Organisation for Economic Co-operation and Development

DAF/COMP/WD(2024)32

Unclassified

English - Or. English

10 June 2024

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Cancels & replaces the same document of 7 June 2024

The intersection between competition and data privacy – Summaries of contributions

13 June 2024

This document reproduces summaries of contributions 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

JT03545729

Table of contents

Austria

The Austrian contribution illustrates the growing synergy between competition and data protection laws. The convergence of competition and data protection law aims to protect fair competition but also the right to data protection by fostering an environment in which competition law and data protection law complement each other.

Competition law and data protection law both aim to prevent exploitation of imbalances. While competition law focuses on efficient markets in which consumer welfare is increased by appropriate competition in the relevant market, whereas data protection law ensures confidentiality and privacy of personal data. Privacy can also serve as a quality differentiator in products, influencing competition. However, integrating data protection assessments into competition evaluations poses challenges, such as addressing GDPR infringements that unfairly advantage companies.

Austrian data protection law provides strong data protection rights to both natural and legal persons, through the Austrian Data Protection Act (DPA), surpassing GDPR in some respects. According to Austrian national law companies can also file data protection complaints in case of violating the right to secrecy. The Austrian Federal Competition Authority (AFCA) must balance data protection during dawn raids, ensuring legal bases for data processing.

During dawn raids, the AFCA secures and analyzes (electronic) data at its premises, balancing data protection rights with investigation needs. Secured data is handled with stringent safeguards to protect personal and confidential information. The AFCA's procedures aim to minimize business disruption and ensure transparency, with secured data evaluated in controlled environments and deleted after proceedings.

Advancing digitalisation and its regulation require the AFCA and the Austrian Data Protection Authority to cooperate more closely with other supervisory and regulatory authorities in Austria, but also among themselves, in order to ensure the most consistent approach possible. This cooperation, although resource-intensive, is vital for consistent enforcement and mutual support. The European Court of Justice's ruling in case C-252/21 further emphasizes the need for cooperation to address evolving data-driven business models.

Competition and data protection laws are inextricably linked and require harmonisation of legislation and competent authorities to protect fair competition and data protection rights at the same time. Co-operation between regulators is crucial to manage the complexity of the digital age.

BIAC

Business at OECD (BIAC) is grateful for the opportunity to comment on the relationship between competition and privacy laws.

The digital economy is increasingly driven by data, with technological advancements such as machine learning elevating its importance and complexity. These evolutions have rendered data to be an increasingly important aspect of competition law assessment, especially where data may function as a crucial input or product. To illustrate the power of data in machine learning, one might consider a simple non-technological analogy from agriculture: just as seeds require soil, water, and nutrients to grow into crops, learning algorithms (seeds) need data (soil) to develop into sophisticated programs (crops). The availability of data directly correlates with the learning potential of an algorithm – without data, there is nothing to learn. This underscores the significance of "big data" in the machine learning process.

Amidst this backdrop, concerns about the impact of data on consumers and markets are intensifying. Debates are focusing on issues such as the role of privacy as a consumer preference and the potential for privacy regulations to restrict competitiveness, for instance by limiting or prohibiting data portability or interoperability. This intersection, and the idea of needing cooperation between competition law and privacy law enforcement, is an evolution from the view that these two areas of the law are distinct.

Given the diversity of privacy and competition laws across jurisdictions and the constant evolution in related jurisprudence, competition authorities and data protection authorities must navigate the intersection of these domains with caution. The 2019 *Meta* decision by the German Federal Cartel Office (Bundeskartellamt or BKartA) is illustrative of the possible tension between the two areas.[1]

In this controversial case, it was eventually decided that Meta (formerly Facebook) had exploited its dominant position in the German market for social networks for private users by making the use of its social-network platform conditional on users granting extensive data collection permissions, not only for Facebook itself, but also for other sources, such as Meta's other services and third-party service providers. In its decision the BKartA concluded that Facebook's terms and conditions infringed both data protection regulations and competition law. However, the case was reviewed by several courts. First, the Higher Regional Court in Düsseldorf suspended the Authority's decision having serious doubts on whether the decision had the right legal basis.[2] Subsequently, the German Federal Supreme Court overturned the Higher Regional Court's judgment, reinstating the consequences of the Authority's decision, but based on the reasoning of an exclusionary and exploitative abuse.[3] Due to this divergence between the German courts, the Higher Court of Dusseldorf

[1] Bundeskartellamt, Case Summary: Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing, Case B6-22/16 (Feb. 15, 2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3.

[2] Case VI-Kart 1/19, Facebook/Bundeskartellamt, Judgment of the Higher Regional Court Dusseldorf of 26 August 2019, https://www.d-kart.de/wp-content/uploads/2019/08/OLG-D%C3%BCsseldorf-Facebook-2019-English.pdf.

[3] Case KVR 69/19, Bundeskartellamt/Facebook, Judgment of the German Federal Court of 23 June 2020, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/BGH-KVR-69-19.pdf?__blob=publicationFile&v=1.

requested a preliminary reference from the Court of Justice of the European Union (CJEU).[4] The CJEU eventually decided that Competition Authorities can investigate violations of GDPR as potential abuses of a dominant position, but that when doing so they are bound by a duty of sincere cooperation with the relevant data protection authority.[5] By doing so, the CJEU essentially recognized the dual role of data as both a competitive tool and a privacy concern. This may guide other authorities and courts in how to address the intersection of competition law and data protection regulations.

This submission adds to BIAC's previous contributions on related topics, including ex-ante regulation and competition in digital markets,[6] abuse of dominance in digital markets,[7] consumer data rights and impact of competition,[8] interactions between competition authorities and sector regulators,[9] competition enforcement and regulatory alternatives,[10] and the evolving concept of market power in the digital economy.[11]

[4] Case Kart 2/19, Bundeskartellamt/Facebook, Decisionn of the Higher Regional Court Dusseldorf of 24 March 2021, https://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2021/Kart_2_19_V_Beschluss_20210324.html.

[5] Case C-252/21, Meta Platforms and Others, ECLI:EU:C:2023:537 (July 4, 2023), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0252.

[6] OECD, Ex-Ante Regulation and Competition in Digital Markets – Note by BIAC, DAF/COMP/WD(2021)79 (Nov. 24, 2021), https://one.oecd.org/document/DAF/COMP/WD(2021)79/en/pdf.

[7] OECD, Abuse of Dominance in Digital Markets – Contribution by BIAC, DAF/COMP/WD(2020)38 (Nov. 25, 2020), https://one.oecd.org/document/DAF/COMP/GF/WD(2020)38/en/pdf.

[8] OECD, Consumer Data Rights and Competition – Note by BIAC, DAF/COMP/WD(2020)46 (May 28, 2020), https://one.oecd.org/document/DAF/COMP/WD(2020)46/en/pdf.

[9] OECD, Interactions between Competition Authorities and Sector Regulators – Contribution from Business at OECD (BIAC), DAF/COMP/GF/WD(2022)64 (Nov. 18, 2022), https://one.oecd.org/document/DAF/COMP/GF/WD(2022)64/en/pdf.

[10] OECD, Competition Enforcement and Regulatory Alternatives – Note by BIAC, DAF/COMP/WP2/WD(2021)18 (May 31, 2021), https://one.oecd.org/document/DAF/COMP/WP2/WD(2021)18/en/pdf.

[11] OECD, The Evolving Concept of Market Power in the Digital Economy – Note by BIAC, DAF/COMP/WD(2022)34 (June 9, 2022), https://one.oecd.org/document/DAF/COMP/WD(2022)34/en/pdf.

Brazil

This article aims to discuss the various intersections between Competition Law and Privacy Law, presenting a Brazilian perspective on merger analyses. In this regard, there is a theoretical divide. Some authors argue, for example, that some mergers need interventions by competition authorities, not because prices will increase if the operation is approved, but because the approval of the merger itself may decrease the level of privacy enjoyed by users of digital platforms in the post-merger period.[12] This kind of concern is exacerbated in a context where people are experiencing changes typical of the industry 5.0 and there is an intensive use of data collected automatically, by different types of devices (via the Internet of Things, for example), or through digital platforms in general. Other authors disagree with this diagnosis[13] and consider that competition authorities should not replicate or replace the work of data protection authorities and consumer protection authorities,[14] urging moderation on this issue. This article seeks to describe these different perspectives and to explain how CADE (Brazilian Administrative Council for Economic Defense) has positioned itself. As will be demonstrated throughout the article, CADE maintains a conservative stance, and understands, in an orthodox manner, that consumer welfare is and should continue to be the value to be pursued in Competition Law.

[12] (FIDELIS, 2017[1]).

[13] (BHATTACHARYA and BUITEN, 2018[2])

[14] (COOPER, 2013[3]; OHLHAUSEN and OKULIAR, 2015[4]),

Canada

Canada's Competition Bureau[15] is pleased to provide this submission to the OECD's "Roundtable on The Intersection between Competition and Data Privacy Policy".

The Bureau, headed by the Commissioner of Competition, is an independent law enforcement agency of the Government of Canada. Among other things, it administers and enforces Canada's competition law – the *Competition Act*.[16] Its mandate is to protect and promote competition for the benefit of Canadian consumers and businesses.[17]

The Office of the Privacy Commissioner of Canada ("OPC")[18] is headed by the Privacy Commissioner of Canada ("Privacy Commissioner") and is an agent of Parliament.[19] The OPC oversees compliance with the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").[20,21] Its mission is to protect and promote privacy rights.

The Bureau welcomes this opportunity to comment on the intersection of competition and data privacy in digital markets. In this submission, the Bureau highlights:

- Amendments to our laws, proposed and past, that concern:
  - the organizations' authorities to share information; and
  - the Competition Tribunal's regard for privacy in certain competition enforcement matters.
- A newly-formed partnership with the aim of promoting informal collaboration.

[15] The word "Bureau" is used in this document to refer interchangeably to the Competition Bureau and the Commissioner of Competition.

[16] *Competition Act*, R.S.C., 1985, c. C-34.

[17] For further information about the Bureau, visit (2024) Competition Bureau Canada.

[18] The word "OPC" is used in this document to refer interchangeably to the Office of the Privacy Commissioner and the Privacy Commissioner of Canada.

[19] For further information about the OPC, visit (2024) About the OPC.

[20] *Privacy Act*, R.S.C., 1985, c. P-21, and *Personal Information Protection and Electronic Documents Act*, S.C., 2000, c. 5.

[21] The *Privacy Act* governs the federal government's use of personal information. PIPEDA applies to private-sector organizations across Canada and governs their collection, use and disclosure of personal information. Of the two acts, PIPEDA is most relevant to this submission. For further information, visit the OPC's PIPEDA in brief.

Costa Rica

The intersection between competition and privacy has emerged as an area of growing importance in the contemporary regulatory landscape. One key issue raised is whether competition authorities are adequately considering privacy considerations in their cases. Traditionally, antitrust investigations have focused on issues such as the restriction of competition and abuse of dominant position. However, in the current digital context, data collection and use can play a fundamental role in determining anticompetitive effects. In the digital era, where massive data collection is ubiquitous, the question arises of whether data concentration in the hands of a few dominant companies can undermine competition by creating entry barriers for new competitors.

In Costa Rica, the protection of personal data is regulated primarily by the provisions contained in the Law for the Protection of the Individual against the Processing of their Personal Data, Law 8968. The regulatory framework for the protection of personal data has not undergone substantive reforms to date, and therefore falls short in terms of the necessary provisions to regulate data protection issues in a digital environment.

This has led to the consideration of the need for a new Personal Data Protection Law in the country that addresses current needs in the field. Currently, two draft laws aimed at modernizing the regulatory framework for personal data protection are in the legislative pipeline. These draft laws address elements to confront the challenges of a data-driven economy, as well as to reconcile the importance of cross-border flows of personal data with broad guarantees for compliance with data protection of citizens in a technological uncertain environment.

In relation to the draft laws currently under consideration in the Costa Rican legislative process, it is considered indispensable to ensure that upon the issuance of a new legal framework regarding the protection of personal data, the country adopts a coordinated approach among different government bodies.

Similarly, when analyzing the Draft Law on Remunerated Non-Collective Transportation of Persons and Digital Platforms, it provides a critical insight into how the functional requirements set for technological platforms can impact market competitiveness.

The interface between competition policy and data protection in Costa Rica presents a multifaceted challenge necessitating a balanced approach that considers the interests of both competition and privacy. Despite notable advancements in regulating these domains, substantial hurdles remain in reconciling their occasionally conflicting objectives. Collaboration among competition and data protection authorities, alongside enhanced alignment of laws and regulations, could prove pivotal in overcoming these obstacles and fostering a competitive business environment that upholds privacy standards in Costa Rica.

European Union

The European Commission ("Commission") agrees with the findings of the OECD background note that, in the digital economy, the collection, access and sharing of large amounts of data raises issues both under competition and data protection laws. Accordingly, there is an increasing interplay between those two areas of law [or between the two sets of rules], and between the authorities enforcing them respectively.

While competition law and data protection pursue different objectives, both have a crucial role to play in ensuring that undertakings collect and use data in ways that benefit citizens. Those rules protect different, but complementary interests. Therefore, competition and data protection rules should be used in a complementary way, to ensure consistent outcomes and avoid potential conflicts.

On substance, while violations of the data protection rules as such are assessed by data protection authorities, the Commission can and does consider data protection considerations in competition cases, when they are a relevant parameter of competition. This duly takes into account the realities of the digital economy, as the European Court of Justice ("ECJ") recognized in the *Meta* judgment.

In merger control, the Commission has considered data protection as a qualitative parameter of competition when reviewing certain concentrations. The submission will illustrate those cases. In antitrust, the ECJ has recognized that, when assessing an abuse of dominance, a competition authority can take into consideration compliance with data protection rules, to assess whether a conduct departs from competition on the merits and to assess its consequences. Furthermore, data protection considerations may also arise in the context of remedies design and as a possible objective justification for an abusive conduct.

From a procedural standpoint, the Commission also agrees that it is important to ensure coordination and cooperation between competition authorities and data protection authorities, to share information and ensure consistent outcomes, as required by the *Meta* and *BPost* judgments of the ECJ.

Germany

For many years now, the digital economy has been a key focus of the Bundeskartellamt's work. This has even intensified since the German legislator introduced a new provision, Section 19a, in the German Competition Act in 2021. It allows the Bundeskartellamt to intervene more quickly and effectively against anti-competitive practices by large digital companies.

Accordingly, the intersection between data protection law and competition law has become ever more important for the Bundeskartellamt. Intensive cooperation with other authorities can be crucial in cases involving data-driven business models or data-related theories of harm.

The interplay between data protection law and competition law is particularly evident in the Bundeskartellamt's Facebook case. In the contribution, this case is described in more detail (under 2.) before it is briefly outlined how this case has inspired both national and European legislation (under 3.). Furthermore, cooperation with the (national) data protection authorities is illustrated on the basis of two concrete case studies (under 4.). The paper closes with a short summary (under 5).

Greece

The digital economy is characterized by rapid technological developments and the combination of economic and digital power. Interactions between antitrust and data privacy are the most common in the digital sector. In this new digital landscape, privacy enforcers are intensely focused on protecting individuals from unlawful data processing, while competition law focuses on the role of data in driving competition, particularly in the digital economy.

This Note overviews the intersection between data protection and competition law which has become an increasingly important issue in the new continuously evolving digital landscape. It first delves into the recent experience of the Hellenic Competition Commission ("HCC") in the merger context, focusing on the privacy concerns and implications assessed by the authority.

It then shifts focus to the interaction between the data protection and competition law, highlighting on the HCC's initiatives and the cooperation it has developed with the national data privacy regulator, so that they can ensure the effective application and enforcement of their respective policy realms.

A merger case with privacy considerations and implications was assessed by the Hellenic Competition Commission (2022). The HCC examined various data- based theories of harm and determined that the competition concerns arising therefrom could be alleviated and effectively addressed through the imposition of behavioral remedies.

The HCC's decision followed an in-depth investigation of the proposed merger between a digital platform active in the provision of online ordering and food distribution services and the target companies providing online intermediation services for reservations in restaurants reviewing the merger for horizontal, vertical and conglomerate effects. The HCC's investigation revealed that the combination of the parties' activities in the market for online intermediation for restaurant reservations and in the online intermediation market for food ordering, would give rise to conglomerate effects. The HCC considered theories of harm related to the collection and combination of data from a company that offers more than one platform services. The transaction was cleared by the HCC regarding horizontal effects of the merger without remedies. With respect to conglomerate effects arising from the transaction, the HCC cleared the merger with the adoption of the behavioral commitments.

The HCC recognizes the importance of cooperation with data privacy authorities in a constantly evolving digital landscape and the need to develop innovative strategies to address competition concerns in this dynamic environment. In this respect, it signed a Memorandum of Cooperation, with the greek data privacy regulator, Hellenic Data Protection Authority (HDPA) in August 2022, in its effort to further enhance cooperation between the two Authorities. HCC and HDPA agreed on further tightening the links between them, sharing know-how and building on both Authorities' experience with the aim of benefiting citizens, the economy and the public interest in general, while ensuring the freedoms and rights of individuals, in particular the protection of personal data.

Through its efforts highlighted by the continuing and enhanced cooperation with the data privacy regulator and commitment to respond to new challenges, HCC may contribute more effectively to the achievement of the ultimate goal of benefiting consumers.

Israel

This note examines the interface between competition and data privacy policy from the perspective of the Israel Competition Authority (ICA), focusing on advocacy initiatives concerning data portability and merger review involving data-related competitive concerns.

In advocacy, the ICA has collaborated with other Israeli regulators, including the Israeli Privacy Protection Authority, to promote data portability as a way to advance both competition and privacy goals. Jointly we issued a report recommending a general right to data portability in Israel, enabling consumers to access their personal data in a standardized format. The principles of the report have been implemented in sectoral regulation in the financial sector under the Financial Data Service Law, which grants consumers the right to share their financial data with third parties. Additionally, the ICA recommended transitioning the centralized pension clearing system from its current monopolistic model to a more open and competitive model, enhancing data portability for consumers through a wider range of service providers.

Regarding merger review, in the Harel/Isracard case the ICA assessed potential anticompetitive effects arising from the merged company's access to and use of customer data. While the ICA considered the data privacy policies of the merging companies, privacy laws and privacy-related sectoral regulation, the ICA could not rely solely on such policies or behavioral remedies to address data-related competition concerns.

In conclusion, while data portability can benefit both competition and privacy interests in many instances, there may be some tensions between them, requiring careful analysis of where they may diverge, especially in mergers where the merged company's data advantages could potentially harm competition.

Italy

In prioritizing its efforts in promoting a competitive environment in the digital economy, the Italian Competition Authority (hereafter the Authority or the AGCM) faces a complex challenge in navigating the intersection of competition and data protection laws. By adopting a multidisciplinary perspective, the AGCM has been a pioneer in exploring the various dimensions of consumer data and its implications for competition, consumer protection, and data protection as demonstrated in a 2020 study jointly conducted with the Communication Regulator and the Data Protection Authority.

The AGCM's experience has shown a significant complementarity between competition and data protection policies. In practice, the AGCM has noted that anti-competitive behaviours may emerge through actions that compromise the right to data portability. For example, in the AGCM's case against Google, it was observed that a dominant firm might restrict users' ability to trade and monetize their personal data via intermediaries.

With its dual competencies, the AGCM has also enforced consumer protection laws to enhance both privacy and competition measures, aiming to rectify the misalignment of incentives between market operators and users. AGCM's enforcement practices have addressed deceptive business conduct, such as misleading claims about the cost-free nature of services or inadequate disclosure of how user data is shared with third parties.

A court judgement in January 2024 required the AGCM to collaborate with the Italian Data Protection Authority when investigations involve significant data protection concerns. This judgment refers to the European Court of Justice's preliminary ruling on Meta and applies it to consumer protection cases, thus underscoring the increasing recognition of the interconnectedness of these legal domains.

Kazakhstan

The contribution discusses the challenges and opportunities presented by the digital economy, particularly focusing on competition and data privacy concerns. It emphasizes the importance of balanced regulation to support competition while safeguarding personal data.

Furthermore, it outlines initiatives proposed by the Antimonopoly Agency in Kazakhstan to strengthen regulation in the digital market. These include the development of a model public contract to enhance transparency in digital platform services, mandatory registration of platform operators in Kazakhstan, and restrictions on the use of data to prevent anti-competitive practices.

These measures aim to create a fairer and safer digital economy, protecting consumer rights and fostering fair competition while ensuring transparency and security for all participants.

Mexico

In this contribution, the IFT examines the intersection between competition and data privacy policies, highlighting the collaborative actions conducted with the National Institute for Transparency, Access to Information, and Personal Data Protection (INAI) to promote and protect competition and privacy. The IFT outlines key considerations on the interaction of these policies, the applicable legal and institutional frameworks, and the IFT's experiences.

The IFT underscores that both competition and data privacy policies aim to safeguard users from actions by undertakings that could harm their welfare. The IFT identifies and analyses complementarities and tensions between these policies, given that data is a critical asset, and its extensive collection can affect both privacy rights and market power dynamics.

Through the cooperation of Mexico's privacy and competition authorities, unintended consequences of enforcement might be avoided. To this end, the IFT and INAI signed a Memorandum of Understanding in 2021 which facilitates joint actions to promote transparency, access to information, data protection, and competitive markets, as well as regulation, and the promotion of trust and the responsible and safe use of telecommunications, information technologies and digital services.

The IFT provides examples of advocacy efforts, guidelines, microsites, market studies and judicial rulings, emphasizing the importance to understand competitive dynamics and the impacts of data collection to address challenges at the intersection of competition and data privacy in digital markets.

United Kingdom

The Competition and Markets Authority (CMA) is the UK's competition and consumer protection authority. The Information Commissioner's Office (ICO) is the UK's independent regulator for information rights (including data protection). This joint submission sets out our approach and experience of addressing issues at the intersection of our regimes, and how we continue to closely collaborate to promote market outcomes which support strong and open competition and innovation and respect data subject rights.

The Digital Regulation Cooperation Forum (DRCF) brings together four UK regulators, the CMA, the Office of Communications (Ofcom), the ICO and the Financial Conduct Authority (FCA) to deliver a coherent approach to digital regulation for the benefit of people and businesses online. It is a voluntary cooperation forum that facilitates engagement between the member regulators on digital policy areas of overlap and mutual interest. The key goals of the DRCF are to ensure digital regulation is co-ordinated between our member regulators so we can serve citizens and consumers better, reduce regulatory burdens for industry where appropriate, and enhance the global impact of the UK.

In this submission, we explain the CMA and ICO's joint statement issued in 2021 that sets out our shared views on the relationship between competition and data protection in the digital economy. We also summarise several examples where the CMA and ICO have worked and continue to work closely together, including the Google Privacy Sandbox case, our joint position paper on harmful design in digital markets and our joint statement on Foundation Models. Finally, we summarise some planned changes to the UK regulatory landscape which will affect the CMA and ICO and how we work.

United States

Digitization of the economy has produced important innovations and conveniences. At the same time, it has also created incentives for businesses to engage in constant surveillance of consumers, including, among many other things, tracking their page views, app activity, screen taps, mouse hovers, and geolocation—even their footsteps within retail stores—and then either selling the data or using it for their own purposes. Often, consumers are unaware that firms are collecting, selling, and otherwise exploiting these types of data. These mass surveillance practices can not only violate consumers' privacy, but they can harm competition too. Firms may use personal data to attain or entrench market power, exploit their market power by extracting excessive personal data, or extract data to raise entry barriers or compete unfairly.

Addressing these privacy and competition concerns does not involve choosing between more privacy and less competition, on one hand, or less privacy and more competition, on the other. Instead, the frameworks of fostering both privacy and competition can be aligned, where competition concerns are addressed once a foundation of baseline privacy protections is established through enforcement and/or legislation. Under such an approach, the goal is to identify a regime that facilitates entry through access to data while, at the same time, reducing the risk that incumbents act as gatekeepers, controlling access to key data needed for entry or expansion.

It can be challenging to address the significant privacy harms resulting from business models relying on extracting data from users. The notice-and-consent framework that has been popular with businesses fails to provide adequate privacy protections for consumers, especially as businesses are quietly changing their policies using dark patterns and dense legal jargon. Additionally, enforcement actions involving a few firms may fail to deter others while the rewards from mass data collection remain high. Despite these challenges, the FTC will continue to use its authority, tools, and experience to disrupt the incentives fueling mass surveillance as well as the illegal actions themselves. The FTC's recent enforcement efforts highlight the importance of three substantive privacy principles that support fair competition in the face of mass data collection, including data minimization, restrictions on data use, and prohibitions on sharing sensitive data. In addition to enforcement, the FTC is also undertaking other initiatives that could provide the foundation for establishing substantive privacy protections on a much broader scale. By reducing businesses' incentives to engage in excessive data collection, protecting consumer privacy could spur competition and the development of new business models that do not rely on invading users' privacy.