ICN Steering Group Project – Competition law enforcement at the intersection between competition, consumer protection, and privacy

Task 1: Issues identification

Introduction

This paper identifies for competition agencies relevant issues at the intersection between competition, consumer protection and privacy ("intersection"). It is based on a review of academic literature and nearly a dozen agency responses[1]. The issues identified below consist of a structured list of descriptive and non-conclusive considerations that might arise at the intersection coupled with some open questions for further analysis, with the understanding that not all considerations may be appropriate in all jurisdictions due to the specific legal, legislative, regulatory or political regimes in which competition agencies operate.

In particular with the increased attention to the digital economy, competition agencies may be faced with business practices, including data practices, that raise also consumer protection and/or privacy concerns.

Competition, consumer, and privacy law and policy

Competition law and policy aim at ensuring that, through competitive markets, consumers have the widest possible range of choice of goods and services at the lowest possible prices. Competition law and policy aim at ensuring the functioning of the competitive market. Thus, competition law and policy undertake to prevent certain types of conduct that interfere with competition, notably restrictive agreements, especially cartels, harmful conduct by a monopolist or dominant firm and anticompetitive mergers.

Consumer law and policy aim at ensuring that consumers are able to exercise informed economic choices. Consumer policy may address, among other things, information asymmetry as between sellers and buyers, false and misleading advertising, and contract terms that are not understandable or disproportionate.

Privacy law and policy aim at ensuring personal data protection, defining when, how and to what

[1] This paper was prepared by the Italian Competition Authority with the contribution of the Bundeskartellamt, DG Competition, US DoJ and US FTC. An annex to this paper includes a bibliography of the reviewed literature. Some articles are cited in the paper for reference with the label "ref. [number of the article]".

extent information about a person is collected, processed and communicated by and between undertakings. Privacy legislation, where existing, tends to provide basic protections to consumers and data subjects, as well as affording rights to better control their data. In particular, most jurisdictions operate a consent-based regime (ref. 3 and 76), which provides consumers the ability to control how their data are collected and used by agreeing or withholding their consent. In addition, in some jurisdictions, data protection legislation confers other rights including the right to data portability (ref. 45 and 65).

Sometimes the different above-described regimes may complement each other, while in other circumstances tensions may arise. In some instances, competition agencies may be the best placed authority to tackle directly a specific data practice as an anti-competitive conduct, while in others they may rely on privacy and/or consumer protection authorities.

Consumer data and the data value chain

Concerns about consumer data tend to be at the center of issues related to the intersection. The focus on consumer data[2] practices is driven by many factors, including the increased use of data and computing power to offer ever more complex price menus,-like price discrimination for consumers and yield management for companies (ref. 2, 18); the development of behavioral economics (ref. 11) and a greater academic understanding of interactions between competition and consumer concerns; the growth of the tech sector and user data as "payment" for products and services (ref. 19), and the related value of user data for targeted advertising, product improvement, as well as the risk that data can act as a barrier to entry.

In this context, scholars, practitioners and policymakers are debating whether and to what extent data are related to potential market failures in digital markets, such as market power, information asymmetry, externalities and bounded rationality.

This involves an understanding of consumer data value chain. Businesses collect, process and use consumer data in many ways. The value chain can be simplified to data i) collection/accumulation, ii) access and sharing and iii) utilization/personalization (ref. 76). These are briefly described

[2] The term "consumer data" indicates data concerning consumers, where such data have been collected, traded or used as part of a commercial relationship. This term is also broader than "personal data" (the focus of privacy and data protection legislations) since it may also capture data concerning consumers even where such data cannot necessarily be traced to the individual.

below.

Data collection/accumulation. Consumer data may be collected in a number of ways: for instance, volunteered explicitly by a consumer as part of its interactions with businesses; observed in the course of interacting with a website or using a service, device or application; and inferred from other data. Typically, but not always, the entity collecting data is also the one who determines the purposes for and the manner in which such data is, successively, processed. Lastly, data separation can be mandated by competition agencies as a remedy to a competition infringement or to a merger/acquisition.

Data access and sharing. Businesses in charge of the data processing may have different incentives in sharing the data under their control. Data access or sharing initiatives can be voluntary, such as within a contractual arrangement to develop a complementary product. In addition, businesses can sell consumer data to third parties (potentially subject to consumer approval or anonymization, depending on the regulatory regime in place). Moreover, data access or sharing can be mandated by competition agencies as a remedy to a competition infringement or to a merger/acquisition. Lastly, in some jurisdictions businesses may be required to share data by law.

Data utilization/personalization. Businesses can use the consumer data they have collected in a variety of ways, including, to train machine learning and other forms of analysis underpinning artificial intelligence systems; to increase the quality or functionality of their core products or services and develop new related ones; offer consumers greater personalisation (including, possibly, personalised pricing or offers); sell third parties' advertising products or other targeted services.

Part I of this paper focuses on how competition law enforcement accounts for privacy and personal data issues. Part II presents examples of how the interaction of competition, consumer and privacy regimes can mutually support one another. Part III describes ways the interaction of these disciplines may lead to tensions and trade-offs. The final section looks at interagency coordination.

I. How does substantive competition assessment account for privacy and personal data issues?

Data issues arising at different steps of the data value chain can be considered in a competitive assessment.

Competition agencies may be willing to take into consideration data at the collection/accumulation step when it can be considered equivalent of a price increase or quality decrease (ref. 15, 30). Data accumulation may decrease quality if its collection reduces privacy, when privacy is valuable to consumers and/or an important aspect of quality competition in the relevant market considered (ref. 48). In other cases, privacy may be considered just another good (ref. 23).

More specifically, competition agencies can consider:

- whether there exists a market for data (ref. 1, 5, 21), assessing whether data is a good in itself (e.g., in the case of trading of personal data);
- whether a merger affects the level of privacy offered in the market or whether it should defer to privacy legislation (ref. 73);
- whether there may be exclusionary abuses of dominant position/monopolisation under traditional theories of harm - such as the possible tying of privacy notices (ref. 16) – as suggested in the reviewed literature;
- whether there may be exploitative abuses of dominant position (in jurisdictions where it is an infringement of competition) resulting in the reduction of privacy protection below competitive levels, and/or collecting personal data above competitive levels, or whether it should defer to privacy/consumer protection legislation (ref. 9, 14, 49);
- whether there may be anticompetitive agreements among competitors concerning privacy as any other agreement concerning an element of competition such as:
    - ✓ an agreement to exchange information on planned changes on privacy policies (ref. 24); or
    - ✓ an agreement not to introduce privacy enhancing measures or technologies or to interpret legally binding privacy standards in a restrictive and uniform manner (ref. 48).

Data utilization/personalization is another step of the data value chain where competition enforcement may consider data issues. With the advent of tracking technologies, it has been argued that the willingness to pay of each user can be estimated very precisely and prices can be determined accordingly. The use of data can improve firms' ability to provide personalised

services as well (ref. 62). At the same time, this practice might raise potential competition concerns (ref. 78): in some circumstances it might be possible to qualify personalised pricing as an exclusionary abuse, specifically whenever firms use their pricing strategies to apply lower prices to rivals' customers, in an attempt to foreclose the market; in jurisdictions where exploitative abuses are pursued under antitrust law, personalised pricing could be conceived as a form of excessive or unfair pricing, under the rationale that some consumers are charged higher prices for reasons not related to costs.

In general terms, from an economic point of view, antitrust intervention against data personalization (which includes not only personalised prices and/or services but also targeted advertising and personalised product recommendations or rankings) may be appropriate in a limited number of circumstances as it can increase static and dynamic allocative efficiency. For competition agencies that implement a consumer welfare standard, interventions could in theory be possible to deal with the impact on distribution outcomes that can arise when surplus is transferred from consumers to producers, while for those that apply a total welfare approach, spaces for interventions might be even more rare.

Also, from a legal perspective, competition agencies might be faced with the challenge to tackle discriminations aimed directly at consumers and not more traditional ones targeting undertakings. Moreover, in jurisdictions where it is an infringement, if the possible exploitation of consumers is to be pursued, competition agencies would need to deal with the comparison of the impact of personalisation on the surplus of two different groups of consumers, dealing with a negative impact on the ones with the highest willingness to pay and a positive impact on the ones with the lowest willingness to pay.

Prohibiting price discrimination may result in firms collecting data in order to discriminate in other ways, for example applying different sales services (ref. 11 and 62).

II. Intersection of competition and consumer and privacy goals: areas of mutual support and challenges in selecting the appropriate tools

There are cases where the intersection provides mutual support; that is, where consumer and privacy and competition regimes can work in mutually reinforcing ways. This is because the

application of one regime may relate to the goals of the other, or a finding from one regime may be relevant to another, or to the analysis required by another; moreover, issues that present as a competition problem may on investigation turn out to also present a consumer (or privacy) issue, or vice versa.

In this context, privacy, consumer protection and competition can act as substitutes or complements or they could be totally unrelated to one another, depending on the specific facts of the business practice under consideration.

Three categories of mutual support are addressed below: transparency, fair data processing and portability.

Transparency and informed choice

Firstly, consumer protection laws, which seek to remedy the market failure caused by asymmetric information, can promote competition by discouraging certain data practices.

At the collection step, consumers can be poorly informed about how their data are collected and, to the extent that there is an issue of asymmetric information, and businesses mislead or deceive consumers, there may be a role for consumer policy enforcement (ref. 11, 36).

In that regard, reducing information asymmetry between users and digital operators during the data collection phase might ensure that consumers receive adequate, precise and immediate information on why their data are collected and that users are able to exercise their consumer choices knowingly and effectively. The enforcement of consumer protection rules will not only provide direct protection for consumers, but also assume a pro-competition role to the extent that users are placed in a position to more consciously and actively exercise their consumer choices.

Also, a problem of asymmetric information might arise at the data utilization/personalization step as consumers may not be aware of how platforms use the data they provide or that are inferred from their behaviour. Consumers need to receive adequate information about how their data are used and make their choices accordingly. In that regard, consumer protection can bring awareness about the actual personalisation of prices/services giving the possibility to consumers to opt out if they wish (ref. 78).

Secondly, in a similar way, data protection rules can also provide support to competition goals when the compliance with privacy law contributes to create a level-playing field by promoting

competition on privacy standards at the level set by the data protection legislation or even above. For example, appropriate enforcement of privacy legislation transparency rules can ensure that consumers have easy access to trustworthy information about how firms process their data, in turn empowering consumers to make informed choices about their preferred privacy level when navigating digital markets and therefore stimulating competition on privacy standards.

Establishing in which circumstances competition and consumer or data protection regimes apply as substitutes or complements may depend on the facts as well as a jurisdiction's view on the appropriate role of its legal or regulatory regimes. For the same data collection or data utilization practices, some competition agencies would argue that intersection concerns related to such data practices can be better addressed through consumer protection or privacy law, while other competition agencies would use instead their enforcement powers to ascertain whether a data practice may amount to an antitrust violation, and complement the consumer protection or privacy regime regardless of whether the same data practice underlying the antitrust violation is also found to breach the consumer protection or privacy regime.

This difference in views raises a number of possible issues for further discussion:

- *To what extent a violation of data protection rules can be also configured as an abuse of dominant position? When should competition agencies assume that the enforcement of data protection legislation and consumer laws is not "enough" (to ensure that consumer preferences about privacy are reflected in the market) and antitrust intervention is warranted?*
- *Is there a regulatory failure from privacy agencies? Do privacy regulators lack the power to intervene or - despite having the necessary power - they do not enforce it sufficiently?*
- *Would only users of a dominant firm, as a consequence of antitrust intervention, enjoy a higher effective level of privacy protection?*
- *How should the competitive benchmark be defined in exploitative abuses of dominant position? When should competition agencies rely on legally binding privacy standards or on market-based privacy standards as competitive benchmark?*
- *How could exclusionary theories of harm based on privacy be framed?*
- *How would competition agencies deal with a code of conduct shared among competitors? Would these agreements be treated more favourably because they may enhance compliance with data protection rules or even going beyond them?*

- *To what extent data utilisation and personalisation practices that might potentially foster a firm's ability to offer better and innovative products could also be in contrast with the objectives of consumer law and data protection rules?*

The above considerations refer to the potential intersection and mutual support between, on one hand, competition and, on the other hand, consumer protection or privacy. However, there could be areas of intersection between privacy and consumer protection regimes as it can be difficult to distinguish between the right to be informed under consumer protection and privacy laws: for instance a data personalization practice could potentially be implemented without the full awareness and consent of consumers who may not be aware not only that firms keep detailed profiles about them based on data they have volunteered or that are directly observed by the firm, but also that businesses may infer preferences from consumer behaviour using advanced data analytics or machine learning tools. Whether this intersection could be of relevance from the perspective of a competition agency likely will depend on the facts and the legal and regulatory regimes in place in a particular jurisdiction.

Fair processing of data

One of the fundamental principles of data protection regulations is that of lawful and fair processing which includes all procedures aimed at ensuring transparency, confidentiality, security as well as compliance with the principles of data minimisation, purpose limitation and storage limitation. The principle of lawful and fair processing becomes even more relevant in the context of the use of complex algorithms to analyse data, which may lead to unexpected detrimental results to individuals' interests.

Compliance with this principle generally may contribute to competition goals as it can deter businesses from implementing anti-competitive behaviour based on unfair data processing practices.

As for the mutual support category of transparency and informed choice described above, competition and privacy regimes may apply in parallel or as substitutes depending on the

circumstances of the specific data practices under scrutiny and the approach of the competition agencies. Similar issues for discussion would apply.

Portability

Data portability is a user's ability to download its data from a platform in a format that allows it to use the data somewhere else. Data portability has the potential to reduce barriers to entry, to stimulate innovation, and to lower switching costs for individuals. Accordingly, the right to data portability is often attributed a competition-based rationale in addition to its data protection objective (ref. 45). Also, regulation allowing for data portability may make it easier for consumers to quickly move from a dominant firm that imposed unwanted privacy policies, thus countervailing the effect of an exercise of market power (ref. 34).

Despite being in general a useful tool, a general data portability right could differ in terms of scope and objectives from a specific competition law remedy, and therefore an effective competition remedy may need to go beyond the rights guaranteed by privacy legislation (ref. 45, 50, 76). Also, portability might help to boost consumer choice only where there is already the presence of several competitors.

Moreover, in order to make portability effective, operational details particularly matter as the use of different formats might not allow for the actual transfer of data between competitors (ref. 65) and consumers need to understand its usefulness in specific sectors so that it is not considered only as an abstract possibility.

Lastly, data standardization initiatives might offer a solution as they can enhance competition by increasing the incentives of firms to collect and share data (ref. 53, 74, 79 and 80), as well as facilitate portability of data.

Possible issues for further discussion:

- *When is data portability likely to be useful from a competition perspective?*
- *Which information should be considered portable?*
- *When is data standardization likely to raise privacy concerns as it can increase too much diffusion of consumer data?*

- *Should standardisation be a bottom up process from self-driven market forces or top down imposed by legislation?*
- *How can the right balance be found in relation to the appropriate level of standardisation that might be needed as it can, on the one hand, favour interoperability but, on the other hand, reduce product differentiation that seems to be especially relevant to succeed in the digital sector?*

III. Intersection of competition and consumer and privacy goals: possible tensions

There are areas where academic literature has identified potential conflicts arising at the intersection. For example, it has been claimed that privacy legislation is capable of hindering unfettered competition, at least in some contexts. This could be the case, for example, if privacy legislation makes it more difficult for personal data to be shared among market players, including given the difficulty of identifying a valid justification for sharing, and of ensuring sufficient transparency for the consumers concerned. If the data in question is needed for rival firms to be able to compete, it is important that privacy rules are calibrated in a way that does not undermine competition. In addition, remedies taken in competition cases (for example to enhance third party access to data) should take account of the applicable rules on the consumer and privacy side, to the extent relevant to the competition case.

Privacy legislation dampening competition

Firstly, some literature indicates that the "notice-and-consent framework" adopted by some data protection regulations is inadequate to protect privacy (ref. 63-64). Indeed, there are not only differences between stated and revealed preferences (ref. 15), that determine the so-called "privacy paradox", but also revealed preferences do not necessarily reflect the real underlying preferences of users as (ref. 76):

- preferences are not static but are malleable in that they depend in the way in which privacy options are framed; depending on the context, two identical situations might lead to different privacy behaviours (ref. 4);

- service operators may take advantage of the fact that consumers tend to stick with default privacy settings due to their status quo bias; in such a context, service providers may be able to nudge users in certain directions; and
- consumers are affected by some decision-making hurdles such as asymmetric information, bounded rationality and other cognitive/behavioural biases (ref. 7).

These demand-side market failures may inhibit competition on privacy. Consequently, a better understanding of how much consumers value privacy and engage with privacy notices appears to be needed (ref. 73).

Secondly, some literature considers that competition agencies rely too much on the effectiveness of data protection law, which might still not function well, in relation, for example, to the combination of databases in mergers and effects of portability rights (ref. 3, 15). More awareness in relation to the powers of privacy regulators and how they use them is needed.

In addition, some literature indicates that consent-based models for privacy regulation may also adversely impact on competition as they may advantage and entrench larger incumbents, especially those that operate across multiple markets. This has been found to be particularly pronounced in markets with less price flexibility, such as in zero-price markets. Similarly, other research has found that the need for consent and compliance at each stage of the online advertising supply chain increases pressures for vertical integration (ref. 3, 12 and 76).

Moreover, it has been argued that privacy legislation might reduce the incentive to share data as it might determine liabilities and compliance costs, damaging relatively smaller rather than larger players. It can, consequently, strengthen the role of players which have the ability to process internally the data collected from various sources, leading to a possible increase of market concentration (ref. 12, 25, 47, 76).

Finally, some literature indicates that privacy legislation might also impact innovation and dynamic competition as it can significantly increase the cost to start-up a new technology venture (ref. 27, 33).

Possible issues for further discussion:

- *Would a better utilisation by privacy regulators of their statutory principles (in terms, for example, in Europe, of purpose limitation and data minimisation) lead to better competitive outcomes?*
- *Should competition agencies advocate for new privacy rules or for a more strategic interpretation of the existing ones?*
- *As today, generally, the privacy legal framework does not impose additional legal responsibilities on entities with "data power", should competition agencies advocate for increased privacy legal responsibilities for firms with data power?*
- *Are there lower protections for consumers when their data are merged by the post transaction new entity as opposed to when their data are shared through data portability between two competitors?*
- *Should competition enforcement give more weight to factors that might offset the negative effects of the privacy legislation on competition? For example, in a merger of small firms, should more weight be given to the ability of the merged firms to share data in ways that enhance efficiency that, as independent firms, privacy legislation might discourage?*
- *Does the possible reduction of investment consequent to the cost increase determined by privacy legislation reduce welfare? Or does, to the contrary, privacy legislation prevent firms from coming into existence that engage in harmful activity and could encourage new types of innovation in the longer run?*

Forced sharing remedies

The data access/sharing phase of the value chain seems to give rise to a possible tension between competition and privacy regimes. Sharing or granting access to consumer data to actual competing businesses, and/or potential new entrants or firms active in other markets, can raise different issues.

Besides the theories of competitive harm relative to quality considerations explored in the previous paragraph, other ones may relate to raising barriers to entry or rival costs through privileged/exclusive access to consumer data. The entrenchment of dominant positions may impede small competitors and new entrants to compete effectively or to enter due to the lack of comparable data plus the effects of scale economies/network effects and the tipping nature of some markets (ref. 44).

Under competition law, a dominant undertaking may be required only exceptionally to provide access to data that are indispensable and not easily duplicated in order to safeguard competition in one or more markets. Even in those circumstances in which data are an important source of competitive advantage and a barrier to entry, antitrust law does not necessarily require companies to supply the data they collect to their competitors. An obligation to supply could act as disincentive to invest in those activities through which data are collected and analysed that might bring benefits to consumers in the forms of innovative services.

More specifically, competition agencies in relation to possible mergers and exclusionary abuses of dominant position/monopolisation, can envisage a remedy mandating data access and might give consumers the opportunity to opt-out of sharing their data to address concomitant privacy concerns or to opt-in by granting their consents first, depending on the applicable data protection law. Moreover, competitors may agree to share among them data of their users raising competition concerns that can, however, be overcome if possible benefits in terms of efficiency outweigh negative impacts on competition. Some literature also warns about the implications of data access in the case of mergers between data brokers (ref. 39).

Possible issues for further discussion:

- *Could dominant undertakings justify the refusal to grant access to the data they have collected, and/or generated, by invoking obligations under privacy law?*
- *Should consumers always be allowed to object and/or provide their consent to the sharing of their personal data when the sharing has not been mandated by law but rather by a competition authority as an interim measure or competition remedy?*

IV. Interagency cooperation

Besides the above described issues that arise at the intersection, a more integrated approach among agencies is needed to ensure that:

- the objectives of one policy area are not undermined by the actions taken by the other agencies;
- the appropriate enforcement tools are used according to the facts of the case.

More specifically, competition, privacy, and consumer protection agencies together should share information and ideas in taking enforcement action and developing/advocating for policy change

when and where needed. Collaboration might be also organisational, with a shared programme of work or reciprocal programmes to second staff in the other agencies. This might be especially needed towards the privacy regulator, that may seem more "culturally" distant than competition and consumer protection agencies. In particular, some scholars have discussed coordination problems between the competition agencies and data protection regulators which arise under certain scenarios (ref. 70).

Privacy and consumer protection regulators are internationally represented, respectively, by the Global Privacy Enforcement Network (GPEN) and International Consumer Protection and Enforcement Network (ICPEN) and the need might arise for ICN to liaise with them.

Possible issues for further discussion:

- *Is there a need to advocate for more convergent statutory obligations or a better alignment among the respective legislations?*
- *Is the creation of a specific mechanism for inter-institutional cooperation in specific cases involving data concerns at the intersection needed? For example, is there a specific need for an exchange of information between the different domestic agencies? Is there a specific need for competition agencies to have access to privacy expertise under the tight timeline of competition assessment of mergers?*
- *After the ICN has adopted the final document ("agency considerations document") in the context of the present project, should it liaise with GPEN and ICPEN?*
- *How should competition agencies deal with the claims, made by firms, that, because of privacy legislation, they are prevented from disclosing personal data in RFIs or inspections, or are required to inform data subjects of such disclosures?*