or consumer protection authorities, though in some jurisdictions these missions are combined with competition in a single authority. Thus, privacy "guard rails" (as well as consumer protection measures) can ensure that the competition is a race to the top (rather than the bottom).

---

[30] Behavioral advertising means the targeting of advertising and promotions to individuals based inter alia on the personal data collected about the person's online and offline activities. See, e.g., Dissenting Statement of Commissioner Rohit Chopra, In re Google LLC and YouTube, LLC, Commission File No. 1723083 (Sept. 4, 2019):

> *Behavioral advertising, unlike contextual advertising, is about targeting each individual – a demographic of one. Google is able to do this by tracking and collecting an enormous amount of information on users' behavior wherever Google embeds its technology. This includes activity on their phones, home devices, on YouTube, and nearly everything they do online. When individuals use a mobile device with Google's Android operating system or give commands to a Google Home device, Google is able to glean more and more insights about their personal lives. Google then monetizes these insights by using them to psychologically profile each user and predict in real time what content will be most engaging and which ads will be most persuasive.*

[31] See, e.g., Complaint, filed in Arizona v. Meta, 4:23-cv-05448 (N.D. Cal. filed Oct. 24, 2023) (alleging how Meta tracks and logs the behavior of millions of young users and utilizes that data to refine and strengthen the features that induce their compulsive use of the company's social media platforms); STUCKE, BREAKING AWAY; EZRACHI & STUCKE, BIG TECH BARONS.

[32] CMA Final Report at ¶ 5.326 (estimating that U.K. publishers "earned around 70% less revenue when they were unable to sell personalised advertising but competed with others who could"); see also Dissenting Statement of Commissioner Rebecca Kelly Slaughter, In the Matter of Google LLC and YouTube, LLC (Sept. 4, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-commissioner-rebecca-kelly-slaughter-matter-google-llc-youtube-llc at 2-3 (noting how both YouTube and the channels have a strong financial incentive to use behavioral advertising, so while "YouTube has long allowed channel owners to turn off default behavioral advertising and serve instead contextual advertising that does not track viewers . . . vanishingly few content creators would elect to do so, in no small part because they receive warnings that disabling behavioral advertising can 'significantly reduce your channel's revenue'").

[33] See White House, Blueprint for an AI Bill of Rights Making Automated Systems Work for the American People, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

These regulatory "guard rails" can include:

- Prohibiting dark patterns that, among other things, "deceive consumers into giving up more data than desired (e.g. through hidden privacy-intrusive settings turned on by default) or manipulate them into spending more time on a website (e.g. through addictive interface design) might support a business model involving capturing consumer attention and collecting consumer data for advertising, e.g. of an online platform."[34]

- Privacy regulations that provide that consent secured by dark patterns is voidable (or illegal).[35]

- Regulations that give users the choice to opt out of the collection of data from third parties.[36]

- Regulations that give users the choice to opt out of the firms' combining their personal data collected across their different services, or cross-using the data across services.[37]

- Regulations limiting (or requiring individuals to opt out of or into) behavioral advertising and personalized recommendations.[38]

- Enforcing consumer protection laws in that jurisdiction to the extent they prohibit unfair, deceptive, or exploitative commercial practices, such as (i) the omission of information about the collection and use of personal data when creating an account and

---

[34] OECD, Dark Commercial Patterns, Digital Economy Papers No. 336, at 12-13 (Oct. 2022).

[35] Conn. Public Act No. 22-15, An Act Concerning Personal Data Privacy and Online Monitoring, § 1(6) (consent obtained through dark patterns is void); California Privacy Rights Act of 2020 [CPRA] § 1798.140(h) (same); DMA ¶ 37 (providing that gatekeepers "should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent"). Of particular concern is the use of dark patterns to manipulate children's behavior. *See, e.g*., the California Age-Appropriate Design Code Act § 1798.99.31(b)(7) (providing among other things a "business that provides an online service, product, or feature likely to be accessed by children shall not take . . . [u]se dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being").

[36] *See, e.g.,* DMA Art. 5(2) (which imposes this duty on gatekeepers to "not unfairly undermine the contestability of core platform services").

[37] *See, e.g.,* DMA Art. 5(2).

[38] *See, e.g*., Conn. Privacy Law § 4 (providing that consumer can opt out of the processing of the personal data for purposes of some types of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer); California Privacy Rights Act § 2(I) (providing that consumer has right to opt out of having sensitive personal information used for behavioral advertising or personal information shared to third-parties for behavioral advertising, noting how "some advertising businesses today use technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles of their individual interests," and how consumers "should have the information and tools necessary to limit the use of their information to non-invasive, pro-privacy advertising, where their personal information is not sold to or shared with hundreds of businesses they've never heard of, if they choose to do so," and how "[a]bsent these tools, it will be virtually impossible for consumers to fully understand these contracts they are essentially entering into when they interact with various businesses").

(ii) the imposition of an opt-in as the default option for data sharing consent for commercial purposes.

D. FOURTH CATEGORY: WHERE PRIVACY AND COMPETITION CONFLICT

Even when incentives are aligned and firms robustly compete on privacy and data protection, privacy and competition policies, at times, will conflict. Conflicts may arise in the following scenarios:

1. Antitrust remedies, at times, can have important privacy implications, and can pose conflicts with privacy interests even where the rules of decision at issue do not. (See case study below.)

2. Privacy (or consumer protection) policies can favor entrenched firms and deter entry (when compliance costs are significant); or

3. When a jurisdiction's data minimization and other privacy principles are in tension with its antitrust data sharing policies.

To illustrate this potential tension, consider this simple metaphor. Suppose policymakers had two levers for the flow of personal data: one for privacy, another for competition. The privacy lever, through data minimization policies, tightens the flow of personal data. Privacy regulation would limit (i) the types of personal information that firms could collect, (ii) the way the firms could collect the information, (iii) how the firms could internally use the information within their organization, and (iv) for how long the firms could use the data.

The competition lever, on the other hand, would seek to increase the flow of personal data throughout the industry through data-sharing requirements and data portability frameworks.

Each lever can play an important role to promote competition. For example, the privacy lever can reduce the volume and variety of personal data that the dominant firm collects to a fraction, basically, the minimum data necessary to provide the service. A navigation app, for example, could use the smartphone user's geolocation data to provide directions and assess traffic conditions. But the dominant firm could not use the geolocation data for other purposes, such as behavioral advertising,[39] training their algorithms for other services they provide (such as search engines), or to leverage into other markets that rely on deep learning. As a result, the firm, due to network effects and scale economies, might remain dominant for navigation apps; other markets, however, might become more contestable and competitive (because of the data minimization policies). It is also possible that other markets would become less competitive than they would be, when the dominant firm is more innovative or has other advantages that make it a lower cost provider or a provider of a higher quality services.

[39] One argument is that absent behavioral advertising, consumers will be harmed with fewer free services. Whether this is true has been disputed. See, e.g., Stucke, *Breaking Away* at 218-19 (discussing how digital firms can rely on contextual advertising revenues and how limiting behavioral advertising and profiling can level the competitive playing field). Moreover, in some jurisdictions, the user's privacy interests and fundamental rights may override the operator's interest in such personalised advertising by which it finances its activity. See, e.g., Meta Platforms, E.C.J., Case C-252/21 (July 4, 2023).

But one could argue that the competition lever could promote competition even more. To compete and innovate in many markets today, companies need access to personal data. So, the competition lever could widen the flow of personal data across the economy. When personal data is non-rivalrous, other firms, as well as non-profit organizations, could extract value from the data, and data-driven innovations and insights could increase. Smaller, data-poorer firms could more effectively compete and differentiate themselves by offering greater privacy protections and privacy-centered innovations.

One might also point out the unintended harm from the privacy law's "data minimization" policies. In limiting the flow of data from users, privacy regulation may increase the costs that others would now have to expend to access the personal data. It is often cheaper to re-circulate the data to other businesses with the competition lever. Other firms can mine the data without expending the extra time, money, and resources to directly access this data from consumers and clean, process, and organize this data. So, when the privacy policies restrict the platforms' data collection, the potential reservoir of personal data for data circulation also shrinks. Smaller firms and non-profits would now have to incur the costs to collect, clean, and organize that data. As these costs increase, less personal data will be circulated, which can limit the potential value that could be unlocked from the data, and all the potential data-driven innovations.

A dominant company, for example, collects personal data in compliance with that jurisdiction's privacy law. Another company requires access to these data to offer other (value-adding) services or to compete with the dominant company. But that jurisdiction's privacy laws might significantly limit the transfer of personal data.

So, how should the jurisdiction trade off the privacy and competition levers? As discussed below, one should not reflexively opt for either lever. Moreover, the choice will depend, in part, on how one defines value and who receives this value. For example, a user's geolocation data is non-rivalrous, that is, its value does not diminish if used for multiple, non-competing purposes:

- The navigation app could use the smartphone's location for traffic conditions.
- The health department could use the geolocation data for contact tracing (to assess whether the user encountered someone with COVID-19).
- Law enforcement or national security agencies could use the data for surveillance.
- The behavioral advertiser could use the geolocation data to profile the individual, influence her consumption, and assess the advertisement's success.

Each actor derives value from the geolocation data, but the individual and society may not necessarily benefit from all these uses. Individuals in that jurisdiction, for example, may not believe they benefit from this level of tracking and data collection.[40] Even if the government

[40] See, e.g., Brooke Auxier et al., *Americans Concerned, Feel Lack of Control over Personal Data Collected by Both Companies and the Government*, Pew Res. Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-

and behavioral advertisers might derive value from the geolocation data, the welfare-optimizing solution is not necessarily to share the data with them and anyone else who derives value from the data. Nor is the welfare-optimizing solution to encourage competition for one's data. As one survey of the economic literature noted, "exploiting the commercial value of data can often entail a reduction in private utility, and sometimes even in social welfare overall. Thus, consumers have good reasons to be concerned about unauthorized commercial application of their private information."[41]

But what if the data were limited strictly to beneficial uses, the data were anonymized, and the data were non-rivalrous (in that each can derive prosocial value from the data)? It still does not mean that the use by multiple entities is costless to one's privacy. The risk of re-identification remains (as Part III explores).[42]

Consequently, privacy and competition, at times, will be at odds. As one 2019 IMF report recognized, "The collection of personal data has always involved a trade-off between respecting the individual's desire for privacy—including from government—and reaping the commercial and social benefits that can be derived from its collection and dissemination."[43]

Case study – Utility Monopoly in France

A dominant French electricity provider used the personal data it collected as a regulated monopoly to compete in another market. In 2007, French gas customers could drop the

data-collected-by-both-companies-and-the-government/ (approximately "three-quarters of adults say they benefit very little or none from the data that companies (72%) or the government (76%) collect about them. On the other hand, only three-in-ten Americans (28%) say they get a great deal or some personal benefit from companies' collecting data, and 23% say the same about the government's efforts"); Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442, 476 (2016), https://dx.doi.org/10.1257/jel.54.2.442; Note by the European Union, Consumer Data Rights & Competition, OECD Doc. DAF/COMP/WD(2020)40 (June 12, 2020) at ¶ 11, https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf ; Special Eurobarometer survey no. 447 on "Online platforms," June 2016, p. 52, https://ec.europa.eu/information_society/newsroom/image/document/2016-24/ebs_447_en_16136.pdf ("clear majority of Internet and online platforms users feel uncomfortable with the fact that the different types of online platforms use information about their online activity and personal data to tailor advertisements or content to what interests them"—55% were uncomfortable with search engines using information about their online activity and personal data to create tailored advertisements or content; 56% were uncomfortable with the fact that online marketplaces use information about their online activity and personal data; and 58% were uncomfortable with online social networks using information on their online activity and personal data to tailor advertisements or content).

[41] Acquisti et al., *supra*, at 476 (collecting earlier studies).

[42] One norm among computer scientists is that the privacy risk increases (however small) with the repeated mining of anonymized data for different purposes. This is true with or without any privacy-preserving techniques, like differential privacy tools. Once this privacy risk is considered, the optimal result is not necessarily to democratize even large, anonymized datasets (by enabling others to derive value from it), as the privacy risk might be too great. See Stucke, *Breaking Away*, at 168-70.

[43] Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund Policy Paper No. 19/16, at 3 (Sept. 2019), https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596.

incumbent GDF Suez monopoly for other gas supply offers. Consumers could choose either (1) GDF Suez offers at the regulated tariffs or (2) market offers, which all suppliers including GDF Suez provided.

The government hoped to inject competition into this concentrated market. But, by 2014, the new gas suppliers' market shares remained low (between 5 and 13 percent). In 2014, a competitor Direct Energie complained that GDF Suez was seeking to drive its competitors out of the market with anti-competitive practices. One practice was GDF Suez's using its voluminous data of customers on the regulated tariffs (that it acquired as a regulated monopoly) to offer them deals on gas and electricity. The customer data, the rival alleged, gave the monopoly an unfair advantage for maintaining its dominant position in the gas market and acquiring new customers in the electricity market.

The French competition authority investigated whether GDF Suez abused its dominant position in the gas market "by using the infrastructure dedicated to regulated tariffs (i.e., customer database, website, customer platform . . .), which is in the realm of a public service activity, to market its gas and electricity offers, which are marketed in a competitive market."[44] The regulated monopoly had an unfair competitive advantage, the competition authority found, "since no database exists that would allow competitors to precisely locate gas consumers and know their consumption level, in order to propose them offers that are better suited to their profile."[45] This database was not the "product of a specific innovation that GDF Suez may have introduced, but [was] merely inherited from its former status as monopolistic gas supplier."[46]

In that case, the smaller competitors wanted access to the dominant firm's data on its consumers. Here, the competition agency was confronted with a trade-off: increasing competition versus privacy. In allowing competitors' access to the voluminous dataset, the playing field hopefully would become more level, as competition increased. But releasing this data to other companies would potentially infringe on the consumers' privacy interest. We'll turn next to issues the agency should consider in seeking a remedy.

Implications for authorities

At the onset, competition officials must recognize when privacy and antitrust policies are in tension.

For example, the competition authority may consider data sharing as a remedy to promote competition. This may be the case when smaller firms compete against state-owned enterprises that benefit from the personal data that it and other governmental agencies collect. In considering whether to impose a duty on the dominant firm to share personal data with rivals, the agency must decide:

- Whether the dominant firm should disclose the personal data to its rivals;

[44] Autorité de la Concurrence, 'Gas Market', Press Release, 9 September 2014.

[45] Ibid.

[46] Ibid.

- If so, the limitations on the recipients' use and retention of the personal data; and
- The privacy default.

But even here, the competition agency must consider ways to minimize privacy concerns by, among other things, considering:

- Data minimization principles, such limiting what personal data can be collected, for what particular use, with whom the data can be shared, and for how long the data can be retained;
- The extent to which individuals can elect not to have their data disclosed; and
- The privacy default (opt out versus opt in).

Presumably, for the privacy default, the dominant firm would want consumers to opt in. Specifically, the monopoly would release to its rivals the personal data of only those consumers who provided the monopoly with authorized written consent. Rivals would likely object. An opt-in would reward the monopoly, as many consumers would, for reasons other than privacy concerns (such as inertia or procrastination), not opt in. Instead, the rivals would prefer customers to opt out, namely, the monopoly would disclose the customer's data unless the customer expressly says no.

In the French utility case, the competition agency ordered the disclosure of only that data "strictly necessary to ensure effective competition among suppliers, i.e., the customer's name and address and the technical characteristics of his consumption." The agency also recognized that some consumers may not want their personal information disseminated. So, the agency chose the opt-out default, i.e., the data can be disclosed, unless the customer disagrees.

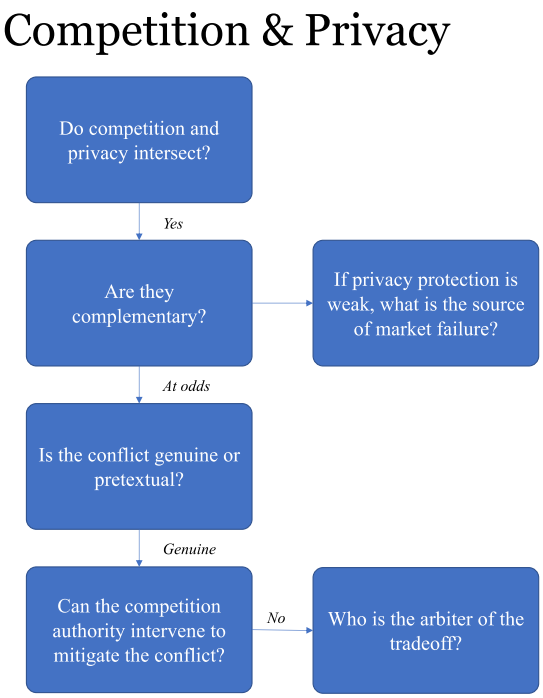
Consequently, at times, privacy and competition policies will conflict, especially when the jurisdiction's privacy regulation seek to minimize data collection and processing while the competition policies may seek to foster greater data mobility. The next Part addresses how to address these conflicts when they arise.

II. ISSUES TO CONSIDER ABOUT THE PRIVACY AND COMPETITION INTERSECTION

As mentioned at the onset, the nature of the intersection may vary by jurisdiction. Moreover, when privacy and competition policies conflict (or when competition degrades or fails to improve privacy), the choices and policy remedies available to the competition enforcers or courts may be limited. Some choices or policies may be reserved for other agencies or the legislature. Some agencies may have greater latitude, whether through rulemaking or affecting the common law, than other agencies. Moreover, the existence and nature of the jurisdiction's privacy law and any digital platform-specific competition regimes may also affect how the agency navigates the privacy/competition intersection.

Since the demarcation between enforcement and policymaking may vary by jurisdiction, outlined below is a general framework of how authorities can account for privacy and personal

data issues. This checklist may be helpful when conducting specific competition investigations or more generally when considering policy reforms.



1. *For this particular matter, do privacy and competition policies intersect?*

To help answer this question, the jurisdiction can consider the following questions for particular antitrust investigations:

- Is privacy a key parameter of competition in that industry?
- Is personal data (or third-party data) a key input or output to effectively compete?
- Is access to personal data a barrier to entry?
- What caused the privacy concerns? Was it related to --
    - the absence of meaningful competition (e.g., market power),
    - "race-to-the-bottom" competition (e.g., misaligned incentives), or
    - something else unrelated to competition?

If the answer is something else, then there may be little, if any, need for the competition authority to intervene. The focus here is whether competition policy has a role to play. If not, the issue is better left to other policies (e.g., privacy or consumer protection).

2. *If there is an intersection, are privacy and competition complementary?*

Issues to consider include:

- Do consumers in that sector generally value privacy and data protection?
- If so, do firms generally compete significantly to protect privacy and data protection?
- If the answer is yes to both questions, is the privacy concern a result of market power?

Here one concern is that the exercise of market power will diminish existing privacy competition.

- How will the merger, restraint, conspiracy, or conduct by a firm with significant market power affect privacy?
- Can the competition authorities effectively remediate this exercise of market power?
- Are the current antitrust tools, for example, sufficient to deter data-driven mergers that may substantially lessen privacy protection (e.g., by removing a privacy focused competitor) or tend to create a monopoly? Deter firms from abusing their dominance by extracting too much personal data?
- If the competition authorities cannot effectively remediate this exercise of market power, what additional tools are needed to restore privacy competition and promote market contestability?

3. *If there is an intersection, but privacy competition is weak or non-existent, then what is the source of the market failure?*

Consumers in that sector may generally value privacy and data protection. But firms may not significantly compete to protect privacy and data security, and this lack of competition is not always attributable to market power issues. Here the competition agency may face a market failure, where competition is failing to provide consumers what they want (namely, more privacy and data protection).

Issues to consider include:

- Are the firms' incentives aligned with individuals' privacy incentives? For example, does the company's business model promote privacy and data protection, or do firms typically make more money degrading privacy and underinvesting in data protection? Are the platform's interests aligned more with one group (e.g., behavioral advertisers) from which they derive most of their revenues and profits than from another group (e.g., private users)?
- Do firms limit their use and monetization of consumer data to the specific purpose for which the consumers expect?
- With or without consumer consent, are firms exploiting that personal data to compete in ancillary, adjacent, or completely unrelated markets?
- Has the entry of rivals in that segment improved or reduced consumer's privacy interests?
- Is there any evidence to suggest that increasing competition will significantly improve privacy and data protection?

If incentives are misaligned, the competition agency may want to assess whether:

- the jurisdiction has privacy regulation to limit surveillance and behavioral advertising?
- there are policy guard rails to deter firms from employing dark patterns, deception, etc.?

- the jurisdiction's proposed (or existing) privacy regulation improves or hinders competition, or have no effect?

Thus, the competition agency may want to coordinate with privacy regulators and policymakers (in accordance with its mandate) in providing adequate guardrails, so that firms are competing in ways to promote citizens' and societal interests (rather than competing to exploit individuals and degrade their privacy).

4. *If incentives are aligned, adequate privacy guardrails are in place, and privacy and competition policies are seemingly in conflict, is this conflict genuine conflict or pretextual?*

To answer this question, issues to consider include:

- Are firms using privacy as a pretext for anticompetitive behavior?[47]
- Are firms using competition justifications as a pretext for behavior that degrades privacy (such as when firms within an advertising network share sensitive personal information to compete for behavioral advertising revenue)?

5. *If there is a genuine conflict, can the competition agency mitigate the conflict?*

Issues to consider include:

- Is the conflict the result of the antitrust agency's actions or broader policy issues?
- If the former, can the agency consider in its competition analysis the privacy concerns, such as in:
    - Tailoring its antitrust remedies (when imposing a duty on a dominant firm to share personal data with rivals)?
    - Its analysis of data-driven mergers (when it results, for example, in greater efficiencies from the collection of a greater variety and volume of personal data but subjects the consumers to greater risks from data breaches)?

If there is a genuine conflict and the competition agency cannot unilaterally mitigate the conflict, the agency will need to coordinate with policymakers and other regulators to address the conflict. This might include reworking privacy (or consumer protection) policies that unnecessarily impose significant compliance costs or otherwise favor entrenched firms and deter entry.

6. *Finally, if competition, privacy, and other policies are calibrated, and there still is a conflict between privacy and competition which is unavoidable, who should be primarily responsible to address the trade-off?*

Depending on the context, the legislature, courts, or enforcers might bear this responsibility.

[47] See, for example, CMA Final Report at ¶ 5.265 (questioning Google's privacy justifications for bundling YouTube advertising with its DSP advertising services).

The next Part addresses several tools and principles to help the jurisdiction weigh privacy and competition concerns when they conflict.

III. HOW SHOULD JURISDICTIONS HANDLE THESE TRADE-OFFS CONSISTENT WITH RULE-OF-LAW PRINCIPLES?

When privacy and competition conflict, there is no uniform response. The trade-offs may depend on the case's particular facts and context. Nor can the trade-off between the incommensurable interests underlying both competition and privacy be reduced to a cost/benefit analysis. Different jurisdictions may place greater weight on different aspects of privacy (including informational privacy). But, as this Part explains, there are several things that each jurisdiction can do.

A. Antitrust and Privacy Regulators Need to Assess Matters on a Case-By-Case Basis with No Pre-Determined Bias Towards Competition or Privacy.

Even in jurisdictions where privacy is a fundamental constitutional right, privacy is not an absolute right. Nor is the right to a competitive market an absolute right. Instead, jurisdictions balance privacy and competition with other public interests. But in trading off privacy and competition, each jurisdiction should avoid the following two traps:

1. When in doubt, automatically opt for either competition or privacy.

Increasing privacy protection, at times, can benefit individuals and society. But at other times, it can harm them. From this, one might deduce that increasing privacy will not always improve welfare but increasing competition always will. So, when privacy and competition clash, and one cannot calculate the welfare gains from increasing either, one might conclude that increasing competition (at the cost of privacy) is the prudent choice to maximize well-being. In uncritically assuming that competition is always good, enforcers and policymakers might discount privacy protections.

The trap is in assuming that the competition will benefit citizens and society. As we have seen, when incentives are misaligned, competition, at times, can worsen, rather than improve, the situation. But even when the competition is healthy, the incremental welfare gain from the increased competition may be outweighed by the welfare losses from the degradation in privacy.

Likewise, when in doubt, enforcers and policymakers cannot automatically opt for greater privacy. In some jurisdictions, privacy is viewed both as an end itself (i.e., as an inherent human right), and the means to promote other societal goals (for example, associational privacy can promote, at times, social change and a vibrant democracy). On the other hand, competition is generally not seen as an end itself, but rather as the means for other greater ends.

The trap is that an overly stringent privacy regulation (in minimizing the amount of data collected, processed, and stored; and the uses for such data) can reduce overall well-being. Just as too much personal data can exclude persons from the market (such as those with severe pre-existing health conditions), so too the opposite poses risks. With too little personal data collected and shared, some individuals will be excluded from the marketplace, health, and

safety risks can increase, and overall well-being can decline. Access to data can also foster health insights, improve security, reduce fraud, promote innovation, and provide other benefits.

Thus, when privacy and competition conflict, policymakers cannot reflexively opt for either policy.

2. Confusing what is measurable with what is important.

Most, if not all, competition agencies today look beyond price effects in mergers, restraints, and abuses in the digital platform economy. For example, the fact that their services are ostensibly free does not immunize powerful digital platforms from antitrust scrutiny.

Nonetheless, in assessing the trade-off between privacy and competition, some may give undue weight to what is quantifiable, while discounting the harder-to-quantify, but more significant privacy harms. One example is behavioral advertising. On a quality-adjusted basis, behavioral ads for some advertisers might be more cost-effective in driving sales than contextual ads. But what is good for the advertiser is not necessarily good for the individual or society, especially when one considers the harms from behavioral advertising and its underlying surveillance, including the costs to privacy, costs of data breaches, the harms from behavioral discrimination, the costs in seeking individuals' attention on their well-being and autonomy, and the greater costs to society.[48]

B. Rule of Law Concerns

Jurisdictions, while avoiding these two traps, must still at times trade off privacy and competition interests. While jurisdictions may weigh these interests differently, nonetheless there are core values, such as the rule of law, transparency, and process, that they all share. Thus, the legal standard and its objectives in deciding how to weigh the competing privacy and competition interests should promote rule-of-law principles, such as:

- *Consistency* (the legal standard should yield consistent, predictable results),
- *Objectivity* (the legal standard should leave little, if any, subjective input from the decision-makers),
- *Transparency* (the reasoning for the trade-off should be understandable and clear), and
- *Administrability* (the standard should be easy to apply).

C. Incentivizing De-Identification Privacy Innovations and Protocols

Given the importance of personal data to compete and innovate, firms will seek access to that data. At times rivals may want to impose a duty on dominant firms to share the data. Thus, when personal data is non-rivalrous and a key input for competition and innovation, the jurisdiction may strive to protect privacy while promoting the flow of personal data.

Policymakers might inquire about a win-win scenario: Can we promote competition through the free flow of personal data while adequately safeguarding our privacy, such as requiring the

[48] See, e.g., Stucke, *Breaking Away*, at 213-244.

personal data to be aggregated or anonymized? Can technologies such as anonymization provide this win-win by enabling the benefits of data access while maintaining adequate privacy?

In several applications, data analytics can provide valuable insights without data being individually identifiable. Consider training artificial intelligence to drive automated cars, to recognize images of specific objects, to give a medical diagnosis based on an x-ray or blood test, or to study the effects of new pharmaceuticals based on anonymized data. All these applications rely on a lot of data to train the algorithms but do not require that the data be linked to an individual.

But for other personal data sets, the value often comes from a more granular analysis. Although one can de-identify granular personal data, it is often easy to re-identify that data using other data sources.[49] Even for an aggregated anonymized dataset, there remains the privacy risk of individuals being re-identified in this dataset, and this risk can increase the more the dataset is dissected and analyzed.

Consequently, to successfully de-identify the data, one might have to strip away much information, and the data can lose its value.

One area of potential promise is the increase in demand for innovations and protocols to de-identify data. De-identification technologies might allow firms to extract perhaps a little more value from slightly less aggregated data without a significant decline in privacy.

Firms and scholars are currently experimenting with "differential privacy" tools, where researchers can have access to large datasets while reducing the risk of re-identification to an acceptable level.[50] One method is adding random "noise" to the data.

---

[49] Consider for example one US case *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330 (4th Cir. 2021). The city of Baltimore had a very high per capita murder rate, and only 32.1% of homicide investigations were solved. So, the city partnered with a private firm to undertake aerial surveillance. Three small planes equipped with cameras would cover 90 percent of the city. The cameras, however, employed a resolution that reduced everyone on the ground to a pixelated dot, thus making the cameras unable to capture identifying characteristics of people or automobiles. Upon receiving a notification, analysts could "tag" the dots photographed around the crime scene and track those dots' public movements in the hours leading up to and following the crime.

Ostensibly the data is de-identified, as the cameras could only identify individuals as pixelated dots in a photograph, and analysts examining these photographs could not identify an individual's race, gender, or clothing. But as the court noted, it was easy to re-identify individuals. First, the court relied on research showing that, because people's movements are so unique and habitual, it is almost always possible to identify people by observing even just a few points of their location history. For example, one can easily re-identify these "dots" by seeing where they go in the evening or leave in the morning, as they likely live in that residence. Moreover, by using other data sets, the police could also re-identify these dots, such as the data from the city's surveillance camera network, license plate readers, and gunshot detectors. For example, if the tracking of a car is interrupted, the city's license plate readers could help relocate it over the following days.

[50] Differential privacy "protects an individual's information essentially as if her information were not used in the analysis at all, in the sense that the outcome of a differentially private algorithm is approximately the same whether the individual's information was used or not." Alexandra Wood et al., *Differential Privacy: A Primer for a Non-Technical Audience*, 21 VAND. J. ENT. & TECH. L. 209, 212 (2018). Ideally, the difference between the results when a person's data is included in the analysis and the results when her information was excluded would be zero. In reality, the difference between the two is a positive number, called the privacy loss

Nonetheless, differential privacy raises the trade-off between privacy and accuracy. To increase privacy, one might need to add more noise to the data, which reduces accuracy. Adding less noise to the data increases accuracy but reduces privacy. Thus, for small datasets, for datasets with many dimensions, or when the dimensions have large domains, one might have to add much noise, thereby reducing accuracy.

Researchers are now studying ways to improve differential privacy tools and ways to obtain more value from the data while preserving privacy.[51]

Competition agencies, of course, may lack the resources to invent de-identification privacy technologies. But they can potentially help increase the demand for these technologies or the use of synthetic data.[52]

We are already seeing this with some jurisdictions' privacy regulation. If the firms successfully "deidentify" the personal data, then the privacy laws do not apply to that data.[53] Firms can freely collect, use, retain, sell, or disclose de-identified information. But to qualify as "deidentified" data, the firm must implement reasonable technical safeguards and business processes that significantly reduce the risk of re-identification. The GDPR, for example, requires firms to continually assess whether the data can be re-identified using the available technologies.[54] Moreover, if the jurisdiction bans or limits behavioral advertising and allows users to opt out of profiling, firms will likely have less incentive to hoard personal data and be more inclined to reduce their compliance costs under the jurisdiction's privacy laws. By successfully anonymizing personal data, firms can avoid spending a significant sum in complying with privacy laws and reap greater profits in doing so. In that case, they will have greater incentives to find ways to de-identify data.

Likewise, competition agencies can explore ways their policies can increase demand for de-identification technologies and protocols. Given the importance of personal data to effectively compete in many markets, rivals will seek access to the data. The current legal framework in that jurisdiction may encourage data-hoarding, which deprives rivals of scale, increases entry barriers, and widens the dominant firm's competitive advantage. When dominant firms have the incentive to hoard data, rivals will likely ask policymakers to impose a duty to deal, which

---

parameter, which "measures the effect of each individual's information on the output of the analysis." Ibid at 235.

[51] See, for example, using representative, yet synthetic, datasets to train artificial intelligence models. European Data Protection Supervisor, Synthetic Data, https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en.

[52] Hradec, J., Craglia, M., Di Leo, M., De Nigris, S., Ostlaender, N., Nicholson, N., Multipurpose synthetic population for policy applications, EUR 31116 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-79-76-53478-5, doi:10.2760/50072, JRC128595.

[53] *See e.g.*, GDPR Recital 26 (stating that the data protection principles should "not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" and the GDPR does not "concern the processing of such anonymous information, including for statistical or research purposes"); CPRA § 1798.145(a)(6).

[54] GDPR Recital 26 (requiring an assessment of all the means reasonably likely to be used either by the controller or by another person to identify the natural person directly or indirectly, including "the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments").

would require the dominant firm to share personal data with rivals. While data-sharing might increase competition, it can also increase privacy risks. To mitigate the privacy risks, the data must be de-identified. But rivals must also convince the competition and privacy officials that the data, once de-identified, cannot be re-identified. That gives rivals the incentive to find ways to successfully de-identify data and still glean insights from the data.

For example, Europe's Digital Markets Act will require gatekeepers to provide any third-party providers of online search engines, upon their request, with access on fair, reasonable, and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on the gatekeeper's search engines, *subject to anonymization* for the query, click and view data that constitutes personal data.

When data is necessary to compete (whether to train algorithms, improve services, or gain insights), rivals will likely press the competition agency to require dominant firms to turn over personal data. But in recognizing the privacy risks of re-identifying granular data, the jurisdictions should require rivals to have protocols and technologies in place that effectively de-identify the data, perhaps not at its granular level, but at a more aggregated level, where the data is still useful for their purposes and the privacy risks are minimized.

Consequently, one way to harmonize privacy's data minimization policies with competition's data openness policies is to allow firms to collect data that is necessary to provide the services or products (but not for profiling and behavioral advertising purposes), and then let (or require) firms to share aggregated de-identified data when it would benefit society (such as fostering insights on health and safety) without increasing the privacy risk beyond a specific threshold.

In the advertising sector, data could help with verification, measurement, and attribution. So, one way to harmonize the privacy and competition levers, as the U.K.'s competition authority is considering, is by "shifting the matching between exposure and conversion events to the device, and only sending anonymous and or aggregate attribution data to advertisers, rather than relying on individual-level tracking."[55]

Once privacy and competition policies are correctly calibrated, the demand for de-identification protocols and techniques will likely increase. Although jurisdictions may never reach the win-win scenario of successfully de-identifying granular personal data, improvements in synthetic data and de-identification privacy tools can help many more entities derive slightly more value from the data while still safeguarding privacy, thereby promoting healthy competition, closing the AI divide, and fostering innovation.

D. Market Studies or Sector Inquiries as a Tool

To the extent they have these tools, competition authorities can use market studies or sector inquiries to better understand complex digital markets and analyze issues involving competition and privacy.

---

[55] CMA, Online Platforms & Digital Advertising: Market Study Interim Report Appendix L at ¶ 95 (2019), https://assets.publishing.service.gov.uk/media/5df9efa2ed915d093f742872/Appendix_L_Potential_approaches_to_improving_personal_data_mobility_FINAL.pdf.

This is already happening. Some market studies and inquiries were particularly broad, covering a wide range of markets and issues. For example:

- The Australian Competition and Consumer Commission (ACCC) has produced a number of reports that examine digital platform services, including the Digital Platforms Inquiry Final Report (2019) and the Digital Advertising Services Inquiry Final Report (2021).[56] The ACCC's current Digital Platform Services Inquiry (2020-2025) has published seven reports on a range of issues including social media, app marketplaces, general online retail marketplaces, search defaults and choice screens, and the need for regulatory reform and is due to publish three more by March 2025.[57]
- Similarly, the Italian Competition Authority (AGCM)'s Big Data Sector Inquiry considered big data across a broad range of sectors, including telecommunications, media, digital platforms, information technology, insurance, and banking.

In contrast, some studies and inquiries had a narrower focus on a particular market or segment of a market. For example:

- The Competition and Consumer Commission of Singapore's (CCCS) Online Travel Booking Market Study focused on competition and consumer concerns associated with the provision of online flight and accommodation booking services.
- Another market study by CCCS focused on e-commerce platforms operating in its region.[58]
- The French Autorité de la Concurrence undertook a sector-specific inquiry into "fintechs" and financial payment services.[59]

Just like the markets that were explored, the themes and issues explored in these inquiries and studies were also diverse. However, some common themes across several survey responses included a consideration of data portability,[60] personal data regulation, discriminatory practices in online specialised search (e.g., travel booking), structural distortions to competition in the market for internet of things (IoT), the impact of technology-led innovation in the financial services sector, and digital advertising services.

---

[56] Digital Platforms Inquiry Final Report (2019): https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries/digital-platforms-inquiry-2017-19; Digital Advertising Services Inquiry Final Report (2021): https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries/digital-advertising-services-inquiry-2020-21/final-report.

[57] https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25. The seventh interim report of the digital platform services inquiry considered the Expanding Ecosystems of digital platform service providers. https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-inquiry-2020-25-reports/digital-platform-services-inquiry-september-2023-interim-report.

[58] https://www.cccs.gov.sg/media-and-consultation/newsroom/media-releases/cccs-market-study-on-e-commerce-platforms-recommends-update-to-competition-guidelines

[59] https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/fintech-sector-specific-inquiry-autorite-de-la-concurrence-issues-its-opinion.

[60] The AGCM's Big Data Sector Inquiry recommended expanding data portability requirements; the CCCS published a paper on data portability in collaboration with the Singapore Personal Data Protection Commission; and the FTC) held a 2020 workshop on data portability.

Case study – Online advertising markets

The interaction of privacy and competition has been considered in several market studies on online advertising markets conducted in the UK, France, Germany, Australia, Canada, and the US.

In the UK, the Competition and Markets Authority ("CMA") concluded its market study into online platforms and digital advertising in 2020.[61] In its analysis of competition in UK digital advertising markets, the CMA found that Google's access to better data for ad targeting contributed to Google's market power in search advertising and that Facebook had a significant data advantage over smaller publishers that significantly raised barriers to entry in the market for display advertising.

In this market study, the CMA considered tensions between incentives between market participants to compete for increasing amounts of user data and privacy laws put in place to protect consumers' privacy.[62] Many stakeholders raised concerns that stronger privacy regulations such as the General Data Protection Regulation (GDPR) could be used by large digital platforms as a justification to restrict access to data for third parties to entrench their market power and data advantage.[63] The CMA found that large platforms such as Google and Facebook act "in a quasi-regulatory capacity in relation to data protection considerations, setting the rules around data-sharing not just within their own ecosystems, but for other market participants."[64]

However, despite the GDPR applying also to combining and sharing of data within a digital platform's ecosystem, there is evidence suggesting that platforms combine and share data much more freely inside their "walled" gardens while restricting similar sharing of data with third parties.[65] In the CMA's view, large platforms have the ability and incentive to interpret and implement privacy laws in a way that entrenches their own data advantage: by adopting a more restrictive approach to data-sharing with third parties and a more expansive approach to data-sharing within their own ecosystems.[66]

To address the competition concerns raised by the data advantages of the large platforms in targeted advertising (without compromising consumers' privacy), the CMA recommended that it be granted powers to make a range of pro-competitive data-related interventions if it finds that there are sufficient benefits to outweigh any costs of intervention.[67] These data-related remedies may include imposing data silos that separate data within a digital platform's ecosystem, mandated access to large platforms' data for targeting and attribution, and measures to promote data mobility.[68]

Thereafter, a Digital Markets, Competition and Consumers Bill [Bill 294, 2022-23] was introduced in the UK House of Commons in 2023. A key focus of the Bill is in empowering the CMA in dealing with digital markets, including:

---

61 CMA, Online platforms and digital advertising market study, 1 July 2020.

62 Ibid, Chapter 5.

63 Ibid at 16, 293.

64 Ibid at 293.

65 Ibid at 294.

66 Ibid at 293-94, 395.

67 Ibid, Chapter 8 and Appendix Z.

68 CMA, Online platforms and digital advertising market study, 1 July 2020, Appendix Z.

- "Designating" businesses that are very powerful in particular digital activities, giving them strategic market status in relation to those activities, and
- Ensuring that these designated undertakings comply with rules (called conduct requirements) on how they treat consumers and other businesses in relation to the activities for which they have "strategic market status."
- Giving the CMA powers to address the root causes of competition issues in digital markets, including requiring designated undertakings to share information that might help new competitors enter the market.
- Requiring designated undertakings to be more transparent about mergers which pose risks to competition.
- Allowing the CMA to enforce obligations on designated undertakings and impose penalties including fines of up to 10% of a firm's global turnover for breaches; and
- Empowering the CMA to resolve payment-related breaches of conduct requirements to deal on fair and reasonable terms with third parties, through a 'Final Offer Mechanism' as a "backstop" enforcement tool.[69]

E. INTER-AGENCY COORDINATION MODELS

As Europe's Digital Markets Act observes, powerful "gatekeepers typically operate cross-border, often at a global scale and also often deploy their business models globally."[70] The Internet has no borders. Thus, one cannot expect any single jurisdiction to address or fix all the competition and privacy issues. Privacy and antitrust agencies worldwide must collaborate on a "common strategy" to rein them in.[71]

Noting that "[c]oordination across national borders is critical" to address the "competition and consumer concerns that arise from the conduct of the leading digital platforms, given their global operations," the ACCC's Digital Platforms Branch, for example, aims to "work closely with equivalent teams at overseas competition agencies and overseas consumer agencies," as this coordination "will enable competition and consumer agencies to learn from each other,

[69] https://commonslibrary.parliament.uk/research-briefings/cbp-9781/ https://bills.parliament.uk/bills/3453.

[70] Digital Markets Act at 2 & 5.

[71] Background Note by the Secretariat, Consumer Data Rights and Competition, OECD Doc. DAF/COMP(2020)1 (Apr. 29, 2020), at ¶ 193 (quoting Wolfgang Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection*, J. INTELL. PROP. L. & PRAC. 856 (2016), http://dx.doi.org/10.1093/jiplp/jpw150); see also Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy, Paris, 5th June 2019," (https://www.ftc.gov/system/files/attachments/press-releases/ftc-chairman-supports- common-understanding-g7-competition-authorities-competition-digital-economy/g7_common_understanding_7-5-19.pdf) (calling for the promotion of greater international cooperation and convergence).

enhance cross-border enforcement and, where appropriate, share information and align their approaches to meet the same objectives."[72]

Even if the same agency is responsible for both privacy and competition policy, the agency cannot assume the silos will naturally collaborate. Any large organization, while benefitting from more resources, faces the risks of silos and less communication and collaboration across departments. The agency must proactively work to align/lower opportunities for a clash to occur both domestically and internationally. When there is an actual clash, the jurisdiction will need a legal framework and principles for who will address the conflict, and how.

Checklist of Issues

Thus, each jurisdiction should consider the following checklist of issues:

- Who are the relevant domestic regulators or authorities in your country that have responsibility for privacy, data protection, consumer protection, and competition?
- How can you draw on the expertise of relevant agencies to ensure the goals and knowledge of each agency inform your consideration of intersection issues?
- Can you leverage your informal relationships with your privacy or data protection agency to create a formal cooperation model?
- What broad terms of reference would you envisage for a formal cooperation model? For example:
    - Purpose: agree on the purpose of the working group
    - Membership: identify and invite relevant agencies
    - Scope: In addition to regular meetings, your model may also include information and data sharing, enhancing regulatory capabilities, and identifying collaboration opportunities.

When assessing the benefits of different models of interagency cooperation, the agencies should consider, among other things, whether:

- Agreeing and publicly releasing terms of reference for the group (of privacy and competition authorities).
- Establishing a framework for the group to jointly consider the intersection between competition, privacy, and/or data protection law.
- Pre-empting and addressing any criticism that individual agencies are not communicating with each other to address intersection issues.
- Facilitating a consistent message to stakeholders (such as consumers, digital platforms, and ecosystems).
- Allowing the group of agencies to test or assess the consistency of messages received from stakeholders.

[72] ACCC Final Report at 29.

- Providing a mechanism for domestic advocacy on overlapping areas of policy reform. For example, by bringing to light opportunities for collaboration on joint proposals or submissions.

One well-supported response to the intersection of privacy and competition law has been to create new models of interagency coordination, four examples of which are outlined below.

Four Case Studies of Cooperation

United Kingdom

In the United Kingdom, the Digital Regulation Cooperation Forum (DRCF) was formed in July 2020 and brings together the Information Commissioner's Office (ICO), the Competition and Markets Authority (CMA), the Office of Communications (Ofcom), and the Financial Conduct Authority (FCA). Separately, these agencies have regulatory responsibility for data and privacy, competition and consumer, telecommunications, and financial services.

Building on the strong working relationships among these organizations, the DRCF has been established to ensure a greater level of cooperation, given the unique challenges posed by the regulation of online platforms and digital services.[73]

In seeking this coordination, the UK agencies "believe that competition and data protection law are strongly synergistic, and any areas of perceived tension can be reconciled through careful consideration of the issues on a case-by-case basis, with consistent and appropriate application of competition and data protection law, and through continued close cooperation between [their] two organisations."[74]

The Netherlands

The Netherlands also has launched its own Digital Regulation Cooperation Platform (SDT) in October 2021. This body consists of the Dutch Data Protection Authority (AP), the Netherlands Authority for Consumers and Markets (ACM), the Dutch Authority for the Financial Markets (AFM), and the Dutch Media Authority (CvdM).[75] Separately, these agencies have regulatory responsibility for data protection, consumers and markets, financial markets, and media and broadcasting.

Within the Digital Regulation Cooperation Platform, the participating regulators exchange knowledge and experiences gained from their day-to-day oversight activities in areas such as artificial intelligence, algorithms, data processing, online design, personalization, manipulation, and misleading practices. The participating regulators intend to explore where

[73] For the DRCF's 2022-2023 workplan, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1071501/DRCF_Annual_Workplan.pdf

[74] CMA/ICO Report, 2021.

[75] https://autoriteitpersoonsgegevens.nl/en/news/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation

they can strengthen each other's work in enforcement procedures, for example, by dealing with digital market problems collectively.

Spain

The Spanish National Markets and Competition Commission (CNMC) and the Spanish Data Protection Agency (AEPD) signed in 2018 a Memorandum of Understanding (MoU). This MoU is an administrative agreement in accordance with Spanish Law 40/2015 on the Legal Regime of the public sector, **for cooperation between the two public bodies.**

In the agreement, the cooperation, in all markets and productive sectors may consist of:

- Definition of areas of common interest in the scope of their respective objectives and functions;
- Mutual exchange of information and knowledge in order to achieve the exercise of their respective competencies;
- Early detection of possible infringements in their respective fields of action;
- Set up working groups to respond to specific situations that might arise;
- Other forms of technical cooperation deemed appropriate.

Achievements to date include:

AEPD legal report: The respect of Data Protection Rules (GDPR rules and Spanish Law on Data Protection) by the CNMC performances on competition inspections and handling competition cases. https://www.aepd.es/es/documento/2019-0074.pdf

AEPD shared with CNMC suspicions of competition infringements in a specific market.

Australia

In Australia, the Australian Communications and Media Authority (ACMA), the Office of the Australian Information Commissioner (OAIC), the eSafety Commissioner (eSafety), and the Australian Competition and Consumer Commission (ACCC) have formed the Digital Platform Regulators Forum (DP-REG). Separately these agencies have regulatory responsibility for media and broadcasting, data and privacy protection, online safety and competition and consumer protection, respectively.

DP-REG members share information about, and collaborate on, cross-cutting issues and activities including consideration of issues at the intersection of competition, consumer protection, privacy, media, and online safety regulation. DP-REG has released a joint statement and developed a Terms of Reference that further outlines the purpose and goals of the group.[76] DP-REG's strategic priorities for 2023-24 include assessing the impact of algorithms, improving digital transparency, and increased collaboration and capacity building.

[76] https://www.acma.gov.au/dp-reg-joint-public-statement.

Three working groups were established to progress these priorities and other activities of DP-REG:

- Digital Technology Working Group to jointly explore relevant digital platform technologies (including algorithms) and their regulatory implications;
- Codes & Regulation Working Group to undertake activities that promote a coordinated approach to regulatory frameworks and common regulatory issues, and to build regulatory capability across DP-REG members; and
- Data & Research Working Group to undertake activities that reduce barriers to and support the collection and sharing of relevant data, research, and information across DP-REG members.

Recent activities undertaken by DP-REG include:

- drafting two working papers that examine large language models[77] and algorithms relevant to the regulatory remit of DP-REG members, respectively;
- joint submissions to Australian Government processes in which member agencies have a shared interest;
- ongoing collaboration, information sharing and coordination on matters relating to digital platforms regulation; and
- engagement with international counterparts to scope future opportunities for international collaboration.[78]

* * *

AEPD shared with CNMC suspicious of competition infringements in an specific market.

[77] https://dp-reg.gov.au/publications/working-paper-2-examination-technology-large-language-models.

[78] https://dp-reg.gov.au/news-and-media/digital-platform-regulators-forum-2023-communique,

.