Competition & Markets Authority: Call for information – Digital mergers (CMA109con)

Consultation response from the

Centre for Competition Policy

University of East Anglia, Norwich Research Park, Norwich NR4 7TJ

Date: 12 July 2019

Authors:

- Elias Deutscher
- Dr. Michael Kummer

This consultation response has been drafted by the named academic members of the Centre, who retain responsibility for its content.

The Centre for Competition Policy (CCP)

CCP is an independent research centre established in 2004. CCP's research programme explores competition policy and regulation from the perspective of economics, law, business and political science. CCP has close links with, but is independent of, regulatory authorities and private sector practitioners. The Centre produces a regular series of Working Papers, policy briefings and publications. An e-bulletin keeps academics and practitioners in touch with publications and events, and a lively programme of conferences, workshops and practitioner seminars takes place throughout the year. Further information about CCP is available at our website: www.competitionpolicy.ac.uk

1. Overview and recommendations

The members of the Centre for Competition Policy (CCP) welcome the opportunity to contribute to this call for information. By discussing the role of privacy concerns for merger control, we limit our response to Question 3.1.(d) of the call for information: **How should we approach the assessment of non-price parameters of competition in digital markets?**

Our response supports recommendations with respect to the following issues:

How can privacy-concerns be accounted for in the review of digital mergers (section 2)?

- The assessment of the adverse impact of a merger on the level of privacy protection can be integrated into merger analysis without there being the need of a complete overhaul of the existing legal and analytical framework.
- For purposes of merger analysis, the level of privacy protection can be operationalised as non-monetary parameter of competition and subsumed as important element of consumer choice, quality or non-monetary price.
- The CMA could therefore account for a merger's adverse impact on the level of privacy protection under its existing PQQRI framework that focuses on price, quantity, quality, range, and innovation.[1] Alternatively, it could factor privacy as separate competitive parameter into its analysis of digital mergers, establishing a P**P**QQRI (Price-**Privacy**-Quantity-Quality-Range-Innovation) framework.

When does privacy protection as non-price parameter of competition become relevant for merger control (section 3)?

- The effect of a merger on privacy should be examined on the basis of a clear-cut counterfactual analysis. Privacy concerns are only relevant for merger analysis if the merger between two firms leads to a decrease in the level of privacy protection that consumers would have enjoyed *but for* the merger.
- The CMA's assessment of the impact of digital mergers on privacy should concentrate on the following three theories of harm:
    1. downward privacy pressure resulting from non-coordinated horizontal effects (theory of harm # 1)
    2. elimination of a privacy alternative as the consequence of non-horizontal effects (theory of harm # 2)
    3. privacy harm resulting from the matching of previously separate datasets (theory of harm # 3).

When does a merger lead to a downward privacy pressure resulting from non-coordinated horizontal effects (theory of harm # 1; section 4)?

- To assess whether a merger leads to a downward privacy pressure the CMA should focus on the following factors

[1] Merger Assessment Guidelines 2010. CC2/OFT1254 para. 4.2.3; OECD, 'Non-price Effects of Mergers - Note by the United Kingdom' (2018) DAF/COMP/WD(2018)54 para. 5.

Stage	Conditions for a downward privacy pressure	Factors
Pre-merger	Contestability and privacy externality	Can the parties divert sales from each other, as well as from their competitors by increasing the level of privacy protection pre-merger? Does the decision of a merging party to increase its level of privacy protection impose a negative externality on the sales of the other merging party?
	Cannibalisation of the profitability of the existing customer base	Does an increase the level of privacy protection have an adverse effect on the profitability of the parties' own customer base?
Post-merger	Internalisation of the privacy externality post-merger	Does the merger allow the merged entity to internalise the privacy externality that the two parties imposed on each other pre-merger? What is the privacy diversion ratio between the parties? Does the merger eliminate a significant competitive force?
	Cannibalisation	Does the merger amplify the cannibalisation effect by increasing the existing customer base of the merged entity?
	Countervailing factors	How do actual and potential competitors react to a decrease in privacy protection by the merged entity? Do pro-competitive efficiencies outweigh the adverse effect on privacy protection resulting from the merger?

When does a merger lead to the elimination of a privacy alternative as a consequence of non-horizontal effects (theory of harm # 2; section 5)?

- To assess whether a merger leads to the elimination of a privacy alternative the CMA should focus on the following factors

Stage	Conditions of a downward privacy pressure	Factors
Post-merger	Ability and incentive to foreclose, plus effect on privacy competition	Does the merged entity have the (i) ability and (ii) incentive to foreclose a competitor and does this foreclosure have (iii) the effect of substantially lessening privacy-competition?
	Countervailing factors	How do actual and potential competitors react to the foreclosure and decrease in privacy competition? Do pro-competitive efficiencies outweigh the adverse effect on privacy protection resulting from the merger?
Pre-merger	Important privacy alternative	Did the foreclosed competitor offer an important privacy alternative (e.g. higher privacy protection) pre-merger? The actual degree of privacy-related competition and contestability is **not** a determining factor.

When does a merger lead to privacy harm resulting from the matching of previously separate datasets (theory of harm # 3) (section 6)?

- To ascertain whether a merger leads to privacy harm resulting from the integration of previously separate datasets, the CMA should examine whether the combination of both datasets
    - requires the change of the parties' privacy policy
    - allows the merged entity to learn more about and better profile its users.
- If the combination of both datasets also entails a substantial lessening of competition ('SLC'), for instance, in the form of the foreclosure of a competitor offering an important privacy alternative, the CMA should assess the merger under the theory of harm #2.
- If the combination of the parties' datasets does not entail any foreclosure and substantial lessening of competition, its adverse impact on privacy could only be addressed at the stage of merger control through an amended public interest review of privacy-sensitive mergers.

Towards a unified framework for analysing privacy-related consumer harm (section 7)

- We recommend the development of a systematic classification of different degrees of privacy sensitivity of the information that an entity holds about consumers along the following lines

Degree of privacy sensitive information	Characterisation
1st degree	Access to personal data which enables more targeted advertising
2nd degree	Access to personal data which enables more price discrimination
3rd degree	Access to data that allows to infer whereabouts, contacts, times of social interactions or even the content of those interactions.
4th degree	Access to highly sensitive personal data (e.g. health data, financial data, credit information) which enables price / economic discrimination on the basis of gender, sexual orientation, health condition, or even identity theft etc.
6th degree	Access to personal data which enables political micro-targeting, online campaigning, etc.

- Such a framework might serve as useful administrative screen to flag mergers that have the potential to adversely affect privacy-competition and give rise to privacy-related consumer harm.
- It would also allow the CMA's merger review to account not only for the likelihood of a SLC in digital mergers, but to also gauge the magnitude of its potential harm to privacy-based competition and consumer privacy.

2. How can privacy concerns be accounted for in the review of digital mergers?

The question as to whether privacy and data protection concerns should be taken into account in merger control constitutes a central issue of the current policy and academic debate on non-price effects in digital mergers. Recent cases, such as the Facebook/WhatsApp[2] merger, have shown that mergers between digital platforms might not only lead to higher prices, but also entail a decrease in the level of privacy protection that consumers would have otherwise enjoyed in the absence of the merger.

The fact that this non-price privacy effect of mergers normally materialises on the 'free', user-side of online platforms where consumers receive free services in exchange for disclosing their personal information does not necessarily mean that it does not cause any harm to consumer welfare. On the contrary, the terms and bargains of the non-monetary transactions between platforms and consumers in those zero-price markets are determined by the amount and type of information consumers have to reveal in exchange of free services. We therefore suggest that the CMA should scrutinise how mergers affect consumers' level of privacy or data protection on the 'free' user side of multi-sided platforms.

A recent paper by Elias Deutscher[3] identifies three ways of how such a decrease in the level of privacy protection can be integrated into the analysis of non-price effects in merger control. Following the example of the European Commission in *Microsoft/LinkedIn*, competition authorities could approach privacy protection as a central aspect of consumer choice in digital markets.[4] Along similar lines, they could account for the level of privacy protection as important element of product quality. A third avenue for incorporating privacy-related consumer harm into merger analysis consists of conceptualising personal data as non-monetary price consumers pay when using free online services and products. Drawing upon the economic 'privacy-calculus' literature, competition analysis could approach a decrease in the level of privacy protection resulting from a merger as being tantamount to a (non-monetary privacy) price increase. The paper also proposes the use of willingness-to-pay studies in the form of conjoint analysis as a methodological tool that would enable competition authorities to quantify privacy-related consumer harm in monetary terms for the purpose of balancing it with potential welfare-enhancing efficiencies.

The integration of privacy concerns into merger control would not require a fundamental overhaul of the existing legal or analytical framework of the CMA's merger control. One way of factoring in privacy concerns would consist of framing it as an element of product quality, choice or non-monetary price under the existing PQQRI framework[5] that the CMA currently uses to assess whether a merger will give rise to a SLC. Alternatively, the role of privacy for merger analysis could also be made more prominent by ascribing to it the role of an independent factor of merger analysis and transforming the PQQRI into a PPQQRI (Price-Privacy-Quantity-Quality-Range-Innovation) framework.

---

[2] Case COMP/M.7217 Facebook/Whatsapp. C(2014) 7239 final.

[3] E. Deutscher, 'How to measure privacy-related consumer harm in merger analysis? : a critical reassessment of the EU Commission's merger control in data-driven markets' (2018). EUI Law Working Paper 2018/13. http://cadmus.eui.eu//handle/1814/58064

[4] Case COMP/M.8124 Microsoft/LinkedIn. C(2016) 8404 final [290] - [350]; see in particular [350].

[5] Merger Assessment Guidelines (n 1) para. 4.2.3; OECD, 'Non-price Effects of Mergers - Note by the United Kingdom' (n 1) para. 5.

3. When does privacy protection as non-price parameter of competition become relevant for merger control? – Three theories of harm

While recent studies mainly discuss how a loss in consumer welfare as the consequence of a decrease in privacy protection can be operationalised and measured by competition authorities when reviewing a digital merger, little attempts have so far been made to spell out when privacy should be taken into account in merger analysis. In other words, when does a merger between two firms actually have an adverse effect on the level of privacy protection?

As a general point, we suggest that the effect of a merger on privacy should be ascertained on the basis of a clear-cut counterfactual analysis: Does a merger between two firms lead to a decrease in the level of privacy protection that consumers would have enjoyed *but for* the merger?

Against the backdrop of this counterfactual analysis, three principal theories of harm of how a merger between two firms might cause a decrease in the level of privacy protection can be identified, namely:

- downward privacy pressure resulting from non-coordinated horizontal effects
- elimination of a privacy alternative as the consequence of non-horizontal effects
- matching of previously separate datasets

Each of these three theories of harm is set out in the following. Our discussion thereby focuses on the specific conditions which would have to be fulfilled for each of these theories of harm to operate. Those conditions constitute relevant factors that should guide the CMA's analysis of the effect of mergers on privacy protection. We also discuss whether those effects are best addressed within the existing legal and analytical framework for UK merger assessment or whether revisions of the current system are necessary.

4. Theory of harm # 1 - Downward privacy pressure resulting from non-coordinated horizontal effects

A merger between two horizontal competitors A and B (e.g. two providers of a consumer communication app such as in Facebook/WhatsApp[6]) may lead to a reduction of competitive pressure in the relevant market. As a consequence, the merger may decrease the incentives of the merged entity AB and its non-merging competitors not only to compete on price, but also lessen its incentives to maintain or increase a certain level of privacy protection and thus to compete on privacy post-merger. This theory of harm is closely modelled upon the standard non-coordinated horizontal effects analysis which normally assesses the extent to which a merger between two competitors leads to upward pressure on prices (or a decrease in quality, innovation etc.). No major overhaul of the existing legal and analytical framework is therefore necessary to scrutinise the impact of horizontal digital mergers on privacy. On the contrary, this theory of harm can be addressed within the current horizontal unilateral effects analysis. [7]

In the following, we propose a simple model to identify the conditions that must be fulfilled for a horizontal merger to lead to a downward pressure on the level of privacy protection.

4.1. Pre-merger

We assume that pre-merger firm A's and B's incentives to maintain or increase the level of privacy protection are driven by two essential channels or factors:

- **contestability on the basis of privacy and**
- **cannibalisation**.

4.1.1. Contestability

Pre-merger, the incentives of Firm A and B to compete not only on the basis of price, but also on privacy, depends on the extent to which their decision to increase the level of privacy protection allows them to gain profits by contesting the market shares of their rivals. If this contestability condition is fulfilled, either firm can divert sales from the other, or prevent the other from doing so, by increasing its level of privacy protection. In this case, each firms' choice of a specific level of privacy protection imposes an externality on the other, because firm A by increasing its level of privacy protection captures sales from (and thus reduces the profitability of) firm B and *vice versa.*

Clearly, this contestability condition is the strongest and arguably the most controversial assumption of this theory of harm. Recent empirical research by Kesler et al., 2019, shows that there is only a limited effect between market concentration and the level of extraction of personal data by mobile apps (i.e. one dimension of the level of privacy protection they offer).[8] While the findings suggest a limited increase of data collection in response to a reduction of competitive pressure in the market for mobile apps, this research may not carry over to mergers, because a merger might affect the incentives of firms to increase or lower the level of privacy

[6] Case COMP/M.7217 Facebook/Whatsapp (n 2).

[7] Merger Assessment Guidelines (n 1) Section 5.4.

[8] Kesler, R, M. Kummer, P. Schulte "User Data and Competition in Online Markets - Evidence from the Mobile App Industry", *Working Paper* (2019)

protection differently. Whether the results allow to infer how mergers affect data collection would have to be investigated in a separate analysis, and the study is also agnostic towards the effect of concentration on entrants. Also, the fact that a low level of privacy protection prevails in a given market does not conclusively exclude the possibility that privacy may become an important parameter of competition in the future.[9] On the contrary, there is also some empirical evidence that privacy considerations at times do influence consumers' product choices. For instance, in its Facebook/WhatsApp decision, the European Commission observed that a considerable number of users switched from WhatsApp to more privacy-protective apps in response to the announcement of its takeover by Facebook.[10] This substitution suggests that privacy is perceived at least by some consumers as an important non-price parameter of competition.

In our view, the extent to which privacy constitutes a competitive parameter and the contestability condition is met is an empirical question, which should be addressed by the CMA on a case-by-case basis in each particular merger it reviews. The contestability assumption could be tested by means of customer surveys or choice experiments that gauge whether consumers perceive privacy as important non-price feature of a given product (e.g. conjoint analysis[11]). Internal documents of the merging parties and customer switching in response to the announcement of a merger might equally provide the CMA with additional evidence and insights as to whether the merging parties and consumers see privacy as competitive parameter.

Since this theory of harm crucially hinges on the contestability assumption, the analysis of the degree to which sales in the relevant market are contestable through increased privacy protection might serve as administrative filter that would allow the CMA to identify at an early stage those horizontal mergers which might lead to privacy-related consumer harm.

4.1.2. Cannibalisation

Pre-merger, firm A's and B's incentives to increase their respective level of privacy protection also depends on the potential adverse cannibalisation effect of an increase in privacy protection on the profitability of their respective existing customer bases. Such cannibalisation of pre-existing profits is plausible, because a higher level of privacy protection generally limits platforms' ability to extract personal data from their users with a view to improving their algorithms or services and thus to monetising their data.

4.2. Post-merger

If the contestability and cannibalisation conditions are present, a horizontal merger between firm A and B might have an adverse effect on both firms' incentives to maintain or increase the level of their privacy protection after the merger. This downward pressure on privacy protection is the compound effect of:

1. the internalisation of the contestability effect or privacy externality by the merged entity;
2. the amplification of the cannibalisation effect due to an increase in the customer base.

[9] OECD, 'Considering non-price effects in merger control – Background note by the Secretariat' (2018) paras. 118-119.

[10] Case COMP/M.7217 Facebook/Whatsapp (n 2) para. 174 and fn 96.

[11] ibid.

The likelihood and magnitude of this downward pressure on privacy depend on

- the closeness of privacy competition or what one could call 'privacy diversion ratio' between both parties and/or the elimination of a significant competitive force;
- countervailing effects such as the reactions of potential and actual competitors and efficiencies.

4.2.1. Internalisation of the privacy externality post-merger:

If the contestability is met, pre-merger a decrease in the level of privacy protection by one of the merging parties would have prompted at least some of its customers to switch their demand to the other merging party and the non-merging competitors. Post-merger both parties A and B become part of a single merged entity AB. As a result, A and B can recapture the sales from those consumers who would have diverted their demand to the other merging party in response to a decrease in the level of privacy protection in the absence of the merger. Thus, A's and B's decision to increase the level of privacy protection for their services is no more only determined by its impact on the profitability of their own customer base (cannibalisation effect), but they will now also account for the externality such a decision has on the sales of the other party. Post-merger, this externality imposes additional opportunity costs on the parties' decision to increase the level of privacy protection for their services. The merger between A and B will have an adverse effect on the level of privacy protection, because it allows the two parties to internalise the mutual externality their privacy decisions imposed on each other's sales and profitability pre-merger, for instance by discontinuing or delaying their efforts to increase the level of privacy protection.[12] A merger between two competitors thus might decrease the parties' overall incentives to compete with respect to privacy protection.

4.2.2. Closeness of competition ('privacy diversion ratio') and the elimination of a significant competitive force

The magnitude of this internalisation effect on AB's incentives to compete on privacy depends on the closeness of the competitive relationship between A and B or, in other words, the **privacy diversion ratio** between the two firms pre-merger. The higher the privacy-diversion ratio between A and B (i.e. the more one firm could divert sales from the other by raising the level of privacy protection), the higher will be the merged entity's (AB) incentive to discontinue or slow down its privacy competition post-merger. The closeness of competition or the privacy diversion rate thus measures the degree to which A and B exerted on each other competitive pressure with respect to privacy protection pre-merger. It is thus an important indicator as to whether the combination of A and B will lead to a substantial lessening of competition (with respect to privacy) post-merger.

Likewise, the adverse effect of the merger on privacy protection is likely to be high, if one of the two merging parties is a significant competitive force that, for instance, has a strong track record in competing on privacy protection.

[12] After the merger, both parties might also try to avoid such cannibalisation between their sales by repositioning their products, for instance, by offering a low-price/low-privacy protection and a high-price/high-privacy protection app, rather than two low-price/high privacy protection apps they offered pre-merger.

4.2.3. Cannibalisation

Cannibalisation is another important channel that operates post-merger with respect to the merged entity AB. Accordingly, the merged entity's incentive to increase the level of privacy protection depends on how this affects the profitability of its customer base. If the merged entity increases its privacy protection post-merger, it could not only offer this higher level of privacy protection to newly acquired customers but would have to apply the same terms and conditions to its existing customer base. If the combination of A and B leads to an increase in the customer base of the merged entity (AB), the cannibalisation effect on the profitability of the merged entity AB would be higher than on A and B in the absence of the merger. In this case, the cannibalisation effect reinforces the contestability effect and additionally dampens the incentive of the merged entity AB to enhance the level of privacy protection post-merger. The size of this cannibalisation effect post-merger depends on the extent to which both parties unify their services, networks or platforms post-merger and the merged entity's ability to apply differentiated privacy policies to the users of its different services.

4.2.4. Countervailing factors

The likelihood and magnitude of a lessening of privacy competition between firm A and B post-merger also depends on how actual or potential competitors respond to AB's slowing down its efforts to increase or even lowering of the level of privacy protection post-merger. The merger's adverse effect on privacy protection will be defeated, if potential entrants and/or existing competitors respond by maintaining a higher or by enhancing their level of privacy protection. In the presence of barriers to entry or expansion (e.g. network effects and high switching costs), it is unlikely that existing or potential competition prevents the merged entity AB from decreasing its level of privacy protection. This is also the case if consumers are privacy-insensitive and do not quickly switch to competitors in the response to a decrease in privacy policy

The reaction of competitors is determined by the degree of strategic complementarity between their incentives and those of the merged entity. When the strategic complementarity between those firms is high, it is unlikely that the reaction of competing firms will offset AB's decision to lower privacy protection. Rather, owing to the overall reduction of competitive pressure in the market as a consequence of the merger, the competitors might have an incentive to respond by equally lowering the level of privacy protection of their own products. This assumption is in line with the standard analysis of non-coordinated effects in mergers, which assumes that a merger between two close competitors in an oligopolistic market will not only lead to an upward pressure on prices as a result of the elimination of competition between the two merging parties (first order effect), but will also create incentives for the non-merging competitors to increase their prices due to the reduction in the overall competitive pressure at the industry level (second order effect). Along similar lines, a horizontal merger might give rise to a market-wide downward pressure on the level of privacy protection offered by both the merged entity and the non-merging competitors. This second-order effect might be quite substantial, in so far as a decrease in the level of privacy protection may also increase the profitability of the customer base of the non-merging firms, by enhancing their capacity to collect more personal data with a view to improving and monetising their services.

The consumer harm resulting from a decrease in privacy protection might be outweighed by pro-competitive efficiencies. Further research on how to evaluate and balance these countervailing factors with consumer-related privacy harm is needed.

5. Theory of harm # 2 - Elimination of a privacy alternative as the consequence of non-horizontal effects

A second channel by which a merger might adversely affect privacy protection is when it leads to the foreclosure of a competing firm which offers its customers a high level of privacy protection. This foreclosure scenario normally materialises in non-horizontal (vertical and conglomerate) mergers between two non-competing firms active on two separate levels of the supply chain. Take for instance the merger between Microsoft, a producer of software applications and operating systems for PCs, and LinkedIn, a professional social network provider. In this case, the Commission found that the merged entity Microsoft/LinkedIn would gain the ability to marginalise other competing professional social network providers, such as XING, which at the time of the merger provided a higher level of privacy protection to its users than did LinkedIn. The Commission, therefore, concluded that the merged entity would eventually eliminate an important privacy alternative from the market and, thus, reduce consumer choice with respect to privacy, which in the eyes of the Commission, constituted an important dimension of competition.[13]

This theory of harm differs from the standard non-horizontal effects analysis only in that it assesses the extent to which the foreclosed competitor offers an important privacy alternative. No major overhaul of the existing legal and analytical framework is therefore necessary to assess the impact of non-horizontal digital mergers on privacy. On the contrary, this theory of harm can be addressed within the current non-horizontal effects analysis.[14]

5.1. Assessment of contestability is not necessarily required

Unlike in the previously discussed theory of harm # 1, in the case of non-horizontal foreclosure, the degree of contestability of demand/sales in the markets where the parties are active is not an essential element of the theory of harm. The negative impact of the merger on privacy does not directly flow from a decrease in the level of privacy competition between the merging parties. Rather, it results from the foreclosure of a non-merging competitor which happens to offer a higher level of privacy protection than one of the merging parties. The harm to privacy is in this case not the primary effect of the elimination of privacy-competition between the parties, but rather a secondary, collateral effect of the foreclosure of a competitor. This explains why the Microsoft/LinkedIn the European Commission applied this theory of harm without looking into the degree of privacy-based competition and contestability prevailing in the relevant market for professional social networks pre-merger.

5.2. Ability and incentive to foreclose and effect on privacy competition

To assess whether a merger leads to a non-horizontal foreclosure of a competing firm which offers a high level of privacy protection, it is therefore sufficient to ascertain in line with the

[13] Case COMP/M.8124 Microsoft/LinkedIn (n 4) [290] - [350]; see in particular [350].

[14] Merger Assessment Guidelines (n 1) Section 5.6.

standard non-horizontal effects analysis[15] whether the merged entity will have the (i) ability and (ii) incentive to foreclose an upstream or downstream competitor and whether this foreclosure has (iii) the effect of substantially lessening privacy-competition because the foreclosed firm would have provided a higher level of privacy protection post-merger.

5.3. Countervailing effects

The likelihood and ability of the merged entity to foreclose a competitor and the magnitude of the ensuing harm to consumers (i.e. here the lower level of privacy protection), depends on the reactions of existing and potential competitors and buyers. In the presence of high barriers to entry or expansion (e.g. data-driven network effects, economies of scale or scope, high sunk costs) and switching costs (e.g. consumer lock-in), it is unlikely that the entry or expansion of existing or potential competitors will defeat the merging parties' ability and incentive to foreclose a competitor. The consumer harm resulting from a foreclosure of a competitor and the ensuing decrease in privacy protection might however be outweighed by pro-competitive efficiencies.

6. Theory of harm # 3 - Privacy harm resulting from the matching of previously separate datasets

A merger between two firms might decrease privacy protection via a third channel, if it enables them to combine and match their previously independent datasets. The combined data might allow the merged entity to learn more about their consumers. In so far as at least one of the two firms shares its data with the other party, such a merger might lead to a decrease in privacy protection of the consumers of at least one of the two firms. An indication of such a reduction would be if one of the two firms has to change its privacy policy to obtain the consent of its users to the sharing of their data with the other party. Privacy harm might also arise from the fact that the combination of the two datasets enables the merged entity to profile the consumer to a larger extent than it would have been possible in the absence of the merger.

It is conceivable that the combination of both data sets will bestow the merged entity with market power and the ability and incentive to foreclose existing competitors. If the combination of two datasets allows the merged entity to marginalise competing firms (e.g. due to higher economies of scale and scope or network effects), it might give rise to a substantial lessening of competition.[16] This lessening of competition, in turn, might reinforce the merging parties' incentives to lower the level of privacy protection with a view to combining both parties' datasets. The adverse impact on privacy is even more pronounced, if the merger drives important privacy alternatives out of the market. Those foreclosure effects could be addressed within the framework of the theory of harm 2 set out in the previous section.

Yet, the reduction in privacy protection resulting from the combination of previously separate datasets might also materialise in cases where the merging parties are active on two rather unrelated markets (e.g. an online platform and a supermarket such as in Amazon/Wholefoods) and the merger does not lead to a foreclosure of non-merging competitors. Assuming that

[15] ibid Section 5.6.6.

[16] This theory of harm has for instannce been assessed by the European Commission in Case COMP/M.4731 Google/DoubleClick. C(2008) 927 final; Case COMP/M.7217 Facebook/Whatsapp (n 2); Case COMP/M.8124 Microsoft/LinkedIn (n 4); Case COMP/M. 8788 Apple/Shazam. C(2018) 5748 final.

privacy protection constitutes an important parameter of product quality or even a non-monetary price, such a conglomerate merger reducing privacy protection might create consumer harm in the same way as a horizontal or non-horizontal merger. But as long as the reduction in privacy protection does not involve a lessening or distortion of competition, such a merger could not be reviewed and remedied under the current legal framework.

Privacy harm arising from the combination of datasets as a consequence of a merger which does not entail a substantial lessening of competition could only be addressed at the merger review stage by an amendment of Section 58 of the Enterprise Act that introduces a public interest review of mergers which give rise to a high privacy risk.[17] Such a public interest review of privacy-sensitive mergers could account for the broader implications and externalities that might arise from the matching of user datasets for the affected data subjects, but also more broadly for our society and democracy.[18] For instance, the revelations surrounding the cooperation of Facebook and Cambridge Analytica suggest that privacy might play a similarly important role for the integrity and resilience of democratic processes and institutions as does media plurality. While the Enterprise Act provides for a public interest review of media mergers that might adversely affect the plurality and quality of media and broadcasting (Section 58 (2) of the Enterprise Act), no such review for mergers that might lead to privacy harm exists so far.

7. Towards a unified framework for analysing privacy-related consumer harm

To account for the multidimensional nature of privacy and provide a unified framework for thinking about how reduced privacy protection could affect consumer welfare, we recommend the development of a systematic classification of different degrees of privacy sensitivity of the information that an entity holds about consumers. Those degrees of sensitivity would depend on the type and sensitivity of information contained in the personal datasets and the potential use of that data.

The following table provides for a stylised example of such a classification.

Degree of privacy sensitive information	Characterization
1st degree	Access to personal data which enables more targeted advertising
2nd degree	Access to personal data which enables more price discrimination
3rd degree	Access to data that allows to infer whereabouts, contacts, times of social interactions or even the content of those interactions.
4th degree	Access to highly sensitive personal data (e.g. health data, financial data, credit information) which enables price / economic discrimination on the basis of gender, sexual orientation, health condition, or even identity theft etc.

[17] See for such a proposal Select Committee on Communications of the House of Lords, 'Regulating in a digital world' (2019). 2nd Report of Session 2017–19 HL Paper 299 paras. 15, 147-148.

[18] See in this respect for instance Information Commissioner's Office, 'Democracy disrupted? Personal information and political influence' (2018).

6th degree	Access to personal data which enables political micro-targeting, online campaigning, etc.

We argue that a systematic taxonomy of different degrees of privacy sensitivity is key to enable a meaningful discussion of the risks and potential harms to consumers that emerge from firms holding privacy sensitive data and the combination of datasets as the result of a merger. While the gradation above is only an initial proposition which should be further elaborated in cooperation with privacy and data protection experts, a similar scale could serve as a useful unified framework for discussing potential privacy concerns and evaluating privacy harm to consumers emanating from platform conduct or digital mergers. For example, the scale could be used to evaluate whether the involved parties (or the competitors) offer differentiation with respect to privacy. It could also be used to evaluate the potential privacy harm that might be created by the combination of two previously independent data sets in the aftermath of a merger. If the separate entities have access to sensitive data of degree 3, but the merged entity would have access to sensitive data of degree 5, this might be a case for a public interest review.

In general, such a graded framework might serve as useful administrative screen that could help to flag mergers that have the potential to adversely affect privacy protection and give rise to privacy-related consumer harm. Furthermore, a unified and coherent framework to operationalise privacy-related consumer harm would allow the CMA's merger review to account not only for the likelihood of a SLC in digital mergers, but to also gauge the magnitude of the potential harm to competition and consumers.

Our recommendation thus ties in with a central recommendation in the Report of the Digital Expert Group ('Furman report') in support of an amendment in the existing legislative framework to transform the 'balance of probabilities' into a 'balance of harms' standard 'which takes into account the scale as well as the likelihood of harm in merger cases'.[19] We further point out that consumer harm could emerge not only from being exposed to a firm's actual *use* of consumers' data in privacy intrusive ways, but also from the mere threat that results from the firm's ability to use a consumer's data intrusively.

[19] J. Furman and others, 'Unlocking digital competition: Report of the Digital Competition Expert Panel' (2019) 12–13, 99-100. See also in this respect Professor Bruce Lyons' response in E. Deutscher, B. Lyons and W. Lam, 'CCP response to HM Treasury: Digital Competition Expert Panel - Open consultation' (December 2018) 6.