MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE
Liberté
Égalité
Fraternité

Tresor-Economics

No. 310 • July 2022

Direction générale du Trésor

Privacy Protection and Competition in the Digital World

Mélanie Thoinet and Léa Dardelet

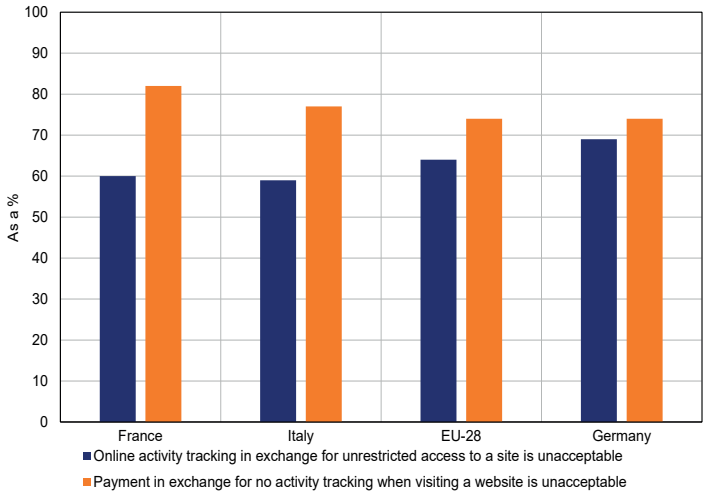
- In the digital realm, privacy protection is closely linked to the concept of personal data. Privacy protection can be defined as the control of data relating to each citizen that other stakeholders have access to.

- The digital economy has given rise to cross-cutting, complex and ambivalent impacts between privacy protection and competition, blurring the lines between these two, historically distinct policies. Safeguarding competition may result in a restriction of the personal data collected by a platform or in authorisations granted to competitors to access data owned by other companies, bolstering or weakening privacy protection. Similarly, more stringent privacy protection may increase competition by restricting data accumulation, a potential factor for establishing a dominant position, or may reduce competition by generating compliance costs that have a relatively greater impact on small companies.

- The European Union and national authorities are striving for improved coordination between these two policies. The Digital Markets Act and the Data Governance Act address these issues at European level. The competition authorities are also attaching greater importance to personal data-related issues: in the name of privacy protection, several national authorities have launched investigations into the practices of platforms to ascertain whether they constitute anti-competitive conduct. To address these issues, various regulators are increasingly cooperating with each other.

- If consumers were more aware of the value of their data, the goals of competition and privacy policies would be less conflicting. Today a "privacy paradox" is apparent: while Internet users are concerned about protecting their privacy on the Web, they still freely give out their data to companies, notably because they unable to determine its value. A 2016 European Commission survey revealed that 64% of Europeans questioned believed that tracking user activity online in exchange for free access to a website was unacceptable, even though 74% of them would not be willing to pay in order not to be monitored (see chart). Thus, while Europeans are mainly concerned about their online activity being tracked, very few would be happy to pay to visit web pages.

Online privacy preferences of Europeans



Source: European Commission, Flash Eurobarometer 443 – e-Privacy, 2016.

1. The digital economy is changing the dynamic between privacy protection and competition[1]

1.1 For a long time privacy protection and competition were addressed separately

Traditionally, privacy protection and competition policies have had diverging approaches to the collection, use and protection of personal data, meaning "any information relating to an identified or identifiable natural person".[2] While the right to privacy is enshrined in the French Civil Code,[3] the separate treatment of the two policy types was not immediately scrutinised with the emergence of digital technology.[4]

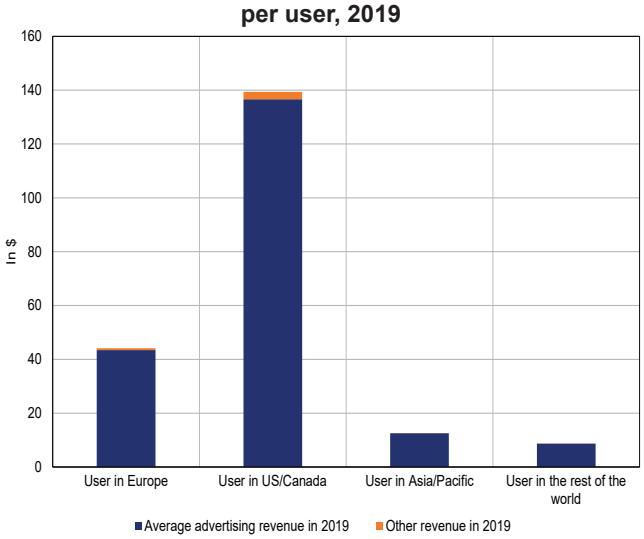
Competition law initially adopted an "optimistic" approach to the digital economy. This approach was based on the premise that the extensive use of users' personal data and/or user privacy protection guaranteed by platforms could improve competition on the markets: these factors would form an element of service and product quality that could give competitors an edge over others. One example could be a route planner service which collects an increasing amount of data to continuously improve its routes to gain an advantage over its competition. Likewise, services with varying privacy levels could let users decide whether they would give away their data to use the service, thereby bringing in a competitive element since the platform would be required to provide a high-quality service or else lose the user to another provider. On this basis, if a company continues to provide its product free of charge so long as a greater volume of personal data is used or this data is sold to other companies, the resulting reduced privacy protection is akin to a price hike or a reduction in the product's quality (since privacy is a hidden cost of using platforms).

At the same time, privacy policies have continued to cautiously address data usage, underscoring the risks of any data collection, with no consideration made for its economic impacts on competition in particular.[5]

1.2 As platforms have developed, the cross-cutting and ambivalent impacts spanning the two policies have become apparent

Many digital players such as Google and Facebook provide seemingly free services to users. Their business model is based on collecting and using the data provided by customers (e.g. profile information), including indirectly collected data (e.g. cookies). This data allows platforms to have a greater insight into their users' preferences and thereby provide targeted advertising to them. This represents a source of revenue, as platforms can sell advertising space of a greater value. Although difficult to estimate, the value of personal data can be approximated with the "advertising revenue per user" indicator. In 2019, Facebook earned around $29 in advertising revenue for each global user, $137 for each North American user, $13 for each Asian user and $43 for each European user (see chart 1).

Chart 1: Facebook's average advertising revenue per user, 2019



Source: Facebook Q4 2019 Results.

(1) These issues were the subject of a seminar at the DGT on 14 October 2021 (Nasse Seminar), which was recorded and posted online: https://www.tresor.economie.gouv.fr/Evenements/2021/10/14/protection-de-la-vie-privee-et-concurrence (*in French only*)
(2) CNIL (French Data Protection Authority).
(3) Article 9 of the Civil Code.
(4) C. Caffarra, G. Crawford & J. Ryan (2021), "The antitrust orthodoxy is blind to real data harms", VoxEU; L. Liguori (2021), "Data Privacy and Competition Protection in Europe: Convergence or Conflict?", CPI.
(5) The CNIL objectives have from the outset made no reference to economic considerations.

The idea that the consumer's freedom of choice and privacy protection are stand-out factors for platforms however has its limitations. Users are often unable to grasp the value of the data they give out, given the complexity of how it is collected.[6] This information asymmetry therefore undermines the users' informed choice and feeds into the "privacy paradox": although users are concerned about their online privacy, they freely give out their data to various companies. In this respect, according to the European Commission, while 64% of Europeans polled in 2016 believed that tracking user activity online in exchange for free access to a website was unacceptable, the majority of them would not be willing to pay in order not to be monitored (see chart on page 1). A pattern emerges from these preferences: the countries where consumers are more willing to be tracked in exchange for a free service (e.g. France and Italy) are also those which are less willing to pay in order not to be monitored.

Lacking reliable information on data use, and with few alternatives to the services offered by the platforms, users struggle to switch to different service providers, particularly for a less data-intensive company, due to the impact of direct networks.[7] Lastly, dark patterns[8] also compromise personal data protection.

In addition, due to the characteristics of the digital markets (direct and indirect networks effects),[9] data control could be a source of market power and result in anti-competitive conduct. The most appealing networks generate the majority of advertising revenue from data use, and they can maintain this appeal by optimising their services through investment and innovation. Another potential strategy is to acquire other companies to collect even more data. This encourages monopolistic positions against small companies,[10] which can be problematic when this leads to abuse of a dominant market position.[11]

Box 1: Case study of Google and Australia

The Australian Competition and Consumer Commission (ACCC) stated in its August 2021 report[a] that Google had engaged in anti-competitive conduct to hold onto its dominant position, for example by restricting the sale of its advertising spaces on YouTube to its own bidding platform.

The ACCC also shed light on friction between the transmission of data to advertisers and the legal constraints of privacy protection. In the ACCC's view, Google had allegedly justified several updates, with potentially negative impacts on competition on the advertising market, as data protection measures. This is thought to be the case for its Privacy Sandbox initiative: by disabling third-party cookies, the information collected could no longer leave Google's browser (Chrome), preventing other companies from collecting it directly via Chrome. As well as controlling the entire value chain, Google is therefore allegedly the only provider of data on Chrome users. In a similar vein, Google recently announced the launch of Topics, the tool that targets users by topic based on the sites they have visited. Google will transmit only three of these topics – chosen at random on a weekly basis – to companies requesting the information for their advertising.[b] This Privacy Sandbox is still the subject of ongoing discussions between various national competition authorities. In 2021, investigations were launched by the European Commission and the British Competition and Markets Authority to determine the impact of the Privacy Sandbox on competition and potential anti-competitive conduct on the part of Google.

a. Digital Advertising Services Inquiry – Final Report.
b. PEReN (2022), Éclairage sur Privacy Sandbox (*in French only*).

(6) Furman et al. (2019), "Unlocking Digital Competition" report.
(7) A platform is more appealing to a user if it has other users.
(8) For example, an allow button that is more visible than the reject one, or pre-selected options when making online purchases.
(9) A platform's appeal depends on the user on one hand and the users already on the platform on the other.
(10) The French Competition Authority and the Bundeskartellamnt, the German competition authority ("Competition law and data" report, 2016), stress that when large companies have a very broad information database, it can be difficult for other companies to match the same data volumes and variety.
(11) Analysing these situations from a competition perspective may be more difficult in that an increase in a platform's revenue may be achieved through the provision of new or improved services.

A competition policy may therefore bolster[12] privacy if it curbs the concentration of personal data in the hands of a small number of large platforms that could use it for intrusive purposes and thereby compromise consumer well-being.[13] Upholding competition on the markets can sometimes foster innovation, resulting in improved personal data protection. However, a competition policy could also undermine this protection if under its terms platforms are not required to restrict the access of competitors to data, so that new companies – they themselves respecting the privacy of individuals to a varying degree – can enter the markets.

Likewise, a privacy protection policy can help to prevent the creation of dominant positions since it can either prohibit the use of data which would provide a competitive advantage or act as a tool for companies to make their products stand out (based on the degree of privacy guaranteed), thereby stimulating competition. However, it can also expand the dominant positions of some companies when the rules protecting personal data give competitors less of a chance to innovate based on the data they hold – and in turn to stimulate competition through disruptive innovation – or when these rules increase costs (e.g. compliance costs) to a prohibitive degree for small competitors. This dual nature can be observed in the General Data Protection Regulation (GDPR): the regulation is said to on the one hand have anti-competitive repercussions, bolstering the dominant position of major platforms due to compliance costs acting as barriers to entry for competitors,[14] and on the other impacts conducive to competition with the data portability requirement, which cuts costs for consumers changing their provider and gives them greater control over their data.

1.3 Discussions are under way for a regulation that best strikes the balance between competition and privacy protection

Unless public authorities take action, it seems that the workings of digital markets do not allow for a satisfactory balance between competition and privacy protection. Some search engines stress that privacy protection constitutes a comparative advantage, but this only applies in limited cases. In addition, this non-price factor does not seem to be appealing enough to substantially change the business models, which are based on data use and advertising. Consequently, regulation seems necessary in order to introduce a framework allowing competitors to freely enter digital markets without compromising innovation or privacy. The issue is of particular concern to the European Union, which champions a business and social model based on individual rights and personal data protection.

Regulations have been adopted to step up digital platform regulation. At European level, the Digital Markets Act (DMA), approved in March 2022, seeks to safeguard competition on digital markets while factoring in privacy protection issues. For example, combining personal data for targeted advertising, deemed a source of “potential advantages [...], lifting the barriers to entry”, will be subject to the user’s consent. The Data Governance Act, approved in November 2021, aims to step up data sharing while increasing trust in data intermediaries with a protection framework (e.g. the reuse of personal data is regulated). In the United Kingdom, the 2019 National Data Strategy led to the British government’s proposal for data protection arrangements that support innovation and competition and foster economic growth, all the while guaranteeing data protection.

(12) M. Manant, A. Rallet and F. Rochelandet (2018), “Privacy et antitrust: des régulations contradictoires ou complémentaires ?”, *Revue Économique* (vol. 69).
(13) Combining personal data could give a monopolistic company the means to target consumers and differentiate between them (e.g. based on price, particularly in healthcare, personal finances or employment). Monopoly situations worsen the negative impacts, as consumers are given no other choice (e.g. such impacts cannot be mitigated precisely because of a lack of competition).
(14) M. Gal and O. Aviv (2020), “The Competitive Effects of the GDPR”, *Journal of Competition Law and Economics*.

Striking the balance between privacy protection and competition also depends on the preferences of platform users. With that said, users themselves struggle to identify these preferences as the privacy paradox illustrates. In light of this, some have pushed for a system to reveal these preferences through data monetisation: for example, rather than continuing with the format of payments in the form of users' personal data in exchange for targeted advertising, as is implicitly the case these days, data monetisation could take the form of monetary sums paid by users to opt out of advertising, offsetting the platform's loss in advertising revenue. Supporters of the latter believe that monetisation would raise user awareness about the value of personal data and compel users to adjust their practices based on their privacy protection preferences. This method would also promote competition, with companies that best meet these preferences acquiring market shares, while ensuring possibilities for abuse of a dominant position are limited. Users, in choosing which data they provide access to for each platform, may pay relatively substantial sums to competitors of major platforms. The proprietary approach, which consists of each user owning a "personal data wallet" to freely manage with the platforms, is still far off and uncertain, and could face conceptual challenges.[15] It would redefine the meaning of personal data, which is currently considered a fundamental right in Europe (it is inalienable, in the same way as an individual's body). It may therefore not be legally possible to establish such a right of ownership.[16]

2. The practices of national and supranational regulatory authorities are changing in line with these theoretical considerations

2.1 Initially, the various regulatory authorities worked independently

For a long time, privacy protection authorities dealt with personal data with a view to preventing any privacy risks (e.g. the French Data Protection Act of 1978). In this respect, in France, the French Data Protection Authority (CNIL) considers that only specific identified parties should be able to use personal data.

However, when it came to competition policy (e.g. control of concentrations), use of personal data was either considered from the perspective of sharing between economic players (to prevent dominant positions from being established, which could result in a single entity controlling masses of data) or was completely overlooked. For example, in 2008, when the company DoubleClick was bought out by Google, the European Commission only considered the competition law aspects and not those affecting privacy protection (i.e. the impact of combining the data of the two companies).[17] Similarly, when WhatsApp was acquired by Facebook in 2014, the Commission separated the two issues (see Box 2).

Box 2: Facebook's acquisition of WhatsApp in 2014

In 2014, in relation to the Facebook/WhatsApp deal, the European Commission ruled that the privacy protection concerns did not fall within the scope of EU competition law.[a] This case appeared to raise few privacy protection concerns since WhatsApp used to scan address books but did not sell personal data to advertisers. Facebook also announced that it would not be able to automatically match its user accounts with WhatsApp accounts, which the Commission had taken into account when authorising the acquisition. However, in 2016, Facebook changed WhatsApp's privacy policy: WhatsApp data was now collected and used for targeted advertising across the group's applications. The Commission responded to this by fining Facebook €110 million for providing misleading information and a failure to ensure the independent and autonomous operation of WhatsApp and Facebook services. Facebook received an additional fine of €225 million in 2021 from the Irish Data Protection Commission on behalf of the European Commission, as it failed to provide sufficient information to WhatsApp users on the use of their personal data, as required by the GDPR adopted in 2016.

a. See point 164 of the Commission decision of October 2014.

(15) Génération Libre (2019), "Aux data, citoyens!" report.
(16) Winston Maxwell, Maxime Cordier (2018), "Le tabou de la propriété des données personnelles, éléments de la personnalité et objets de commerce", Edition Multimédi@ (*in French only*).
(17) Competition Policy Newsletter 2/2008. Drafted by staff who handled the case, this document does not reflect the Commission's official view.

2.2 Competition authorities now take a greater interest in the impacts of privacy protection

For a number of years, the European Commission has focused its interest on the cross-cutting impacts of competition and privacy protection policies. In 2015, a Commission publication on the Facebook/WhatsApp deal[18] also pointed out that data can help to make a competition-based assessment on mergers, constituting a means to achieving a competitive edge. This is because privacy protection can be regarded as a non-tariff competition factor (when products are given away for free to users because they are funded by targeted advertising, personal data is the "currency" used by users or an aspect of product "quality"). Such considerations were able to be taken into account in some decisions and investigations. These include the Microsoft/LinkedIn merger decision in 2016 (in which privacy protection was deemed a driver of customer choice and a competition factor)[19] and the investigations into the Amazon and Meta marketplaces in 2020 and 2021 (in which consideration is given to the possibility that data introduces entry barriers and is used in an uncompetitive manner).[20] The Commission takes an active interest in the practices revolving around privacy protection concerns, when they are likely to entail competition law infringements. The warning issued by Commissioner Margrethe Vestager in 2021 to Apple, concerning changes to its privacy rules (a change brought in by the iOS 14 update that sends users a pop-up message, asking them if their activity can be tracked) reflects this approach: while Apple claims that this change was made to protect personal data, Vestager stressed that this does not exempt the company from compliance with competition law.

At national level, several competition authorities are now addressing privacy protection issues. In Germany, the competition authority launched an investigation into Facebook in 2016 based on allegations of misuse of market power. The investigation sought to ascertain whether Facebook was abusing its dominant position to infringe data protection law and extend the conditions of use by setting the volume of data processed. In 2019, the competition authority implemented restrictions on Facebook's capacity to share data between its own platforms and third-party applications, on the grounds that collecting data without obtaining the consent of users and sharing it among its services constituted an abuse of a dominant position. Following legal developments in this case, the CJEU will be required to pass judgment on this matter, particularly on the jurisdiction of a national competition authority in respect of compliance with the GDPR by the company subject to an antitrust audit.

In 2020, the French Competition Authority received complaints from online advertising companies, who challenged the changes brought in by iOS 14, claiming that Apple was abusing its dominant position and could potentially make targeted advertising less effective. In March 2021, the authority did not consider the changes to constitute anti-competitive practices, and deemed them to be in line with Apple's privacy protection and business policy decisions, helping to protect user data. Nonetheless, it is continuing its investigation in order to determine whether Apple is unduly favouring its own services. In 2021, the non-profit France Digitale also lodged a complaint against iOS 14 with the CNIL, claiming in this instance that Apple has not respected the principle of user consent since the update enables targeted advertising by default for Apple applications.

(18) Competition merger brief 1/2015. Drafted by staff who handled the case, this document does not reflect the Commission's official view.
(19) Point 350 and footnote 330 of the Commission decision of 6 December 2016.
(20) Speech given by Margrethe Vestager at the European Data Protection Supervisor conference, "Data Protection and Competition: enforcement synergies and challenges", June 2022.

In September 2021, the Chair of the US Federal Trade Commission announced her intention to make personal data protection a priority for the institution in line with the application of antitrust laws. This is done in an effort to prevent any harm caused by surveillance practices and gaps in federal law on privacy.

2.3 Greater cooperation between authorities and national regulators

In France, the many cooperation initiatives between the Competition Authority and other institutions demonstrate the public authorities' determination to understand every facet of the digital economy. In 2019, the Competition Authority, the Financial Market Authority, the Transport Regulatory Authority, the Electronic Communications, Postal and Print Media Distribution Regulatory Authority, the CNIL, the Energy Regulation Commission and the Audiovisual Board published a joint statement on "New regulatory procedures - Data-driven regulation". The Apple case in 2020, which involved the French Competition Authority using a CNIL opinion, is one of the first examples of such cooperation. Since then, several other collaborations have developed: in 2020, the Directorate General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF) and the CNIL signed a cooperation agreement to harmonise consumer law with GDPR compliance more effectively; in May 2021, the Competition Authority and the Digital Regulation Expertise Unit (PEReN) signed an agreement under which the PEReN will be able to analyse data and provide technical expertise in investigations relating to digital platforms. In a recent speech,[21] the President of the French Competition Authority advocated "increased cooperation" between competition authorities and personal data protection authorities, in particular due to the ambivalent nature of interactions between competition analysis and personal data protection law.

In spring 2021, the British Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA) published a memorandum of understanding to formalise a closer working relationship between the two institutions. They had previously given consideration to their respective objectives in investigations (e.g. the joint investigation into the Privacy Sandbox in 2021). Each authority will now be able to send the other information obtained during its investigations provided that it is crucial to achieving the other authority's objectives.

Lastly, in 2021,[22] the national data protection and privacy authorities of the G7 countries stressed the need to step up collaboration amongst themselves and their national counterparts in competition, specifically in relation to digital market regulation. In June 2022,[23] Commissioner Vestager underscored the importance of collaboration between policy makers in the competition, data protection and consumer protection fields, highlighting that the institutional structure set forth in various EU legislation adopted or currently the subject of talks should enable such synergies to be identified.

(21) Speech given by Benoît Cœuré, President of the French Competition Authority, before the CNIL Commission, "Droit de la concurrence et protection des données personnelles", June 2022 (*in French only*).
(22) "Data Free Flow with Trust" – Roundtable of G7 data protection and privacy authorities.
(23) Speech given by Margrethe Vestager at the European Data Protection Supervisor conference, "Data Protection and Competition: enforcement synergies and challenges", June 2022.

Publisher:
Ministère de l'Économie,
des Finances
et de la Souveraineté
industrielle et numérique
Direction générale du Trésor
139, rue de Bercy
75575 Paris CEDEX 12

Publication manager:
Agnès Bénassy-Quéré

Editor in chief:
Jean-Luc Schneider
(01 44 87 18 51)
tresor-eco@dgtresor.gouv.fr

English translation:
Centre de traduction
des ministères économique
et financier

Layout:
Mimose Mellia
ISSN 1777-8050
eISSN 2417-9620

Recent Issues in English

https://www.tresor.economie.gouv.fr/Articles/tags/Tresor-Eco

Direction générale du Trésor

@DGTresor

To subscribe to *Trésor-Economics*: **bit.ly/Trésor-Economics**