Privacy policies: Is there a risk of anti-competitive collusion?

As data and privacy policies can be parameters of competition, companies must take care when making decisions about commercially sensitive issues. By **Sophie Lawrance** and **Noel Watson-Doig** of Bristows LLP.

Controversially, yet inexorably, big data, data protection and privacy policies are the coming issues in competition law. According to Prof. Dan Ariely[1], "big data is like teenage sex; everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it". Consequently, issues which previously were solely the domain of privacy lawyers are increasingly being viewed through the lens of competition law. It is therefore becoming more important for privacy practitioners to have an understanding of the basic tenets of competition law together with the underlying policy rationale.

This article considers the extent to which collusion in relation to privacy policies is an area that competition authorities may investigate and, if so, what the implications are for online service providers. In particular, it reviews the rules in relation to anti-competitive information exchange and collusion; the rapidly shifting boundary between competition law and data protection; the risks and potential consequences of exchanging commercially sensitive data and privacy; and the consequent advisability of a cautious approach to discussions with competitors. Competition law is about consumer choice and ensuring that markets pass on the benefits of competition to consumers. Competitive prices are central to these benefits. But other forms of non-price competition are also crucial, including notably product variety, innovation and quality. These non-price competition parameters increasingly include access to data and privacy protection.

How does competition law work?

Competition laws in relation to collusion are similar in the EU and the UK. Each regime prohibits agreements (whether formal or informal) between undertakings [companies] or concerted practices which may affect trade between EU Member States or in the UK, and which have as their object or effect the prevention, restriction or distortion of competition within the EU or the UK. This definition is broad enough to capture any anti-competitive "concurrence of wills" between two (or more) parties. Breaches of competition law are investigated, and penalised, by the European Commission at EU level and by the Competition and Markets Authority (CMA) in the UK.

Forms of information exchange between competing companies are a common feature of many markets. Competitors may exchange information either directly or indirectly, for example, via a trade association or through a company's suppliers or retailers. In many cases, the exchange of information will have a legitimate purpose. It is the sharing of competitively sensitive information that is close to the functioning of the market that raises significant competition law risk. The key issue is whether or not the exchange of information reduces the strategic uncertainty of competitors, thereby limiting their incentives to compete against one another or coordinating their behaviour in relation to important parameters of competition.

Data and privacy policies as a competition issue

Case law to date has considered information to be strategic if it relates to (current, recent or future) prices, customer lists, production costs, quantities, turnovers, sales, capacities, qualities, marketing plans, and also future investments, technologies and R&D programmes. The question therefore arises whether data and privacy policies could amount to strategic information, the exchange of which would give rise to an impact on competition, and if so, in what particular circumstances.

The potential competition issues in relation to data protection and privacy policies were highlighted by the European Parliament in 2015: "Access to digital platforms often seems to be free of charge, but by providing the platform operators with personal data, consumers do at least pay a price in terms of switching costs […] Consumers are not always aware that digital service providers collect, analyse and market private data; nor are consumers aware of the security risks involved when that data falls into the wrong hands. Even if consumers are aware, it is not clear to them how firms use or protect the information they retrieve via online transactions."

The rapidly changing nature of the competition law and data/privacy landscape is further illustrated by a paper published jointly by the German and French Competition Authorities in 2016 which noted that "decisions taken by an undertaking regarding the collection and use of personal data can have … implications on economic and competition dimensions. Therefore, privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services." The practical implications of this new landscape is illustrated by the German Competition Authority's (BKA) 2016 investigation of Facebook's privacy policies on the suspicion of abusing its market power (*PL&B International* October 2016, p.1).

Nevertheless, the extension of competition law into privacy is controversial as it raises the question of the extent to which competition law should factor in other fields of law.

 © 2017 PRIVACY LAWS & BUSINESS

Competition Commissioner, Margrethe Vestager, stated in 2016 that she did not think the European Commission needs to look to competition enforcement to fix privacy problems. This echoes the view of the Court of Justice of the EU (CJEU) which has previously considered that "issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection." (Asnef / Equifax (2006)).

It is in the context of merger control assessments that data and privacy policies have been most clearly established as parameters of competition:

- **Facebook / WhatsApp (2014):** This deal was cleared by the Commission under its merger rules on the condition that the WhatsApp service would continue to honour previous privacy policies and obtain users' consent before changing any policies. The review did not specifically take into account the potential that, post-merger, the parties' privacy policies may become weaker and the impact these could have on consumers. However, in commentary published by the European Commission itself on the merger, it was noted that privacy policies amounted to a non-price parameter of competition. Degradation of privacy policies could affect other aspects of product quality, or amount to an increase in the "price"paid by consumers for the product (e.g. in terms of requiring more personal data to be provided). In the merger context, the Commission noted that this would only be likely to have an impact on competition where privacy was a key parameter of competition between substitutable products. In the context of social media, as assessed in 2014, a number of other parameters of competition were deemed by the Commission to be more important (e.g. price, reliability of service, user base and popularity). (The recent €110 million fine levied by the European Commission on Facebook related to the provision of incorrect information in this merger investigation, but not to the particular issues discussed in this article.)
- **LinkedIn / Microsoft (2016):** This more recent merger considered whether the post-merger combination of data was likely to raise competition concerns. However, the European Commission cleared the deal notwithstanding the concerns over "data market power". Nevertheless, privacy related concerns were given greater weight in this case: "the Commission concluded that data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction."

Neither the European Commission nor national competition authorities have yet investigated information exchange in relation to data and privacy policies. However, they have a record of innovative applications of the prohibition on anti-competitive agreements to capture potential abusive conduct in the digital economy, for example:

- **The Eturas case (2014)** confirmed that making technical changes to an online platform, which restricted the level of discounts that could be offered by the travel agents to their customers could amount to a concerted practice if it was not actively repudiated by participating travel agents.
- **The CMA's Trod and GB eye Decision (2016)** found that two Amazon Marketplace vendors had fixed prices by using and configuring "commercially-available automated repricing software" in order to illegally fix prices at an artificially high level.
- **The CMA's case** closure statement in relation to energy price comparison websites (2016) suggested that restrictions on bidding for particular advertising terms, or on negative matching (identifying terms for which advertisements should not be shown) may amount to an anti-competitive agreement.
- **The CMA's market study** into digital comparison tools (DCTs) (2016/17) identified possible areas of anti-competitive concerns including contractual arrangements that could limit competition between DCTs.

How to stay on the right side of competition law

Given that data and privacy policies are now recognised as parameters of competition, there are a number of ways in which companies providing online services to consumers could risk infringing the prohibition on anti-competitive agreements. For example, there may be a risk that exchanging information about planned changes to privacy conditions/other online trading T&Cs, or actually agreeing a common strategy for such changes, could amount to an anti-competitive agreement. An agreement between separate companies to adopt a common practice on such terms (in particular if it resulted in less protection for consumers) could amount to an anti-competitive agreement.

While these concerns are (currently) speculative, the examples of other innovative investigations into anti-competitive agreements online illustrate the expansive approach taken to the anti-competitive agreements. The logic of these cases is that the more important a particular issue is to consumers (such as data and privacy policies) the more likely it is that they could come into focus as part of a future competition investigation. However, agreements are only regarded as anti-competitive if they are likely to have an actual or likely appreciable adverse impact on at least one of the parameters of competition (which as discussed above includes data and privacy policies). Agreements or contacts between competitors in relation to data and privacy policies are less likely to be regarded as inherently anti-competitive in the way that agreements in relation to exchanges of pricing information would be. In particular, some measure of informal benchmarking is unlikely to be problematic in most cases.

In the limited cases where the exchange of information around privacy policies may give rise to competition concerns, there may be counter-arguments that such exchanges of information (provided they do not break data protection laws) are "pro-competitive", as they are likely to result in improvements for consumers. Examples of pro-competitive improvements might include: benchmarking against

industry best practice; simplified privacy policies; improved technical solutions; increasing standards of protection; and improved data portability. However, arguments that potentially anti-competitive behaviour may have pro-competitive justifications are difficult to substantiate and should be treated with caution. Competition authorities take a sceptical view of pro-competitive justifications for potentially anti-competitive conduct, and persuading them to change their mind is often both expensive and resource-intensive.

Potential for large fines

The consequences for infringements of competition law can be severe. The European Commission and the UK's CMA can declare an agreement invalid and fine companies up to 10% of group global turnover; equally companies can be exposed to possible follow-on damages actions. However, in the case of novel enforcement actions (for example the exchange of confidential data and privacy policies), it is perhaps more realistic to anticipate that the Commission or the CMA would either seek to settle cases at an early stage or enter into legally binding commitments with the parties as to future behaviour, without a formal infringement decision.

As with other areas of competition law, conduct which has a negative impact on consumers is particularly likely to be regarded as damaging to competition. Any contacts between competitors which result in reduced choice or degraded protection for consumers is therefore particularly likely to give rise to risks.

The conclusion of all this is that it would be prudent for companies providing online services to consumers, which are often only differentiated by their data and privacy policies, to exercise significant caution in their contacts with their competitors. Using publicly available information to benchmark with competitors' data protection policies and terms and conditions is permissible. However, companies should take their own decisions about commercially sensitive issues, including data and privacy policies. In the event of an investigation by a competition authority, companies should also be in a position to evidence that all commercially sensitive decisions have been taken independently.

AUTHORS

Sophie Lawrance is a Partner and Noel Watson-Doig an Associate at Bristows LLP.
Emails: Sophie.Lawrance@Bristows.com
Noel.Watson-Doig@Bristows.com

REFERENCE

1 See danariely.com