Organisation for Economic Co-operation and Development

DAF/COMP/M(2024)2/ANN5/FINAL

Unclassified

English - Or. English

1 August 2025

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Cancels & replaces the same document of 3 June 2025

Summary of the Roundtable on the intersection between competition and data privacy

Annex to the Summary Record of the 143rd Meeting of the Competition Committee

12-14 June 2024

This document prepared by the OECD Secretariat is a detailed summary of discussion of the Roundtable on the intersection between competition and data privacy, held by the Competition Committee on 13 June 2024.

Please contact Mr Antonio Capobianco if you have questions about this document.
[Email: Antonio.CAPOBIANCO@oecd.org]

JT03569790

Summary of the Roundtable on the intersection between competition and data privacy

1. Introduction by the Chair

On 13 June 2024, the OECD Competition Committee held a roundtable between Competition and Privacy chaired by Frédéric Jenny.

The **Chair** introduced the discussion and explained that it would take place in three parts. The first part will explore the links between competition policy and data privacy. The second part would focus on the experience of countries in their enforcement. The third part will explore the question of cooperation between competition authorities and data protection authorities.

Before delving into specific contributions, the Chair highlighted the increasing relevance of data, particularly in the digital economy, which has made it central to the operations of online platforms and various digital business models. A key question raised was whether data privacy and the collection of consumer data constitute antitrust issues, and if competition considerations should be included in the decision-making processes of data protection agencies. Another critical issue is whether factors traditionally outside one policy domain should be incorporated into assessments. For example, data privacy could be considered a quality parameter in competition assessments, or competition effects could be considered when implementing privacy regulations. These issues are particularly relevant in innovative sectors, often involving complex two-sided digital markets and data monetisation models, such as data scraping and machine learning. Additionally, a many competition and data protection authorities are beginning to collaborate. In various forms (e.g., platforms or forums).

The Chair indicated that three guest speakers would contribute to the roundtable by offering their expertise: **Tim Capel**, Director of the United Kingdom (UK) Information Commissioner's Office (ICO) Legal Service, **Katherine Kemp**, Associate Professor at the Faculty of Law and Justice, University of Sydney, and **Giuseppe Colangelo,** Associate Professor at Basilicata University. Next, he gave the floor to the **Secretariat**, inviting **Carolina Abate** to kick the discussion.

Carolina Abate focused on the interplay between competition and privacy. She stated that even though traditionally, competition law enforcement has been kept separate from data privacy, recent developments indicate a shift, with some jurisdictions recognizing that the collection, accumulation, and sharing of consumer data can raise competition issues. In cases where consumers are also data subjects, data privacy can become a relevant non-price parameter for competition. The Secretariat also mentioned that under a recent "integrationist" approach, data privacy is increasingly seen as a factor in competition assessments, with two key dimensions. First, when companies compete on the level of data protection, competition assessments should consider privacy-based competition and second, even when companies do not directly compete on privacy, their market power may rely on data accumulation, combination and processing making data handling a key competitive factor.

Next**, Prof. Giuseppe Bianco** addressed a complementary question of whether competition in data privacy is concerning. He highlighted the imbalance between data subjects and data controllers, where larger firms may face stricter accountability due to the greater risks, they pose in handling personal data. Another key aspect Bianco explained is the gravity of harm

to individuals. The General Data Protection Regulation (GDPR) preamble suggests that consent may not be valid in situations where there is a significant power imbalance between the data subject and controller. Additionally, the Secretariat noted that data privacy can function as a competitive advantage, as it could be considered a parameter of quality, and firms could compete to offer better privacy protections. The Secretariat also explained that the notion of consent withdrawal is significant, particularly in less competitive markets, where withdrawing consent may negatively impact data subjects. Furthermore, Giuseppe Bianco observed that data protection authorities are increasingly interested in understanding market dynamics and suggested that effective cross-regulatory cooperation is essential.

2. Links between Competition Policy and Data Privacy

The **Chair** thanked the Secretariat and invited **Tim Capel** to provide insights on the work of Data Protection Authorities (DPAs) and his views on whether competition-related consideration should be included in the privacy regulators' assessment or remain solely to competition authorities.

Tim Capel began by discussing how DPAs approach personal data from a rights-based perspective. The expert mentioned that understanding this approach requires a historical view of how privacy laws have developed, notably inspired by Samuel Warren and Louis Brandeis' 1890 article, "The Right to Privacy," which aimed to protect individuals from excessive business and state power, a concern still relevant in today's digital age. The post-World War II recognition of privacy as a fundamental right, particularly in Europe, underscores the DPAs' mission to protect personal data as a matter of human dignity and autonomy.

Tim Capel noted that DPAs also recognize the social value of privacy, considering broader societal harms from unlawful data processing. The GDPR framework reflects this, combining principles of fairness, rights for individuals, right of erasure, etc. While individual rights dominate the interpretation of privacy laws, international frameworks like the GDPR also aim to facilitate the free movement of personal data, striking a balance between privacy and economic considerations. Tim Capel added that DPAs have moved beyond traditional privacy concerns to address the risks posed by Big Data, and algorithmic decision-making. Nowadays, DPAs use economic analysis to understand firms' incentives, considering the dynamics of data-driven business models. Personal data, non-rivalrous in nature, can be shared without losing value, but its accumulation by firms creates privacy risks and reduces transparency. For the speaker, DPAs are increasingly interested in promoting responsible innovation and sustainable economic growth that respects privacy rights. They aim to strike a balance between protecting people's information and encouraging innovation. However, DPAs face challenges in monitoring a wide range of data controllers and processors. Tim Capel also discussed the relationship between privacy and competition. Early intervention to prevent unlawful data collection can limit market concentration, while inaction risks disadvantaging compliant firms. Enforcement by DPAs can reveal hidden data practices, enhancing consumer choice based on privacy and boosting opportunities for challenger firms in markets dominated by incumbents. Lastly, the speaker observed three specific areas where DPAs can apply competition-related concepts, i.e., when considering market power in assessing the controller-data subject relationship, when promoting data portability, and when addressing online choice architecture and harmful design practices like dark patterns to manipulate users into giving up more data than they might willingly provide. In conclusion, Tim Capel emphasised the importance of cooperation between DPAs and competition authorities in regulating digital markets.

The **Chair** thanked Tim Capel for his assessment of the fact that competition authorities and data privacy regulators can cooperate. He then turned to **Prof**. **Katherine Kemp** to address the question of how privacy related consideration should be included in the assessment of competition authorities, and to shed light on concealed data practices.

Prof. Katherine Kemp started by identifying key obstacles to understanding and addressing privacy concerns in competition law, providing a perspective beyond the European Union (EU) and the United States (US), challenging several prevailing myths. The first myth is the assumption that privacy is merely a matter of subjective consumer preference. The speaker argues that privacy degradation leads to objective harm, increasing the risk of identity theft, fraud, manipulation, and discrimination. The second myth is the "privacy paradox," which suggests that consumers claim to value privacy but continue to use services with poor privacy practices. Prof. Katherine Kemp argued that as consumers often lack full knowledge of the privacy risks involved, it is impossible for them to make informed decisions about their data. The third myth is that democratizing data will solve privacy issues. The expert countered that personal data belongs to individuals and should not be commodified for competition purposes. Even anonymised data can often be re-identified, making the concept of democratizing data impractical.

Prof. Katherine Kemp also explained the concept of "concealed data practices", i.e., when companies obscure their privacy policies, use dark patterns in user interfaces, and engage in hidden surveillance. Competition regulators often avoid addressing these issues, treating them as matters of privacy regulation, but this regulatory separation can leave significant gaps, as evidenced by the Google/DoubleClick merger case. Prof. Katherine Kemp recounted how Google initially promised not to combine its search data with DoubleClick's data but later reversed this commitment without facing meaningful regulatory consequences. She argued that this case illustrates how the failure of competition and privacy regulators to coordinate can lead to privacy harms that also distort competition.

In discussing AI development, the speaker highlighted concerns about companies using vast amounts of personal data to train AI models without adhering to data protection regulations. The competition between tech companies in AI, such as Meta's attempts to follow Google's approach, underscores the need for rigorous data protection enforcement to prevent a race to the bottom in terms of privacy standards. Prof. Katherine Kemp also included examples of the Bundeskartellamt’s approach in the Meta case and the US Federal Trade Commission's (FTC) recent focus on consumer privacy. However, these approaches may not easily transfer to jurisdictions with different regulatory frameworks, especially where competition laws focus on exclusionary abuses rather than privacy degradation. In conclusion, Prof. Katherine Kemp emphasised the importance of collaboration between competition and privacy regulators to harmonise enforcement.

3. Experience of Countries in Data Privacy Enforcement

The **Chair** thanked Prof. Katherine Kemp and turned to individual country contributions. He asked **Italy** to discuss the balance in protecting personal data and promoting competition.

Italy discussed the country's extensive experience with big data issues, highlighting a multidisciplinary sector inquiry launched in 2018. Each authority had distinct objectives, highlighting the synergies and potential tensions between different regulatory objectives. The speaker emphasised the importance of understanding the underlying business models in the digital sector rather than just focusing on specific conduct. Digital companies collect data by offering free services initially to accumulate users and data, leveraging network

effects and two-sided markets. Once these companies gain market power, they begin monetizing one side of the market while continuing to accumulate data. Italy included the example of Facebook/WhatsApp and noted that privacy and consumer protection regulators play key roles in overseeing the initial stages of data acquisition, addressing issues such as misleading information, online prompts, and defaults that exploit behavioural biases to obtain user consent. Italy also highlighted concerns about companies' refusing interoperability, as seen in cases like Google/Android and Google/Hoda. These cases, including the ongoing Apple/ATTF case, demonstrate how privacy and data practices can be used as strategies to maintain market power. Italy stressed the importance of understanding the incentives that drive these business models.

The **Chair** thanked Italy and gave the floor to the (**US) FTC** to expand on the interplay between data privacy and competition.

The **FTC** answered that despite some enforcement cases where privacy was a form of non-price competition, broad industry-wide improvements in privacy protections have not been achieved. Instead, firms across various sectors continue to engage in extensive data collection and consumer tracking, often motivated by digital advertising. Consumers are frequently unaware of the large amounts of data collected and the potential harms. One notable case involved Rite Aid, a major US pharmacy chain, which used facial recognition technology for eight years to monitor customers. The FTC found that Rite Aid failed to prevent harm to consumers and the latter agreed to a five-year ban on using facial recognition for surveillance and the implementation of strict safeguards for future use of biometric technologies. Moreover, the FTC criticised the “notice-and-consent” framework for failing to provide meaningful consumer protection, as privacy policies are often complex to comprehend, and businesses use "dark patterns" to steer users toward minimal privacy options. To counter this, the FTC has been pursuing substantive privacy protections in its enforcement, such as restricting the sharing of sensitive information like geolocation data. Additionally, the FTC considered rules that could change the incentives for businesses to engage in mass digital surveillance and promote competition by encouraging business models that do not rely on such practices, potentially allowing new entrants without large data sets to compete more effectively. Lastly, the FTC argues that fostering both privacy and competition is possible by creating a regime that addresses privacy concerns through enforcement, rule-making, or legislation.

The representative, then, gave the floor to the **Department of Justice (DOJ)**. The DOJ added that the 2023 merger guidelines recognize that firms compete along many dimensions, including quality terms like privacy terms, e.g., the Google Search litigation.

The **Chair** thanked the delegates for their comments and invited **Austria** to discuss the synergy between competition law and privacy.

Austria emphasised the growing importance of integrating data protection into competition law through the "privacy as quality" theory. When companies compete based on privacy standards, data protection becomes an important competitive element. One example provided is the change in WhatsApp's terms of service in 2021, which led to a temporary switch of users to messaging services with stronger privacy protections, illustrating privacy’s role in competition law. Another example is the proposed merger of Facebook and GIPHY, which was blocked due to concerns that it would further enhance Facebook's data collection capabilities, raising entry barriers for competitors. To conclude, Austria underscored that data protection is crucial for competition law as consumer preferences shift towards products and services with better privacy standards.

The **Chair** thanked Austria and gave the floor to **Costa Rica**.

Costa Rica first highlighted that the current data protection laws, established in 2011, are outdated for the digital environment. Consequently, two draft laws are currently under consideration, aimed at modernizing the regulatory framework, with a focus on granting individuals rights over their personal data, including access, opposition, data portability, etc. Both competition authorities in Costa Rica, (Coprocom and Sutel) have identified six critical areas that need to be considered in the new legal framework. First, encouraging collaboration among different government bodies to avoid rigid separation between competition, consumer, and data protection authorities. Second, ensuring that the new regulations do not impose excessive compliance costs. Third, noting that the requirement for obtaining express consent might disproportionately impact smaller and newer businesses, which could affect competition. Fourth, pointing out that stricter data protection laws may limit the ability of new companies to acquire consumer data, giving existing companies a competitive advantage. Fifth, emphasizing the need for careful design of data portability mechanisms to address concerns related to the transfer of data. Last, recommending that the DPA should be empowered to establish cooperation agreements with other national authorities to ensure coordination.

The Chair thanked Costa Rica and asked **Israel** to present its framework on data portability.

Israel highlighted the Israeli Competition Authority's joint initiative with the Privacy Protection Authority and the Consumer Protection and Fair-Trade Authority to address data portability. The goal was to empower consumer choice and enhance mobility between service providers. The joint team published a report recommending the adoption of a general right to data portability in Israeli law. Despite the general right to data portability not yet being enacted in legislation, the report's principles have been applied in reforms led by the Israeli Competition Authority. One significant application was during the implementation of data portability in the financial sector, particularly with the transfer of financial data from joint accounts. The DPA emphasised the need for explicit consent from all joint account holders, while the competition authority aimed at reducing consumer burdens. A compromise was reached, allowing one account holder's consent to be sufficient, provided that other account holders are promptly notified and given the right to revoke consent. In conclusion, Israel highlighted that raising and discussing disagreements between authorities during the drafting of the report facilitated future cooperation.

The **Chair** thanked Israel and invited **Prof. Giuseppe Colangelo** to introduce the next part of the discussion.

4. Cooperation Between Competition Authorities and Data Protection Authorities

Prof. Giuseppe Colangelo presented an analysis of the integration between competition law and data protection, as highlighted in a recent paper referenced in the OECD background note. He discussed two main perspectives: the "integrationist" view, where privacy and competition law can complement each other, and the "separatist" view, which warns against merging privacy issues into antitrust enforcement. The integrationist approach suggests that antitrust enforcers should consider how data accumulation strategies undermine privacy and increase market power. In contrast, the separatist approach, which the expert aligned with, argued that privacy and competition pursue different objectives and the integration of privacy into competition law may lead to unintended negative consequences, such as companies exploiting privacy rules to justify anti-competitive conduct. The German "Facebook" case was cited as an integrationist highlight, where privacy was treated as a form of exploitative abuse due to Facebook's data accumulation practices. The speaker contrasts this with the Digital Markets Act (DMA), which introduces

a privacy exception that emphasises the GDPR's role in determining data processing legality, thereby possibly creating privacy primacy over competition concerns. Prof. Giuseppe Colangelo also highlighted that merger control is an area where an integrated approach could be more effective in limiting data accumulation but pointed out that the European Commission (EC) has rarely blocked mergers solely on privacy grounds.

Moreover, several cases were discussed to illustrate how companies may use privacy as a shield against antitrust enforcement, such as Apple/ATTF policy case, and Google Privacy Sandbox, where privacy measures were invoked to justify potentially anti-competitive actions. Four main theories of harm were presented as for the integrated approach. The first suggests a link between a lack of competition, digital markets, and privacy, the second theory relates to merger control, where data accumulation from mergers like the DoubleClick case requires stringent scrutiny due to the potential for privacy violations. The third theory considers privacy as a quality component of products and services. The final theory addresses situations where individuals are forced to accept privacy-invasive terms and conditions under "take-it-or-leave-it" frameworks. The Meta case was referenced as an important milestone in clarifying the legal relationship between data protection and competition law, with the European Court of Justice (ECJ) ruling that antitrust authorities could consider data protection issues, even if the practices complied with the GDPR. However, the speaker notes that the ruling does not fully resolve the complexities of integrating the two fields, particularly when there is no clear GDPR violation. The Italian Telepass case exemplifies these challenges, where the DPA intervened. The speaker concluded by warning against over-reliance on the integrated approach, noting that cooperation between antitrust and data protection authorities, while helpful for GDPR application, may not resolve tensions between privacy concerns and anti-competitive behaviour. There is a risk that privacy could be treated as a "greater good," thus undermining the goals of competition law.

The Chair thanked the Professor and gave the floor to **Prof. Katherine Kemp** and then **Tim Capel**.

Prof. Katherine Kemp highlighted the growing trend of firms justifying potentially anti-competitive behaviour by claiming the need to protect consumer privacy. A notable example from nearly a decade ago is the Toronto Real Estate Board case in Canada, where the federal court dismissed a privacy justification in an abuse of dominance case as pre-textual, even though privacy justifications were recognised as valid in principle. Recently, large digital platforms have begun setting their own privacy rules within their ecosystems. Some of these privacy justifications appear to be pretexts for gaining competitive advantages over rivals. While these platforms exclude competitors in the name of consumer privacy, they often share personal data freely within their various business units, disregarding the purpose limitation principle of privacy regulation. A critical issue for regulators is determining whether rivals should also have access to personal data for fairness or whether dominant firms should be restricted from combining data across different businesses. Prof. Katherine Kemp supported the latter, cautioning, against being overly sceptical of privacy defences. A further challenge is that privacy improvements for consumers may occur in one market, while competitive harm takes place in another, thus preventing firms from using privacy justifications for their actions. Prof. Katherine Kemp argued for the harmonisation of privacy and competition laws to ensure consistent and clear regulatory responses.

Tim Capel emphasised the need for DPAs to take a more proactive role in addressing issues that overlap with competition law. He highlighted the potential for data protection enforcement to support competition by tackling practices like data accumulation and web scraping that contribute to market concentration. There is ongoing discussion within the

data protection community about how best to approach such issues, including clarifying legal frameworks and enhancing cooperation with competition authorities. Tim Capel also stressed the importance of collaboration between competition and DPAs, particularly in Europe. Also, in cases like Google's Privacy Sandbox, the UK ICO has played a crucial role by providing expertise to the Competition and Markets Authority (CMA) and scrutinizing privacy-based arguments put forward by companies like Google. Ultimately, he believes that despite ongoing challenges, the increased dialogue between regulators is a positive step toward addressing these complex issues.

The **Chair** thanked the experts and gave the floor to **Italy** for their comments.

Italy emphasised the importance of cooperation between regulatory authorities, particularly in new regulations like the DSA, DMA, and the Data Act. The goal should be to ensure there are no regulatory gaps when handling cases. While acknowledging that some cases might be annulled due to these tensions, Italy remained optimistic, referencing cases involving major companies like WhatsApp, Apple, Google, Meta, and TikTok, many of which are ongoing or have been confirmed. The speaker urged regulators to continue pushing boundaries through active casework.

The **Chair** thanked Italy and asked **Tim Capel** how he sees privacy compared to other rights, like free enterprise and if he considers privacy equal to, or different from, competition law.

Tim Capel first asserted the importance of privacy as a fundamental right, rooted in historical concerns about data accumulation and loss of individual control. He acknowledged the challenge of balancing privacy with other rights, like the right to business and emphasised the necessity of separate authorities for privacy and competition, recognising the potential for conflict between them. Cooperation between these regulators is essential, as there are difficult decisions about which authority should lead certain investigations. Tim Capel lastly stressed the importance of proportionality in decision-making and advocated for regulators to engage with governments to address these complex questions.

The Chair thanked Tim Capel and gave the floor to **Spain**.

Spain explained that Article 3 of their national competition law allows for the examination of unfair competition practices if they also affect competition under Articles 101 and 102 TFEU. Both the legal violations, like privacy breaches, and their impact on competition must be proven. While judges can apply unfair competition law without proving market impact, competition authorities have exclusive competence when market structure or consumer welfare is affected. Article 3 allows enforcement without needing to prove a dominant position, offering flexibility for future cases.

The **Chair** thanked Spain and invited the **EU** to discuss about pragmatic ways in which competition and data protection have overlapped in different jurisdictions.

The **EU** first noted that data protection plays a role in merger and antitrust cases, including theories of harm and remedy design. In mergers, data protection rules may affect transactions by limiting data-related effects, as seen in cases like Meta and Google/Fitbit. Additionally, the EU assesses whether mergers reduce competition in data protection, as in the Microsoft/LinkedIn case. In antitrust cases, in particular cases of dominant position, data protection considerations may either stem from a company's conduct or be integral to it. Procedurally, the EC cooperates with data protection authorities to ensure consistent outcomes. The EU lastly noted that remedy design also incorporates data protection concerns, particularly in data access or portability, as demonstrated in the Google/Fitbit case. However, the suitability of such remedies is highly case-specific.

The **Chair** thanked the **EU** and gave the floor to **Brazil** to discuss the "Magalu Pagamentos and Hub" case.

Brazil stated that data privacy is overseen by the Brazilian Data Protection Authority, while privacy concerns are considered on a case-by-case basis. This approach was demonstrated by CADE in 2021 during the review of a merger between Magalu Pagamentos and Hub Prepaid. Despite concerns, CADE cleared the merger without restrictions, emphasizing compliance with Data Protection Law, as sufficient to prevent inappropriate data use. CADE also supported strong competition policies and collaboration with other agencies. This collaborative approach was evident in a case involving WhatsApp's privacy policy changes, which required users to share data with Facebook or lose access to the app. CADE issued a joint recommendation preventing WhatsApp from enforcing the policy. Overall, while competition policies can indirectly protect privacy by recognizing it as a quality factor, privacy protection is not the primary focus of Brazil.

The **Chair** thanked Brazil and invited **Greece** to expand on their theory of harm in merger cases related to privacy.

Greece firstly said that in 2022, the Hellenic Competition Commission (HCC) assessed a digital merger involving Delivery Hero, a Berlin-based company operating a food delivery platform, and E-table, Greece's largest restaurant reservation platform. The HCC's primary concern was the potential for conglomerate effects and the ability to implement personalised promotion strategies based on the merged data that could further strengthen the entity's market position. The HCC examined these concerns using theories of harm, particularly focusing on data bundling and "privacy policy tying." This could lead to exploitative effects by limiting consumer privacy. Moreover, the HCC raised concerns about potential vertical integration issues, where the merged entity could gain access to sensitive competitor information. Ultimately, the merger was cleared with remedies, e.g., a strict prohibition on merging consumer data from the two platforms unless explicit user consent was obtained following GDPR rules, particularly Article 51.

The **Chair** thanked Greece and invited **Germany (Bundeskartellamt)** to expand on their landmark decision of the Meta case and what were the key substantive elements of this case.

Germany highlighted that in 2019, the Bundeskartellamt initiated a case against Meta, examining its abusive behaviour regarding the collection of user data. The case focused on Meta's dominance in the market and its unlimited data collection practices. The Bundeskartellamt used GDPR principles as a yardstick, although it did not apply privacy laws directly. The case was appealed by Meta, leading to multiple legal proceedings, including a referral to the ECJ. The ECJ ultimately confirmed that competition authorities could consider data protection rules and stressed the need for cooperation between competition and data protection authorities. Germany highlighted three key aspects: first, Meta's data practices were seen as abusive toward consumers, forcing them to accept extensive data collection. Second, the case involved exclusionary abuse against Meta's competitors, who lacked similar access to user data. Third, users must be offered a version of the service that processes only the personal data necessary for the service, potentially for an appropriate fee. Germany further commented that this case is not an isolated phenomenon and has influenced legislation, including Germany's Section 19A and the EU's DMA in Article 5.2. Similar cases have since emerged, such as the Google Data case and an ongoing investigation into the Apple/ ATTF case. This investigation refers to potential self-preferencing and hindering of third parties rather than abuse. The framework of Apple requires additional consent for tracking users on third-party apps and websites. However, Germany stated that ATTF does not seem to apply its own services to Apple, and therefore, this case is about the selection of who acquires the data. Apple claims to

prioritise data protection, but this stance seems limited to external companies, excluding its own services, raising the critical question of whether the law should govern data access or if such control should be left to the dominant market players.

Germany also reflected on the Facebook case, which started in 2019, and although it has gone through multiple legal stages, remains unresolved. The delegate highlighted the significant delays caused by companies using every available legal avenue to postpone outcomes, questioning the ability of current legal frameworks to handle such cases effectively in an era of rapid technological change. The speaker highlights concerns about the lengthy, noting that companies often use delaying tactics. With AI rapidly transforming industries, the speaker questions whether the current legal framework can adequately address outdated cases in a fast-evolving world.

The Chair acknowledged the importance of Germany's last comment and gave **France** the floor.

France emphasised the need for collaboration between competition authorities and DPAs, even when disagreements arise. Cooperation is essential to navigating the regulatory landscape and ensuring that firms understand how to comply with both privacy and competition requirements. especially in the rapidly evolving legal and technological environment. The speaker also expressed surprise at Prof. Giuseppe Colangelo's claim that cooperation between competition and privacy authorities presents an inherent problem, as while differences in outcomes may exist, cooperation is still a legal obligation, and firms should be made aware of how the two regulatory bodies interact. France provided examples of increased collaboration between the French Competition Authority and the CNIL (France's DPA). This collaboration is formalized through joint seminars and workshops and reinforced by a Memorandum of Understanding (MoU) between them. One of the primary cases discussed is Meta, where the legal landscape around data privacy and competition has evolved significantly. This cooperation is also reflected in the new legislative frameworks at the European level, such as the DMA, the Data Act, the Data Governance Act, and the AI Act. The speaker stresses that the authorities need to provide clarity on how these regulations will be enforced and interpreted.

A key example of the interaction between privacy and competition law is the French Competition Authority's investigation of Google, resulting in a €250 million fine related to neighbouring rights for press content. Although this case did not involve personal data, it centred on intellectual property rights and Google's failure to inform publishers or allow them to opt out of data usage. This case highlighted the complexity of data processing and the overlapping interests of privacy and competition law, even when the subject matter extends beyond traditional privacy concerns. The ATTF case is another example of this interaction. The question was whether Apple's actions discriminated against competitors while favouring its services. The CNIL provided guidance based on the consent requirements of data protection law, but the competition authority focused on whether Apple's actions constituted discriminatory behaviour. The case illustrated the complementary perspectives of the two bodies, with the competition authority recognising that consumer privacy protection could be considered a legitimate objective within competition law.

France also addressed the difficulties posed by lengthy legal proceedings, especially when dealing with large tech firms. These companies can delay legal outcomes, creating challenges for regulatory authorities trying to keep up with fast-moving technological changes. In particular, the speaker raised concerns about the balance between competition and privacy in European decisions. While privacy is a fundamental right under Article 8 of the European Convention on Human Rights (ECHR), competition law might not always be given the same weight, even when both aspects are important. In conclusion, France

stressed that while tensions between competition and privacy law will continue to exist, close cooperation between the relevant authorities is crucial.

The **Chair** thanked France for their contribution and introduced the last part of the discussion, i.e., the models for cooperation and the experience of cooperation between data privacy authority and competition authorities. He, then, gave the floor to the **UK**.

5. Models For Cooperation Between DPAs and Competition Authorities

The **UK** was represented by **Andrew Thompson,** from ICO and **Noel Tarleton** from the CMA, who first introduced himself**.** Next, **Andrew Thompson**, from the UK's ICO outlined the growing intersection between data protection and competition in digital markets, noting that these points have been previously well-articulated and will not be readdressed. Instead, he focused on practical considerations, and the approach to cooperation between regulatory bodies, particularly facilitated by the UK's Digital Regulation Cooperation Forum (DRCF). The DRCF was established to address the opportunities and challenges arising from digital markets, which often cut across traditional regulatory boundaries. Operating under a flexible framework, the DRCF coordinates efforts on matters where cooperation will have the greatest public impact. A staffed central team, led by CEO Kate Jones, provides strategic direction and coordination. The DRCF also ensures senior engagement across all four regulators through quarterly meetings and annual work plans. Since 2020, the ICO and CMA have focused on several bilateral regulatory priorities. Key areas include joint statements on the Google Privacy Sandbox and mobile ecosystems, particularly Apple's ATTF and information sharing. As an example of cooperation, the joint position paper on harmful online design was published in 2023. The paper focused on promoting meaningful user choice and control, addressing transparency and consumer autonomy. It also identified harmful practices such as nudging users to accept unwanted data practices and set out expectations for companies to design choice architectures that benefit consumers both in terms of data protection and competition.

Next, **Andrew Thompson** gave the floor to **Noel Tarleton** to continue the presentation.

Noel Tarleton highlighted the rapid evolution of foundation models and generative AI, emphasising the need for proactive regulatory involvement. The CMA initiated its review of foundation models in May 2023, producing reports in September and April. Simultaneously, the ICO is consulting on generative AI and data protection, reflecting the growing need to shape the market rather than react to emerging problems. The April report from the CMA proposed key principles to help guide the development of the market. The purpose of a joint statement from the CMA and ICO was to explore potential overlaps and ensure a coherent regulatory approach. Noel Tarleton used transparency in data usage as an example of overlap, as it is essential for both consumer protection and data protection. Additionally, the CMA and ICO are revisiting their 2021 joint statement, which addressed synergies and tensions between data protection and competition. A significant concern is ensuring that companies do not misuse data protection regulations as a pretext for anti-competitive behaviour. For instance, any competition authority intervention must account for the implications of data protection, as in the case of Google's Privacy Sandbox. The updated statement in 2025 will likely focus on issues such as data access, sharing, interoperability, and user choice.

Andrew Thompson, for the last part of the presentation, emphasised that cooperation between the ICO and CMA extends beyond bilateral priorities. This collaboration also involves Ofcom and the Financial Conduct Authority (FCA) through broader projects

under the DRCF. One major initiative is their work on AI, where they analyse its benefits and harms, ensure coherence on key concepts such as fairness and accountability, and deepen the understanding of AI auditing. Additionally, the DRCF conducts horizon scanning to monitor emerging technologies, including quantum computing, Web 3.0, immersive tech, and digital ID. They also have an ongoing project focused on developing skills and capabilities within regulatory bodies, particularly on acquiring and nurturing talent through training and development. Another key initiative is a pilot project, supported by government funding, aimed at providing advice to innovators whose challenges span multiple regulatory domains. The speaker encourages stakeholders to explore the DRCF website for further information on these projects.

The **Chair** thanked the UK and asked two follow-up questions: (a) if cooperation is needed, and (b) if the joint statement reflects full consensus or acknowledges differences on some issues.

Andrew Thompson acknowledged the complexity of resolving those tensions between data access and privacy, using the example of data access, which can break down barriers to entry and promote competition, but could also degrade privacy and introduce new risks. The solution lies in designing remedies that prioritize data protection and fairness by design. This approach may require trade-offs but aims to deliver a pragmatic and balanced solution that considers both privacy and competition concerns.

Noel Tarleton confirmed that not all tensions between competition and data protection can be resolved. While some challenges remain, the primary goal is clarity, particularly regarding pretextual issues where firms might misuse data protection claims.

The **Chair** thanked the UK delegates for the presentation and gave the floor to **Canada** to share their experience on the issue of cooperation.

In June 2023, **Canada** established its regulatory forum to strengthen collaboration and information sharing among federal agencies. The forum included the Competition Bureau, the Canadian Radio-Television and Telecommunications Commission, and the Office of the Privacy Commissioner. Its primary goal was to address complex digital market issues and enhance cooperation across mandates. During its first year, the forum focused on relationship-building and understanding each agency's responsibilities. It also focused on AI, chosen due to its rapid development and a speaker series was organised to educate staff on AI fundamentals. The second year aims to further develop work on AI and data portability. Overall, Canada noted that the forum's first year was productive, and promises to foster stronger regulatory collaboration.

The **Chair** thanked Canada and invited **Mexico** to describe the content of their Memorandum of Understanding (MoU) between the Federal Telecommunications Institute (IFT) and their DPA.

Mexico stated that their coordination between competition and privacy authorities is becoming increasingly important due to the growing significance of data in digital markets. The National Institute for Transparency, Access to Information and Personal Data Protection (INAI) is the privacy regulator, while the IFT oversees competition in telecommunications and broadcasting. In 2021, these two entities signed an MoU to strengthen collaboration on promoting transparency, data protection, and competition. The MoU focuses on sharing statistical data, conducting joint research, and organizing collaborative activities. Two key advocacy initiatives were highlighted: in 2023, the IFT and INAI released a guide for senior citizens on protecting personal data to enhance digital literacy and prevent data breaches. In 2024, the IFT developed an interactive tool that allows users to compare the privacy notices of major digital platforms. Furthermore, the IFT has conducted market studies on competition in digital markets, including the analysis

of the potential role of massive data collection. Finally, Mexico considered it crucial for telecommunications and privacy regulators to account for competitive dynamics to better address the challenges of competition and privacy in digital market.

The **Chair** thanked Mexico and gave the floor to **BIAC** to provide recommendations to address the complexities and challenges resulting from the interplay between data and competition.

BIAC emphasised that while data is critical to the digital economy, it presents significant challenges for consumers and markets. The speaker raised key questions about how to balance privacy rights with fostering innovation and competition, and how to design adaptable policies that address the complexities of the data-driven world. BIAC explored how data privacy and competition are interconnected, requiring a holistic approach acknowledging the diverse interests of stakeholders, including platforms, advertisers, and users. BIAC also recommended fostering collaboration between competition and privacy authorities, as well as engaging with academics, businesses, etc. and international organisations to share insights and best practices. Three key considerations were highlighted: authorities should continuously evaluate the outcomes of their actions, consider the diversity of the digital sector, and competition and privacy authorities should work together to establish a consistent legal framework enhancing competition and privacy protection. In conclusion, BIAC stressed the importance of collaboration among all stakeholders to ensure that the digital economy benefits consumers and markets.

The **Chair** thanked BIAC and gave the floor to **DSTI**.

DSTI first expressed gratitude to the participants, emphasising that cross-regulatory cooperation is a top priority in their strategy. Two key points were highlighted. First, although the themes of AI, data, and competition were mentioned separately throughout the conversation, the speaker suggested that these should be more integrated. Second, the speaker shared news of an upcoming event with Kate Jones, Chair of the UK DCRF and the International Network for Digital Regulation Cooperation. The event, set for November 8th, 2024, would involve network members and countries interested in digital regulatory cooperation.

The **Chair** thanked DSTI and invited the experts to comment on the previous contributions, starting from **Prof. Katherine Kemp** and then **Prof. Giuseppe Colangelo**.

Prof. Katherine Kemp highlighted two key points. Firstly, she acknowledged that in the Meta case, which focused on exploitative abuse, there were also claims of potential exclusionary harm. However, she pointed out that this case is challenging to replicate in jurisdictions that only recognise exclusionary abuses, as in such cases, courts might question why alternative data sources were not pursued. Secondly, the expert noted that tensions between competition and DPAs often arise when large technology companies fail to apply data protection rules consistently across their various business operations, emphasising the need for uniform enforcement of these regulations.

Prof. Giuseppe Colangelo agreed with some of the points made and stressed that although there is increasing awareness of the potential tension between data and competition, he disagreed with the added value, calling for a cautionary approach on the scope of the intervention.

Tim Capel expressed gratitude for the opportunity to participate in the discussion, praising the examples shared. He expressed optimism while also acknowledging the need for realism. He also pointed out that data protection authorities could benefit from learning about enforcement practices from competition authorities, which often have more resources. Drawing on his experience, he emphasised the value of building closer ties

between regulators, noted the difficulty of lengthy legal processes and expressed enthusiasm for the November 8th event.

The **Chair** thanked all the participants and agreed with Tim Capel's comment on the value of cooperation. He emphasised the importance of continued dialogue between regulators, such as UK and Canada. After a break, the next topic will be the selection of future roundtable discussions.