Organisation for Economic Co-operation and Development

DAF/COMP/WD(2024)35

Unclassified

English - Or. English

22 May 2024

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

The intersection between competition and data privacy – Note by Italy

13 June 2024

This document reproduces a written contribution from Italy submitted for Item 8 of the 143rd OECD Competition Committee meeting on 12-14 June 2024.

More documents related to this discussion can be found at www.oecd.org/competition/intersection-between-competition-and-data-privacy.htm

Antonio CAPOBIANCO
Antonio.Capobianco@oecd.org, +(33-1) 45 24 98 08

JT03544215

Italy

1. Introduction

1. The intersection between data protection and competition law is increasingly important for the Italian Competition Authority (hereafter the Authority or the AGCM. The Authority which has intensified its focus on the digital sector, where the collection and exploitation of data, including personal data, are widespread. Their scrutiny extends beyond competition and data protection aspects to include the impact of these practices on consumer rights, highlighting the AGCM's dual role in addressing both competition and consumer issues.

2. The significance of this intersection was underscored by the AGCM's collaboration with the Data Protection Authority and the Communications Regulator in a joint sector inquiry on big data in 2020. This inquiry aimed to evaluate the implications of data handling practices on competitive markets and consumer protection.

3. Additionally, the AGCM's active participation in the International Competition Network's (ICN) special project group dedicated to exploring the intersection of competition law and data protection further demonstrates its commitment to addressing the complex challenges posed by the digital economy[1]. Such efforts are crucial in ensuring that the digital markets operate fairly and transparently, safeguarding both competitive practices and consumer interests.

4. This contribution is organised as follows. After presenting key findings from the AGCM's Big Data inquiry (section 2), it delves into the synergies (section 3) and conflicts (section 4) that emerge between competition law and data protection law in the context of the AGCM's enforcement actions. Building on this analysis, section 5 shifts focus to the role of consumer protection policy, given the AGCM's dual competences, in supporting data protection objectives and reinforcing the broader regulatory agenda. The final section outlines the ongoing challenges and issues that the AGCM faces in effectively managing the intersection of these critical regulatory areas, by highlighting considerations for future actions and research in this evolving field.

2. The 2020 Joint Study on Big Data with the Data Protection Authority and the Communications Regulator

5. Since 2017 the Authority has sought to explore the practices of digital platforms in collecting and exploiting massive amounts of data and their implication, both for competition and consumer protection (being an agency with dual competences). Recognising the need for multi-disciplinary approach, the Authority undertook a pioneering study on big data jointly with the Communication Regulator and the Data Protection Authority[2]. The study, completed in February 2020, was a first attempt to

[1] See ICN, *Competition law enforcement at the intersection between competition and privacy: Agency considerations*, 2024. For more information about this ICN project, check the dedicated webpage.

[2] The final report of the inquiry n. IC53 - BIG DATA, decision n. 28051 published on the AGCM Bulletin n. 9/2020 of March 2, 2020. For an English summary see the AGCM press release of 10

explore the different dimensions of consumer data and its implication for competition, consumer protection and data protection, in a multi-disciplinary perspective. The study led to some very interesting findings.

6. Firstly, it challenged the traditional binary distinctions of "personal data" and "non-personal data". The advent of big data blurs these distinctions, making it arduous to pre-determine the nature of data collected. Techniques such as psychometrics can derive sensitive personal details like political preferences or potential addictions from seemingly innocuous non-personal data.

7. Secondly, a comparative analysis of over a million apps revealed a striking trend: free apps typically harvest more user data than their paid counterparts, illustrating an implicit data-for-service exchange devoid of transparent contractual terms. This finding highlighted a general consumer unawareness about the true economic value of their personal data, particularly in "free" services where data becomes the sole currency. The consumer survey conducted by the Authority revealed the low awareness of consumers about the use of personal data as a quality dimension for competition in the provision of a service, as well as the existence of the so-called privacy paradox[3].

8. Furthermore, the study addressed the practical challenges of adhering to General Data Protection Regulation (GDPR) principles—such as data minimization, purpose limitation, and storage limitation—in the context of massive data collection by digital firms. Often, the purposes for data processing are broadly defined, complicating compliance efforts[4]. This extensive data collection is not only a privacy concern but also a potential competitive advantage, as it enables companies to refine their offerings. However, stringent privacy regulations may hinder companies without direct consumer interactions from accessing valuable data, potentially stifling competition.

9. In response, the study explored several potential remedies, such as enhancing data portability to prevent technological lock-in and foster competition among digital service providers. Despite its benefits, the practical implementation of data portability faces hurdles, including limited consumer awareness and external network effects that restrict user mobility. The study also advocated for the development of common data transfer standards to maximize the utility of data portability rights under constrained conditions.

10. In sum, this multifaceted inquiry not only provided significant insights but also highlighted the delicate balance between protecting personal data and promoting robust competition through freer data circulation. The recommended measures, including fostering open and interoperable data standards, aim to alleviate these tensions and enhance both consumer protection and competitive dynamics in the digital economy.

February 2020. See also the AGCM contribution (section 3) to the 2020 OECD Roundtable on Consumer Data Rights.

[3] The existence of the privacy paradox, consisting in a discrepancy between expressed privacy concerns and actual online behaviour, was inferred from the findings of the survey. Almost 93% of the interviewed users declared to be interested in their privacy protection, but only one third of them denies consent to the collection and utilisation of their data.

[4] Innovative solutions have been proposed by some stakeholders during the study to encourage the individual to participate in the processing of his/her data that uses big data techniques, such as dynamic consent (whereby an individual initially gives their broad consent to a general notice regarding the possible purposes for processing their data, to subsequently receive more detailed information with a request to give additional and more specific consent).

3. Intersection between competition and privacy: complementarities

11. The AGCM's experience so far has shown complementarity between competition and data protection policies. This synergy is particularly evident in the interplay between antitrust enforcement and the regulatory frameworks of data protection and digital markets, such as the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA). Specifically, antitrust enforcement can enhance the effectiveness of data portability rights as stipulated in Article 20 of the GDPR and the principles of interoperability outlined in Article 6, paragraph 2 of the DMA[5].

12. In practice, the AGCM has identified that potential anti-competitive behaviours may manifest through actions that undermine the right to data portability. For instance, a dominant firm might inhibit the interoperability of its platform with those of competing operators, particularly those offering superior privacy protections. Alternatively, such strategies might also impact users who are less concerned with privacy, by obstructing their ability to trade and monetize their personal data through intermediaries. This was notably observed in the AGCM's case involving Google, where practices that potentially restricted the economic exploitation of personal data by users were scrutinized.

13. In July 2022, the Authority opened an investigation against Google for an alleged breach of Art. 102 TFEU, consisting in the refusal to grant interoperability to other platforms and, in particular, Hoda, a start-up that developed an innovative data-portability service allowing consumers to monetise their data by exploiting their right to data portability. By signing up to its app, 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.

14. In the Authority's preliminary view[6], Google's conduct was likely to compress the right to portability of personal data, established by Article 20 of the GDPR, and reduce the economic benefits that consumers can derive from their data. At the same time, the alleged abuse was likely to restrict competition by limiting the ability of operators to develop innovative data-based services.

15. The investigation concluded in July 2023 with the Authority's decision to accept and make binding Google commitments[7]. They included the implementation of tools designed to ease the export of data to third-party operators and to facilitate access to personal data generated by users through their activities on Google's services[8]. The

[5] Art. 6, paragraph 2, of the Digital Markets Act expressly prohibits designated gatekeepers to use the data generated by end-users interacting with third-party services to compete with the latter.

[6] See the AGCM press release of 14 July 2022 on the opening of the investigation.

[7] See Case *No. A552 – GOOGLE-OBSTACLES TO DATA PORTABILITY*, commitment decision no. 30736 published on the AGCM Bulletin no 29/2023. See also the AGCM press release of 31 July 2023.

[8] Three commitments: first, Google committed to help users better navigate Google's Takeout tool, which allows data to be downloaded across Google's platforms for use on other services. Moreover, Google committed to make available to third-party operators detailed documentation and information regarding the data included in connection to users' searches and their browsing histories in order to facilitate their extraction and importation. Finally, Google created a programme that would allow authorised third-parties to directly access the data that consumers have agreed to export without having to go through an intermediary.

implemented measures are intended to bolster the competitive landscape by enabling rivals to better compete in the provision of data-centric services.

16. Complementarity between these two areas of law rests on the assumption that privacy can serve as a critical quality parameter for competition. This perspective aligns with the growing recognition that privacy features can influence consumer choice and thus, market dynamics. However, despite the significance of privacy in competitive terms, there remains a notable gap in consumer awareness regarding the economic value of their data. This observation was substantiated by the findings from the AGCM's study on Big Data (see section 2), which highlighted a pervasive lack of understanding among consumers about how their personal information translates into economic terms. This disconnect underscores a critical challenge: while privacy can be a lever for competition, its potential is curtailed when consumers do not recognize or value the privacy dimensions of the services they use.

4. Intersection between competition and privacy: tensions

17. As highlighted in the 2020 AGCM study, tension between competition and privacy laws may arise when data themselves become a crucial asset for competition. Companies offering personalized services or targeted advertising heavily rely on user data. Hence, competition law might tend to favour practices that collect vast amounts of data, potentially conflicting with data protection principles. At the same time, privacy rules may prevent companies with no direct access to users to acquire or obtain data to compete vis-à-vis the incumbent dominant companies.

18. Competition remedies such as access to data or interoperability can create tensions with data protection law. For instance, this could be the case in markets under liberalization process when the new entrants want access to the monopolist's data on its consumers. Here, the competition agency can be 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 the consumers' privacy interest.

19. The AGCM has indirectly addressed this tension in the electricity markets[9]. In 2018, the Authority charged that the incumbent provider had unfairly obtained customer consent in the regulated market to receive commercial offers from the liberalized market. The provider did so by using allegedly discriminatory methods, specifically by requesting privacy consent separately for its subsidiaries compared to third parties. The AGCM observed that this approach led customers to believe that giving consent to the incumbent's companies was necessary to continue their electricity supply, thus making them more likely to refuse consent to third-party operators. The AGCM argued that this practice gave the incumbent a dual advantage: privileged access to a list of regulated customers and the ability to shape user perceptions to link the incumbent's regulated services with its liberalized offerings, despite regulations requiring a clear separation of these services.

20. Although the Italian Supreme Administrative Court (*Consiglio di Stato*) dismissed the case[10], it remains noteworthy due to the preliminary ruling from the European Court of

[9] See the AGCM case no. *A511 - ENEL/CONDOTTE ANTICONCORRENZIALI NEL MERCATO DELLA VENDITA DI ENERGIA ELETTRICA*, infringement decision no. 27494, published on the AGCM Bulletin no. 2/2019.

[10] The appeal by the parties reached the second level of the administrative proceedings, that is the Italian Supreme Administrative Court (*Consiglio di Stato*), which made a reference for a preliminary

Justice (ECJ). The ECJ clarified that in markets currently liberalizing—where specific information-sharing obligations exist within the boundaries of data protection regulations—the resources available to the incumbent operator by virtue of its former legal monopoly must be equally accessible to new market entrants. Consequently, leveraging these means to favour companies within their own group over potential competitors does not constitute fair competition on the merits.

21. Tensions can also surface when companies employ privacy-enhancing policies that seemingly serve to entrench their market power within an ecosystem. This concern is currently under investigation by the AGCM and other competition authorities in relation to Apple's recent privacy policies. These policies might have imposed restrictions on third-party app developers, particularly limiting their access to advertising data from device users. Such actions raise questions about whether these privacy measures are genuinely aimed at protecting user privacy or if they are strategically used to reinforce Apple's dominance in the market. This investigation aims to distinguish the protective intentions of these policies from potential anti-competitive practices[11].

22. As indicated in the report by the International Competition Network (ICN), tensions between market operators and users can emerge when there is a misalignment in their respective incentives[12]. In some scenarios, consumers may prioritize privacy, yet market

ruling to the Court of Justice of the EU. Following the Court of Justice's ruling of 12 May 2022, the Consiglio di Stato in December 2022 upheld the appeal of the parties. The Council of State dismissed the case because the AGCM had not showed, through evidence such as behavioural studies, that the procedure used by the electricity incumbent in order to collect its customers' consent to the transfer of their information was indeed discriminatory.

[11] See AGCM Case no A561 - press release of 11 May 2023. In May 2023, the AGCM launched an investigation into Apple for a potential abuse of its market dominance in the application (app) sector. The main allegation was Apple's implementation of a restrictive privacy policy that imposed constraints on third-party app developers, particularly regarding their access to advertising data from device users. Specifically, following a privacy policy revision in 2021, Apple began employing pop-up prompts that required users to consent to data tracking by apps for targeted advertising purposes. The AGCM's initial assessment indicated that these prompts were not only more prominently displayed for rival apps compared to Apple's own apps but also employed language that could potentially deter users from granting their consent. Moreover, the investigation is scrutinizing whether Apple has abused its dominant position by limiting third-party developers' access to crucial data used to gauge the effectiveness of advertising campaigns within their apps. The programming interface provided by Apple to third-party developers and advertisers is reportedly far less effective than the solutions used by Apple for its own services. This discrepancy is critical because both the availability of user profiling data and the effectiveness of advertising campaigns are essential for the marketability of advertising space. Such spaces are crucial revenue streams for app developers and are highly attractive to advertisers. Hence, Apple's alleged discriminatory practices could potentially decrease revenue streams for third-party advertisers, disproportionately benefiting Apple's marketing division. Furthermore, these practices could hinder the market entry or sustainability of competitors in the app development and distribution sectors, thereby favouring Apple's own applications, its mobile devices, and the iOS operating system. This investigation highlights the complex interplay between market dominance, privacy policies, and competition in the digital marketplace.

[12] See section I. D of the ICN report (from page 12). More generally, the ICN report, after analysing four possible relationships between privacy and competition, provides a checklist 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

dynamics fail to accommodate this demand. Instead of fostering environments that protect individual privacy, firms often engage in a competitive race to extract and use personal data, exploiting consumers to maximize profits.

23. In some cases, additional interventions through privacy and other policy measures become necessary as they aim to realign incentives to ensure that competition in the privacy domain becomes a race to the top, promoting higher standards rather than a descent into lower ones. Consumer protection strategies, which will be further explored in the next section, can be relevant for safeguarding user interests against exploitative practices.

24. By the same token, enhancing the enforcement of privacy laws, such as the General Data Protection Regulation (GDPR), can deter firms from engaging in anti-competitive behaviours by imposing stricter controls over personal data handling. Additionally, digital regulation can play a significant role, particularly under Article 5(2) of the Digital Markets Act (DMA) which requires gatekeepers to obtain consent from users when they intend to combine or cross-use their personal data across different core platform services[13]. All these combined efforts – competition, consumer protection, data protection and digital regulation - are essential for fostering a digital marketplace that respects user privacy and promotes healthy competition.

5. Intersection between consumer protection and privacy

25. Consumer protection policies can often complement both privacy and competition measures, helping to correct the misalignment of incentives between market operators and users. More broadly, consumer protection laws serve as tools in regulating the data collection practices of digital platforms. The AGCM, endowed with dual competencies in competition and consumer policies, adopts a holistic approach to overseeing cases. These dual competencies often reinforce each other, leading to more effective outcomes when enforcement responsibilities converge within a single agency.

26. Consumer protection laws specifically target aggressive or deceptive practices employed by companies. For instance, companies may use misleading privacy statements to force users into adopting their products or make deceptive claims about the cost-free nature of their services. A notable example occurred in November 2021, when the AGCM imposed fines on Google for engaging in unfair and aggressive commercial practices related to user data utilization. These practices included failing to inform users about data

recognizing those differences, the ICN report provides several principles for jurisdictions to consider, including a checklist to foster inter-agency coordination.

[13] "*2. The gatekeeper shall not do any of the following: (a) process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper; (b) combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services; (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa; and (d) sign in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and has given consent within the meaning of Article 4, point (11), and Article 7 of Regulation (EU) 2016/679. Where the consent given for the purposes of the first subparagraph has been refused or withdrawn by the end user, the gatekeeper shall not repeat its request for consent for the same purpose more than once within a period of one year*."

collection and usage and setting up data sharing consent as an opt-in default option[14]. Similar fines were levied against WhatsApp in 2017 and Facebook in 2018 for comparable breaches involving deceptive data collection practices and the default opt-in settings for data sharing consent[15].

27. Additionally, consumer protection law can address companies conducts failing to disclose how collected data are shared with third parties. A case in point involves Telepass S.p.A. and Telepass Broker S.r.l, (hereafter Telepass) which the AGCM investigated for alleged unfair commercial practices in the distribution of car insurance via their app[16]. The investigation revealed that Telepass received personal data from potential customers seeking insurance quotes without adequately informing them about the data-sharing process with its insurance partners. Although Telepass' privacy notice indicated that the data would be collected for quote calculation and subsequently processed for marketing purposes, Telepass' actions were assessed under the consumer protection lenses of the Authority who concluded that Telepass' practices could mislead customers into making decisions they otherwise would not have, resulting in a significant fine of EUR 2 million for violating the Consumer Code.

28. When Telepass challenged the decision, the Regional Administrative Tribunal for Lazio (TAR) dismissed the appeal, supporting the AGCM's findings that Telepass had omitted crucial information, misleading consumers. The TAR noted that the presentation of the privacy notice was peripheral and not a central factor in assessing the misconduct. Additionally, the TAR concurred with the AGCM's decision not to consult the Italian Data Protection Authority, as the case did not directly challenge data protection laws. However, the decision was overturned when Telepass lodged an appeal to the Supreme Administrative Court. The Court ruled in favour of Telepass by mandating the cooperation with the Data Protection Authority in cases involving the processing of personal data, thus extending the application of the Court of Justice of the European Union's (CJEU) judgment in *Meta v Bundeskartellamt (Meta)* [17] to consumer protection discipline.

29. All the examples provided demonstrate how the three disciplines not only complement but also mutually reinforce one another, effectively navigating the complexities of the digital age.

6. Conclusions

30. The Italian Competition Authority faces a multifaceted challenge at the intersection of competition law and data protection. Balancing the dynamics of a competitive digital market with the imperative of protecting user privacy involves delving into several critical questions.

31. Firstly, the Authority's experience in enforcing both competition and consumer protection laws reveals that the dominant business models, which depend significantly on

[14] See Cases no. PS11147-PS11150, press release of 26 November 2021.

[15] See Case no PS10601, press release of 12 May 2017, Case no PS11112, press release of 7 December 2018 and press release of 17 February 2021. For an overview of these two consumer protection cases, see the AGCM contribution (section 4) to the 2020 OECD Roundtable Consumer Data Rights and Competition.

[16] See the AGCM press release of 18 March 2021.

[17] See European Court of Justice judgment in 4 July 2023 available here.

the broad collection and use of data, necessitate a complex assessment. This includes evaluating proportionality (determining whether the volume of data collected by companies is essential for delivering their services or if the same goals could be achieved with less invasive data practices), transparency (ensuring that users receive clear, concise, and accessible information about data collection, usage, and sharing processes), and user control (empowering users to make informed decisions about their data through straightforward opt-in and opt-out mechanisms).

32. These issues highlight the need for the AGCM to monitor and regulate data collection practices that, while enhancing user experience and targeting advertisements effectively, may also impinge on user privacy and market competition. The dual role of the AGCM is advantageous in addressing these challenges.

33. Secondly, an empirical research can be whether alternative business models, reliant on massive data collection and exploitation, could strengthen data protection without hindering innovation. This involves considering whether the promotion of privacy-enhancing technologies should occur without sacrificing the efficiency benefits derived from targeted advertising and personalized services.

34. Thirdly, as the ICN report emphasizes, effective cooperation between competition and data protection authorities is critical for a comprehensive approach. Investigating potential violations often requires expertise in both competition law and data protection law. A notable development was the decision by the Italian Supreme Administrative Court in December 2023, which mandated cooperation between the AGCM and the Italian Data Protection Authority, extending to consumer protection cases involving data collection and processing practices. This decision, following the European Court of Justice's preliminary ruling on Meta, underscores the need for collaborative regulatory approaches when investigations involve significant data protection issues[18].

35. Finally, as the digital landscape constantly evolves with new technologies and business models emerging rapidly, the AGCM must adapt and develop innovative strategies to address competition and data protection concerns in this dynamic environment. This may particularly involve developing a flexible toolbox of enforcement mechanisms that can respond to new challenges without stifling innovation.

[18] The judgement of the Supreme Administrative court originated from the AGCM case no. PS11710, involving Telepass described in section 5 above. The AGCM contested that Telepass collected personal data from prospective customers seeking insurance quotes without fully disclosing the data-sharing arrangements with its insurance partners. The AGCM clarified that it did not evaluate whether the privacy notice of Telepass, referenced only at the beginning of the quote request process, complied with the EU General Data Protection Regulation (GDPR) and the Italian Privacy Code (Legislative Decree of 30 June 2003, no. 196). When Telepass appealed the decision, the Regional Administrative Tribunal for Lazio (TAR) dismissed the appeal, supporting the AGCM's findings that Telepass had omitted crucial information, misleading consumers. The TAR noted that the presentation of the privacy notice was peripheral and not a central factor in assessing the misconduct. Additionally, the TAR concurred with the AGCM's decision not to consult the Italian Data Protection Authority, as the case did not directly challenge data protection laws. However, the decision was overturned when Telepass escalated the appeal to the Supreme Administrative Court (CDS). The CDS ruled in favour of Telepass, notably applying reasoning from the Court of Justice of the European Union's (CJEU) judgment in *Meta v Bundeskartellamt (Meta)* to this case, suggesting that principles from antitrust cases could also influence the evaluation of unfair commercial practices.