Facebook / Germany – a new frontier for privacy and competition?

March 2018

On 19 December 2017, Germany's national competition authority found, as part of a preliminary assessment, that Facebook abused its dominant position. It is the first time that a European competition authority has assessed the compliance of a company with competition laws through the application of data protection principles. As the head of the German competition authority noted, "*we are blazing a trail in this case. We are looking very closely at the connection between data and market dominance, data and market power, and the possible abuse of data collection*".

What is the German competition authority investigating?

In March 2016, the Bundeskartellamt, Germany's national competition authority (the 'Authority'), initiated an investigation into whether Facebook may have abused its dominant position in the German market for social networks. The Authority's investigation is ongoing, and is expected to conclude around summer 2018. In its preliminary assessment of December 2017 (the 'Assessment'), the Authority found that:

- Facebook holds a dominant position in the German market for social networks; and
- Facebook is abusing its dominance by imposing exploitative and unfair terms on its users. This also breaches the fundamental constitutional rights of Facebook's German users (in particular, data protection rights).

Facebook's dominant position

The detail of the Assessment of Facebook's dominance is beyond the scope of this article. However, it is relevant that the Authority found that Facebook's users "*cannot switch to other social networks*" in Germany and are effectively "*locked in*" to Facebook as a result. The Assessment then goes on to consider whether Facebook has abused its dominant position.

From a data protection perspective, it is the Authority's approach to establishing Facebook's abuse of its dominant position, and the role of data protection law in that assessment, that is of particular interest. This article will look at these elements in more detail below.

Why does the Authority consider data protection issues are relevant?

In the Authority's view, "*where access to personal data of users is essential for the market position of a company* [here, Facebook]*, the question of how that company handles the personal data of its users is no longer only relevant for data protection authorities. It becomes a relevant question for the competition authorities, too*". In addition, under German competition law access to personal data is a specific criterion for assessing market power.

As the Authority considers personal data (and the processing of that data) to be an essential element of Facebook's business operations, data protection principles are relevant to the Authority's assessment of Facebook's behaviour under German competition law.

What are the specific data protection issues on which the Authority focusses?

Lack of transparency

The Authority is concentrating its investigation on Facebook's policy of collecting user-generated data outside of Facebook and Facebook-owned websites and apps (such as WhatsApp). In particular, the Authority is focussing on terms that allow Facebook to collect user data that is generated on the many third-party websites or apps with embedded Facebook application programming interfaces ('API'). Examples of such API include the Facebook 'Like' or 'Log-in' options that appear on third-party websites.

According to the Authority, these terms allow Facebook to harvest data from users as soon as they navigate to the third-party website, even if the user has blocked web tracking and / or does not click on the 'Like' or 'Log-in' buttons. This data is then merged with data that is generated on Facebook's site and other sites or apps owned by Facebook, to create a detailed profile of each user and their online activities. This dataset can then be used by Facebook, for example for advertising purposes (which generates very significant revenue).

In the Authority's preliminary view, the effect of these terms is that users are oblivious as to which data from third-party sources is being collected by Facebook. A further concern is that, as a result of the merging of data from disparate sources, "*individual data gain a significance the user cannot foresee*".

Consent

As Facebook is considered by the Authority to be a dominant company, the Authority considers that users cannot switch to other social networks and thus have no option other than to accept its terms in order to use Facebook. As a result, users cannot be deemed to have effectively consented to this data collection and processing.

Consequently, the Authority concludes that these terms are not "*justified under data protection principles*". In particular, the Authority notes that "*data protection legislation seeks to ensure that users can decide freely and without coercion on how their personal data are used*".

Which specific data protection rules does Facebook's behaviour relate to?

The exact legal basis on which the Authority has found a breach of data protection law has not (yet) been made clear (although the Assessment notes that the Authority is closely cooperating with the German data protection authorities on this aspect of the case).

That said, the Assessment notes that it "*includes the principles of the harmonised European data protection rules, in particular the EU General Data Protection Regulation*". On this basis, it may be that the Authority considers that, for example:

- Users have not freely consented to the processing of their data, as required by Article 7 of the General Data Protection Regulation (GDPR) which will take effect on 25 May 2018.
- Users have not received adequate information as to the uses of their data, in breach of the transparency requirements under Articles 5 and 12-14 of the GDPR.
- There is a breach of users' reasonable expectations as to the processing of their data by Facebook (which raises issues related to the lawfulness of processing under Article 6 of the GDPR).
- The requirements of Article 21 of the GDPR relating to profiling of users' data are not met.

How do these alleged data protection breaches give rise to an abuse of dominance?

A breach of data protection law by a dominant company does not automatically give rise to an abuse by that company of its dominant position. There must be some additional criteria, aside from Facebook's alleged breach of data protection law, to establish that Facebook has abused a dominant position. It is not precisely clear from the publicly available materials on the Authority's preliminary decision what these additional criteria are.

That said, the Authority is clear that it considers Facebook's terms to be unfair and exploitative of its users – under German competition law, such exploitative terms can be abusive. In assessing the extent of that exploitation (that is, whether it is truly abusive), the Authority explains that German law and case precedent establishes that, if Facebook's terms are "*a manifestation of* [Facebook's] *dominance or superior market power*", and would be inadmissible under German civil law principles (which include data protection principles), such terms can be considered exploitative and therefore abusive.

In particular, the Authority considers it relevant to assess the balance of interests between Facebook and its users – in particular, whether Facebook is so powerful "*that it is practically able to dictate the terms of the contract and the contractual autonomy of the other party* [that is, each Facebook user in Germany] *is abolished*".

On this basis, the Authority appears to find that Facebook, as a result of its dominance, disregards its users' constitutional rights (such as the rights to privacy that are enshrined in data protection laws). It has therefore committed an exploitative abuse of its dominance.

Issues with the Authority's approach

Two observations can be made on the Authority's approach:

- While the Authority has found that Facebook users are 'locked in' and cannot switch to other networks, it is not clear from the available materials whether or how the Authority has explicitly established causation between Facebook's alleged dominance and a finding that a breach of data protection laws is an abuse of that dominance. A simple breach of data protection law does not give rise to a *per se* abuse (and it is not clear that the terms are a clear 'manifestation' of Facebook's dominance).
- The Authority is relying specifically on German law and national case precedent to establish that Facebook has abused its dominance. This may reduce the scope for other national competition authorities to approach data protection and competition law in the same way.

A wider role for data protection?

Facebook is already under scrutiny by data protection regulators. In recent years, a number of data protection authorities in Europe (in France, Belgium, Germany, the Netherlands, Spain and Italy) have opened investigations into Facebook and WhatsApp's data processing activities. A number of these authorities have issued fines for breach of data protection rules (in France, Spain, Italy and – most recently in February 2018 – a €100 million fine in Belgium) or otherwise found that Facebook or WhatsApp is breaching data protection laws (in Germany and the Netherlands).

Separately, the EU's Article 29 Working Party is continuing to investigate WhatsApp's data use policies, its current view being that WhatsApp and Facebook have failed to demonstrate full compliance with data protection rules.

Data protection within competition?

Competition regulators have traditionally not considered privacy and personal data issues to be within their remit. As the EU's competition regulator stated during its review of Facebook's acquisition of WhatsApp in 2014:"*any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of EU competition law rules but within the scope of the EU data protection rules*".

However, this position may be changing, in particular for companies that could be considered dominant:

- The European Data Protection Supervisor has advocated a shift towards a "*more holistic approach to enforcement*" – encompassing closer cooperation between competition, data protection and consumer protection regulators.
- The EU Commission is continuing to investigate (and penalise) allegedly dominant technology companies that rely for their competitive success on the ability to compile and process vast datasets - most recently Google, who was fined €2.4 billion in 2017 for abusing a dominant position and is awaiting the outcome of two further competition investigations.
- The EU Commission Competition Commissioner Margrethe Vestager noted earlier this year that she has an "*open mind*" as to the role that regulators can play when assessing large companies' data assets but considered that "*these data are extremely valuable*".
- A recent joint report by the French and German competition authorities argues for competition law analyses to take greater account of data protection issues where these affect the competitive process in a given market (in particular, where they are relevant to an assessment of market power).
- The French and Italian competition authorities, in conjunction with other regulators including data protection authorities, have both launched sector enquiries on online advertising and Big Data respectively.

Key takeaways

If your organisation could be considered dominant in any of the markets in which it operates (in particular in Germany), and access to customer data is key to its business operations:

- Be aware that an investigation by data protection authorities into an organisation's data protection practices could prompt competition authorities to consider whether the organisation is compliant with applicable competition laws, and vice-versa.
- Competition (and/or data protection) authorities may consider the extent to which customers have freely consented to the processing of their data.
- Consider the extent to which customers have control over how their data is used, as well as the information that your organisation gives customers about how it uses their data. The more control and information they have, the more likely it is that your organisation will be considered compliant with relevant data protection and competition rules.

Conclusion

Whilst it will come as no surprise that Facebook's data protection practices continue to attract the attention of regulators, it is the first time that competition authorities are looking at such practices in the context of competition proceedings. Clearly, potentially dominant companies should be monitoring the development of these proceedings over the course of this year. In the not too distant future, it may be that certain organisations will have to field data protection queries from both data protection and competition authorities.

Slaughter and May advises on all aspects of data protection and privacy, including GDPR compliance programmes. If you would like further information, please contact Rebecca Cousin, Rob Sumroy or your usual Slaughter and May advisor. Further publications are available on our website.

Jordan Ellison
T +32 (0)2 737 9414
E jordan.ellison@slaughterandmay.com

Alexander Chadd
T +32 (0)2 737 9419
E alexander.chadd@slaughterandmay.com

Rebecca Cousin
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Cindy Knott
T +44 (0)20 7090 5168
E cindy.knott@slaughterandmay.com