Internet of Things: Antitrust concerns in the pipeline?

Kluwer Competition Law Blog
May 12, 2016

Bill Batchelor and Grant Murray (Baker & McKenzie)

Please refer to this post as: Bill Batchelor and Grant Murray, 'Internet of Things: Antitrust concerns in the pipeline?', Kluwer Competition Law Blog, May 12 2016, http://competitionlawblog.kluwercompetitionlaw.com/2016/05/12/internet-of-things-antitrust-concerns-in-the-pipeline/

Ever since the incoming EU Competition Commissioner said that information was the new currency of the internet, antitrust commentators started to spill ink on the topic of Big Data and whether it was a Big Deal. The topic now seems to occupy a place on the agenda of many antitrust conferences – and as recently as last month the US Council of Economic Advisers (to the President) flagged it as a potential area for further exploration to enhance competition. An Executive Order followed on the heels of this, asking all executive agencies and departments to take steps to address competition concerns.

When it comes to Big Data, in one camp are antitrust commentators who worry that 'free' internet services are like 'free' lunches (no such thing…) and that rules and regulations must step in to prevent consumer harm. The same camp does not worry about an apparent overlap with data privacy/transparency concerns/laws. Instead, they point to cases like Libor etc which have been the subject of both regulatory and antitrust scrutiny. We've seen the legislative/antitrust interface in the tech space before – e.g. right to interoperability in the Software Directive; data portability provisions in the new General Data Protection Regulation.

In the other camp are those people which assert that Big Datasets are not very different to other types of strategic assets/inputs and that existing rules/procedures can easily handle any antitrust issues that arise.

Looking across US and EU experience, Big Data seems to raise issues in three areas where agencies have plenty of experience/case law:

- Big Datasets are like assets – mergers of companies with those could raise foreclosure/consumer harm issues (and those mergers seem to be on the up)
- A firm's attitude to data collection/privacy could be a parameter of non-price competition and if that is lost due to a merger then that should be a concern. But that case hasn't happened yet. It's possible to imagine how internal documents could get a merger into hot water in this area – but otherwise it's difficult to imagine how this could be measured – in the same way that one might struggle to analyse whether the merger of two oilfield service firms might reduce health and safety efforts
- Holding a large dataset could in theory give rise to market power/barriers to entry and essential facility type arguments in EU-style jurisdictions. But there are challenges around market definition (even with EU rules that allow the upstream input market to be fairly theoretical) and then showing the need for access for downstream competition

Internet of Things

Less has been written about the (potential) antitrust aspects of the Internet of Things: the network of physical objects – devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data.

Think: fridges; home thermostats; heart devices; bridges (whose cement has sensors monitoring stresses) ; self-driving cars; vineyards (which predict when fruit flies will arrive) and cows (collars which track their paths in a field to increase productivity – possibly the same technology used for professional rugby players?). Designer handbags will be able to self-authenticate via embedded codes. Could golf clubs tell us how to perfect a swing?

Wearable devices in the health sector are experiencing huge growth. A blog on the Huffington Post recently referred to a report from a UK innovation foundation which found that 95% of doctors saw an increase in patients attending consultations with health data they had collected themselves and that 90% of doctors said it was useful.

On an even bigger scale, smart cities with smart grids will record when people go to bed at night and when they rise.

The is obviously a growth area for companies producing these connected things. Gartner, a research firm, predicted that the number of wirelessly connected products in existence (not including smartphones or computers) will increase from perhaps 5 billion today to 21 billion by 2020. An IDC report predicts explosive spending on IOT, expanding from US$656bn in 2014 to US$1.7 trillion in 2020.

Some old friends…

When you think of smart cities or power plants, it's natural that security and privacy issues are at the forefront of the minds of Government/regulators (including FTC and EU Commission for whom IoT is not a new issue) – but it's quite possible that antitrust agencies will take an interest before too long.

Looking at IoT market characteristics, there are some familiar factors/issues here from recent high profile antitrust/IP enforcement:

- apparent dependence on the Internet/interoperability/standards (with potential for disputes around disclosure /licensing of SEPs)
- open source versus proprietary models/ecosystems
- direct and indirect network effects
- blurred product markets: improvements to existing products versus new products?
- close interaction (tying?) between physical devices and data analytics
- an instinct to protect valuable datasets through exclusivity or preventing data portability

Aside from market power/foreclosure issues, it is conceivable that agencies might one day want to check whether the interconnection of devices facilitates competitor-competitor contacts (whether direct or through a common 'hub' supplier/customer)? Collaboration between competitors in sharing data from IoT products could may also need some upfront consideration. If the analytics could reveal things about rivals that are competitively sensitive then the usual safeguards of aggregation/use of third parties may be appropriate.

Care also needs to be taken where there is automation/algorithms developing a life of their own. The recent EU case of Eturas (where a systems administrator message risked bringing unwitting recipients into a price-fixing cartel) has notes of this.

So what? Keeping perspective

IoT market characteristics may be familiar to antitrust practitioners – but this doesn't mean that the issues require less thought. Even in the digital context, there is no one size fits all. For example, sometimes closed systems are better for competition than open systems. It's also important to remember that IoT is based on the open standards of the internet so the risk of any proprietary data pool may be less likely than in other sectors.

Even the 'seminal' cases regarding access and foreclosure need a second look. As CMA officials recently emphasised in the context of the ongoing debate regarding platform regulation, the 'essential facilities' doctrine was developed in the context of infrastructure assets that are difficult to replicate. It might be troublesome to transpose concepts applying to ports into the digital world where large fixed costs and large infrastructure requirements may give rise to market power.

As ever, regulatory intervention should only follow an evidence-based assessment of potential adverse effects. Blanket solutions aimed at a sector or practice (e.g. IoT) are certainly to be avoided. To cite the CMA again, there is "no need to reinvent the regulatory wheel". This is particularly important given the risk of inhibiting further welcome innovations by premature or unprincipled regulatory intervention.

In conclusion, it's early days and too early for companies or agencies to be scared into taking action in such a fast-moving area.

But, in the same way that the FTC urged manufacturers of devices to think about security and data privacy principles and hardwire them into their engineering products it might be prudent for companies to at least be aware of the antitrust issues that could be thrown up as they develop their range of IoT devices.