Organisation for Economic Co-operation and Development

DAF/COMP/WD(2024)26

Unclassified

English - Or. English

23 May 2024

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

The intersection between competition and data privacy – Note by Mexico

13 June 2024

This document reproduces a written contribution from Mexico 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

JT03544272

Mexico (IFT)

1. Introduction

1. The collection and processing of data, including user's personal and sensible data, has become increasingly important for competition dynamics in digital markets. As data can serve several purposes at different stages of the value chain of digital services, digital service providers have incentives to engage in activities to collect as much user's data as possible, however these could have detrimental effects on user's privacy and could even constitute a source of market power. Consequently, through the coordination and the collaboration between competition and privacy authorities, they can ensure that the application and enforcement of their respective policy realms does support and do not interfere with each other.

2. In this regard, the IFT and the National Institute for Transparency, Access to Information and Personal Data Protection (INAI, by its Spanish acronym), the privacy regulator, have established collaborative actions.

3. In this contribution, the IFT presents: (i) considerations of the intersection and interplay between data privacy and competition policies and enforcement; (ii) IFT's and INAI's applicable legal and institutional framework; and (iii) IFT's experience on the intersection between competition and data privacy policy.

2. General considerations in the intersection between privacy and competition policy

2.1. The extent to which the goals of competition and privacy policy and enforcement align

4. In general, competition and privacy protection policies share a common goal: to protect users from undertakings' actions or conducts that have or may have detrimental effects on their welfare.

5. In digital markets, the interplay between these two policies is closer since data[1] is one of the most important intangible assets for the provision of digital services. From a privacy policy perspective, the massive collection and processing of data could interfere with the adequate enforcement and protection of privacy rights. From a competition policy perspective, the massive collection of data could contribute to create, enhance or sustain market power of certain digital service providers.

6. Consequently, through the coordination and the collaboration between competition and privacy authorities, they can ensure that the application of policies in their respective realms does not interfere with each other. For example, by implementing certain competition policies, no unintended consequences to privacy protection may arise, or vice versa. Also, coordination and collaboration can promote that these authorities share their expertise and information to improve their respective duties.

[1] For the purposes of this document, 'data' is the term used for any type of users' data collected by digital service providers, that could include personal data and sensible data. It is worth noting that definitions of data, personal data and personal sensitive data, may vary across jurisdictions. For example, see: Bloomberg Law (2023). *Comparing U.S. State Data Privacy Laws vs. the EU's GDPR*. Retrieved from: https://pro.bloomberglaw.com/insights/privacy/privacy-laws-us-vs-eu-gdpr/.

2.2. Complementarities and tensions between competition and data privacy policies

2.2.1. Complementarities:

- Biggest digital service providers: when evaluating privacy and competitive behaviours, both authorities benefit from considering the size of digital service providers, the type and use of data collected, data transfer practices, data processing capabilities, and incentives to limit data access. Some digital service providers possess extensive user tracking capabilities, which can confer competitive advantages. Additionally, providers may have incentives to collect excessive data and engage in anticompetitive practices. Sharing information on provider size and commercial activities can enhance regulatory effectiveness.

- Control of detrimental conducts to privacy: online digital service providers often fail to accurately disclose: (i) data shared with affiliates and subsidiaries, [2] (ii) collected data and its processing methods,[3] and (iii) user interface manipulation, like Dark Patterns.[4] Limited opt-out options may worsen in monopolistic environments. Enhanced competition can improve privacy controls, with dominant players pressured to enhance privacy options. Stronger data privacy enforcement builds trust by empowering data owners.

- Control of detrimental conducts to competition: digital service providers with market power may abuse their dominance by: (i) imposing exclusive data access, creating barriers and increasing switching costs; (ii) pursuing mergers for data value, enhancing comparative advantage; (iii) refusing data access to maintain dominance, distorting competition.[5] Hence, considering privacy effects (i.e. collecting, processing and using data), on competition analysis and enforcement actions, would improve competition in digital markets and would foster leveling the playing field between participants. Also, improving privacy controls incentivizes firms to compete on privacy and innovate in data protection technologies. (e.g. privacy enhancing technologies[6]).[7]

2.2.2. Tensions:

- Competition: imposing of unnecessary privacy regulatory burdens on new players, or to those with lower user reach, may lead to negative outcomes in respect of competition, i.e. by unduly favoring large, integrated platforms over smaller, non-integrated suppliers.

[2] For example, the United Kingdom has established regulation on when does data sharing is considered unlawful, some examples are provided in the following link. ICO (2023). *Data sharing – when is it unlawful?* Retrieved from: https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-sharing-when-is-it-unlawful/.

[3] Relias Media (2020). *Combining Large Data Sets Challenges IRBs, Researchers to Ensure Privacy*. Retrieved from: https://www.reliasmedia.com/articles/146763-combining-large-data-sets-challenges-irbs-researchers-to-ensure-privacy.

[4] Waldman, AE. (2020). "Cognitive biases, dark patterns, and the 'privacy paradox'". *Current Opinion in Psychology*, Vol. 31:105-109. Retrieved from: https://doi.org/10.1016/j.copsyc.2019.08.025.

[5] APEC-IFT and COFECE (2024). *Policies and Tools for Improving Digital Economy and Competition in Digital Markets: Current Issues*. Retrieved from: https://www.apec.org/publications/2024/03/policies-and-tools-for-improving-digital-economy-and-competition-in-digital-markets-current-issues

[6] OECD (2023). *Emerging privacy-enhancing technologies: current regulatory and policy approaches*. Retrieved from: https://www.oecd-ilibrary.org/docserver/bf121be4-en.pdf?expires=1712771083&id=id&accname=oid048326&checksum=D9E5A1C88B8E46D82322BCC0A01EEE98.

[7] Ohlhausen, M. K. and Okuliar, A. (2015) "Competition, Consumer Protection, and the Right (Approach) to Privacy", pp. 134-136. *Antitrust Law Journal*, No. 1. Retrieved from: https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf.

- Privacy: (i) imposing data portability rules could have a negative impact on privacy, whenever data access between undertakings is not limited to what is necessary and proportionate, and it could not have the expected benefits if dominant firms can reduce compatibility and interpretability of this data; and (ii) ex-ante *data sharing* may hamper privacy if they are not implemented in a data protection-compliant way or they can diminish firms' incentives to invest into the collection and curation of data in the first place.

7. In order to solve potential tensions, both authorities need to collaborate and establish institutional mechanisms for working together; this could be done on a case-by-case basis or through a general framework of collaboration. This is the case of the IFT and the INAI, who signed a Memorandum of Understanding (MoU) to undertake collaborative actions. (See paragraph 18).

3. Mexican legal and institutional framework

8. In Mexico, the access to broadcast and telecommunication services, including broadband and the Internet services is a constitutional right and these shall be provided through effective competition (article 6). Also, the Mexican Constitution establishes that every person has the right to the protection of their personal data, to access, rectify and cancel it, as well as to oppose to its processing (article 16).

9. The IFT is the national competition authority for the telecommunication and broadcasting sectors. Hence, the IFT enforces the Federal Economic Competition Law[8] (LFCE, for its Spanish acronym) in those sectors. Regarding confidential, reserved and personal data, laws include specific provisions:

> *LFCE, Confidential information[9] and Reserved information[10]: the IFT shall safeguard at all moments, the secrecy of the investigations and procedures, including Confidential Information and Reserved Information. Under no circumstances the IFT can be compelled to provide Confidential Information, nor may it publish said information, and the IFT shall take the necessary measures for said information's safeguarding (LFCE, article 125).*

10. Regarding data privacy policy, the INAI is the regulator and enforcer of Personal data protection laws. Accordingly, the IFT shall comply with the provisions established in the General Law for the Protection of Personal Data in the Possession of Obliged Subjects —Federal, State or local authorities— (LGPDPSO, by its Spanish acronym), whilst telecommunication providers shall comply with[11] the General Law for the Protection of Personal Data held by Private Parties (private entities) (LGPDP, by its Spanish acronym).

[8] The LFCE forbids any monopolies, monopolistic practices, unlawful concentrations and barriers to entry whenever they diminish, damage, prevent or condition market access or economic competition in the production, processing, distribution or marketing of goods or services (article 52). Also, LFCE establishes a general framework of conducts that are considered unlawful, such as: relative monopolistic practices (articles 54, 55 and 56); entry barriers (article 57); and unlawful mergers (articles 64).

[9] As defined by law, any information which disclosure may potentially damage the competitive position of the Economic Agent who provided it, which contains personal data the disclosure of which requires the Economic Agent's consent, may endanger its security or when its disclosure is legally prohibited.

[10] As defined by law, information which may only be accessed by the Economic Agents with legal standing in a particular procedure.

[11] There are other laws such as: the Criminal Code; the Law for the Regulation of Credit Information Companies; the Law for Regulating Financing Technology Institutions; provisions set forth in the Copyright Law and the Federal Law for Consumer Protection; and some specific provisions set forth in the Civil Code and the Commerce Code, which regulate specific activities of data protection.

Each law establishes obligations for the data holders of Personal data[12] and Sensible personal data[13] and the rights of data owners.

11. LGPDP establishes:

> *Data Owners have the right to: have Access their personal data, request the Rectification of inaccurate data, request the Cancellation of their personal data, and to Object the processing of their data (Access, Rectification, Cancellation or Objection: ARCO, by its Spanish acronym) (articles 22, 23, 24, 25 and 27), the procedure to be informed of the privacy notice (article 23).*
>
> *Private data controllers are mandated to: collect and process Personal data in a lawful manner, and cannot obtained it through deceptive or fraudulent means (article 7); obtain consent from the data owners for all the Processing[14] of their personal data (article 8) and for sensitive personal data they must obtain express written consent (article 9), however they do not have to obtain consent for Processing Personal data when it has been subject to a prior dissociation procedure[15] (article 10); through a Privacy Notice[16] they must inform data owners what information is collected from them and why (article 15); limit the Processing of personal data to the fulfilment of the purposes set out in the Privacy Notice (article 12); cancel any personal data when is no longer necessary for the fulfilment of the objectives set forth in the Privacy Notice (article 11); perform the data Processing as agreed in the Privacy Notice, and Privacy Notice shall contain a clause stating whether or not the data owner agrees to the transfer her/his data to third parties (article 36); inform data owners how they can exercise their ARCO rights and designate a department who will process requests from for the exercise of the ARCO rights (article 30). Regarding data transfers (national or international), data controllers may be exempted to notify the data owners in several cases, for example whenever it is between holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies (article 37, paragraph III).*

12. LGPDPSO, among others, establishes that the State will guarantee the privacy of individuals (article 6), and that Public data controllers shall only process personal data when it is justified by specific, lawful, explicit and legitimate purposes, and cannot obtain Personal Data through deceptive or fraudulent means (article 19); inform data owners what is the information collected from them and why, through the Privacy Notice (article 26).

13. Regarding public access to information, the IFT is required, among others, by General Law for Transparency and Access to Public Information (LGTAPI) to: guarantee effective access to public information (article 1); classify information (article 100) as

[12] Personal data is defined as any information concerning an identified or identifiable individual.

[13] Sensitive personal data, defined as personal data touching on the most private areas of the data owner's life, or whose misuse might lead to discrimination or involve a serious risk for said data owner. In particular, sensitive data is considered that which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, sexual preference.

[14] As defined by the LGPDP, the term "processing" includes the following activities: retrieval, use, disclosure or storage of personal data by any means. Use covers any action of access, management, exploitation, transfer or disposal of personal data.

[15] Procedure through which personal data cannot be associated with the data owner nor allow, by way of its structure, content or degree of disaggregation, identification thereof.

[16] Document in physical, electronic or any other format, generated by the data controller, that is made available to the data owner prior to the processing of his personal data. It must include: The identity and domicile of the data controller collecting the data; the purposes of the data processing; the means for exercising rights of ARCO rights; the data transfers to be made; the options and means offered by the data controller to the data owners to limit the use or disclosure of data, among others (article 16).

Public, Reserved (articles 113-115) or Confidential (articles 116-120); guarantee accessibility measures and conditions so that every person can exercise the right of access to information, through requests for information (art. 121).

14. In their respective laws, it is established that INAI and IFT shall collaborate for the fulfilling of their respective duties. In particular, the IFT has the legal duty to collaborate with public authorities and to issue non-binding opinions to promote the observance of free market access and economic competition principles in their administrative acts.

4. IFT-Mexico's experience

15. The IFT is aware of the importance of data for digital markets competition dynamics, and also the harms that its massive collection can have to the enforcement of privacy rights and competition dynamics.

16. To foster synergies, the IFT's and INAI's institutional frameworks, respectively, include the sufficient provisions to cooperate and collaborate. In 2021, a Memorandum of Understanding (MoU) was signed to undertake collaborative actions.[17] The main objective of the MoU is to enhance the coordination and collaboration to carry out programs, events, works or projects, with the purpose of promoting, among others, transparency, access to information, protection of personal data, and competition; as well as the regulation and promotion of trust and the responsible and safe use of telecommunications, information technologies and digital services. The actions considered for collaboration and coordination, among others, include sharing statistical information and experiences on specific topics, design and development of research projects, as well as promoting the dissemination of information related to the objective of the MoU.

17. In this regard, the following actions have been performed to promote competition and privacy:

18. **Advocacy efforts to promote privacy rights**: the most important actions include advocacy efforts to promote data owners ARCO rights (privacy rights), such as Guidelines on the Protection of Personal Data for elderly population[18] and actions to foster the protection of Personal Data, for which the IFT developed a microsite[19] that presents the Privacy Notices of main digital platforms providers. Also, the IFT developed a microsite where users can access the IFT's Privacy Notices for different administrative, competition and regulatory procedures.[20]

19. **Understanding the intersection of competition and privacy in digital markets:** the IFT acknowledges the critical importance of data in the competitive dynamics of digital markets. Through the Economic Competition Unit (UCE by its Spanish acronym), the IFT has conducted various market studies addressing the evolution of competition in Mexican digital markets. These studies provide essential information about key market players, relevant providers, essential inputs, and entry barriers, enabling the identification of potential anticompetitive behaviours and assessing the challenges facing competition in this environment. For example, the studies have highlighted the involvement of

[17] Retrieved from: https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/acuerdan-inai-e-ift-acciones-conjuntas-para-promover-una-cultura-de-proteccion-de-datos-personales-y.

[18] Retrieved from: https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-ift-y-el-inai-presentan-el-decalogo-de-proteccion-de-datos-personales-para-personas-adultas.

[19] IFT (2024). *Herramienta Interactiva de Políticas, Términos y Condiciones Aplicables en el Uso de Plataformas Digitales*. Retrieved from: https://plataformasdigitales.ift.org.mx/public/categoria/2/plataformass-de-transporte.

[20] Retrieved from: https://www.ift.org.mx/proteccion_de_datos_personales/avisos_de_privacidad.

telecommunications and broadcasting service providers in the digital advertising market, thus underscoring the fundamental role of data collection in this context. Furthermore, the IFT is fully aware of the potential risks posed by massive data collection for privacy protection and competition in digital markets. Companies' ability to share and use collected data can grant them power and generate incentives to engage in behaviours that could distort competition. Understanding how data collection can influence both competition and privacy protection in these digital environments is crucial.

20. In this regard, the IFT's efforts to understand competitive dynamics and the impacts of data collection are vital for addressing challenges at the intersection of competition and privacy in digital markets. Understanding the dynamics among telecommunications service providers, such as América Móvil (the holding company of leading telecommunications service providers), and Grupo Televisa (designated as the Preponderant Economic Agent in Broadcasting), is fundamental for the IFT. These entities not only offer telecommunications and broadcasting services but also venture into the digital realm as OTT service providers and digital advertisers. For instance, América Móvil actively engages in digital advertising by providing data analytics, user profiling services, and digital advertising spaces through its OTT platforms and mobile ads targeted at Telcel users. Similarly, Grupo Televisa offers OTT services and digital advertising, including digital ad spaces and user profiling services.

21. By comprehending how these companies operate and participate in the digital ecosystem, the IFT can more effectively address the challenges and opportunities arising in this domain. This, in turn, contributes to fostering a competitive and equitable environment for all market stakeholders.

22. **Data portability and interoperability**: Currently, the only data subject to portability is considered in the Federal Telecommunications and Broadcasting Law (LFTR, by its Spanish acronym), and it refers to users' telephone number portability (articles 118, 174, 191). Up to date, the IFT is not aware that are any proposals to amend in any law regarding matters of data portability or interoperability in Mexico. Finally, there have been cases where parties involved in an investigation followed under a trial-like procedure (significant market power investigations) have claimed that the IFT limited their right to legitimate defence,[21] since the IFT did not provided access to Confidential Information from third parties. In this regard, whilst LGTAPI article 1 establishes that access of information shall be guaranteed, LFCE article 125 establishes that under no circumstances the IFT can be compelled to provide Confidential Information.[22] The judicial ruling, agreed with the IFT's classification of Confidential information, and asserted that the IFT acted in accordance to article 125 stating that "only specific and precise information was a matter of protection, the disclosure of which may cause disproportionate or unnecessary harm to its owners."[23]

[21] In particular, the Party injuncting IFT's decision claimed that, by not providing confidential information from third parties, the IFT was in violation of articles 120, fraction IV, from LGTAPI, and article 37, fractions V and VI, of LGPDPSO.

[22] See for example IFT's Board Decisions on Megacable and GTV, substantial market power in pay-tv services. Available at: https://www.ift.org.mx/sites/default/files/version_publica_resolucion_ai-dc-002-2019.pdf and https://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/piftext29112136vp.pdf.

[23] Second Tribunal on matters of economic competition, broadcasting and telecommunications, ruling on indirect injunction case 6/2021, p.26.