



Commission's sector inquiry into the Internet of Things: an opportunity to develop regulatory clarity at an early stage

Introduction

The European Commission's announcement, on 16 July 2020, of a sector inquiry into the Internet of Things ("IoT"), provides an opportunity for public debate with the European antitrust regulator on how competition is working in the specific context, and, in an ideal world, might be expected to provide clarity to businesses active in IoT projects and their advisers. Such an outcome is not guaranteed, however, for market reasons – the sector itself is evolving rapidly and will continue to evolve during the inquiry - and reasons connected with the conduct of such sector inquiries – namely the breadth and focus of the Commission. Furthermore, the sector inquiry cannot be separated from wider public policy developments in data protection and consumer law and may be part of a much wider regulatory process. Therefore, all those with an interest in IoT – both those who receive Commission questionnaires (who can be required to answer them) and those who do not - will wish to engage early and deeply with the Commission.

The focus and timetable of the Commission's IoT sector inquiry

The Commission will focus on consumer-related products and services in the EU, connected to a network and capable of being controlled at a distance, for



example, by a voice assistant or mobile device. The inquiry covers wearable devices, such as smart watches or fitness trackers, and connected consumer devices used in "smart homes" – fridges, washing machines, smart TVs, smart speakers and lighting systems. It will also include services available through smart devices, such as music and video streaming services as well as the voice assistants which are used to access them.

Voice assistants such as Apple's Siri, Amazon's Alexa and Deutsche Telekom's Magenta, which according to the Commission allow users to "*control smart devices without even having to look at the screen*" are at the heart of the inquiry.

This scope appears to exclude inquiry into the Internet backbone to the IoT, involving among others, telcos and internet service providers, but the outcomes of this sector inquiry may be highly relevant to such players, both because telecoms provides the connectivity layer, and applications depend on



or integrate with telecoms networks and services. For example, a common IoT wearable is a smart watch. This is often used with a smart phone as well as a basic fitness tracker. Health monitors may be built into those devices and applications, and these collect data not only on the functioning of the device itself but also the individual it interacts with.

The Commission's forthcoming information requests to industry – we are told – may be directed, for example, to smart device manufacturers, software developers and "related service providers". We understand that the Commission has already sent out over 400 questionnaires. However, all players in the IoT should take careful note.

The Commission aims to publish a preliminary report on the replies, for consultation, in the spring of 2021, with the final report to follow in summer 2022. This is an aggressive timetable that puts pressure on market participants to make their cases

cases early and clearly, even as the sector is evolving.

Commentary

Inquiry into a sector under rapid evolution

EU sector inquiries are industry-wide probes where there are concerns that markets may not be working as well as they should, but where the problem does not appear to be related to unlawful action by individual companies. This sector inquiry – the ninth the Commission has conducted under Regulation 1/2003 - will be to a notable degree unlike others. Instead of waiting for the IoT to reach some level of maturity, the Commission has decided to launch now. As a result, it will be examining a sector that is changing rapidly while under observation. Indeed, its decision to open the sector inquiry is curious. It records that the sector for consumer IoT-related products and services is already important and expected to grow substantially – from 108 million smart home devices in 2019 to 184 million in 2023. Yet the legal test for opening an inquiry is – as set out in Article 17 of Regulation 1/2003:

“Where the trend to trade between Member States, the rigidity of prices or other circumstances suggest that competition may be restricted or distorted within the internal market, the Commission may decide to conduct an inquiry into a particular sector of the economy or into a particular type of agreements across various sectors.”

This is a low threshold for

beginning a sector inquiry, and in response to this, the Commission argues (in its decision opening the inquiry) that:

“Despite its relatively early stage of development, the sector for consumer IoTs related products and services in the Union, there are indications of company behaviour conducive to structurally distorting competition in and for this sector. In particular, there are indications of contractual and de facto restrictions of data access and interoperability, the emergence of digital ecosystems and gatekeepers, as well as certain forms of self-preferencing and practices linked to the use of proprietary standards that could represent barriers to entry and innovation, and could lead to restrictions of market access for competitors, thereby restricting and/or distorting competition in the sector.”

None of these identified issues – data access and interoperability, gatekeepers, self-preferencing and standardisation - is novel and the Commission is confident that its enforcement and decisional practice give it the analytical tools appropriate to these newer developments.

In acting quickly, the Commission may prevent a repeat of past accusations that in the past it has been too slow to act in technology markets. But there is an equal and opposite danger in acting precipitously, that the problem under investigation is not defined with adequate clarity, and any solutions may be unworkable or impractical.

Focus on data

Unsurprisingly, given recent enforcement practice as well as the nature of the IoT – is the focus on data collection and use. Such data may be personal data or non-personal data, and the Commission notes that access to these data may be *“an important contributing factor to market power both in the sector for consumer IoTs related products and services, and the competitive structures thereof.”*

The Commission notes that the enormous volumes of data already flowing through consumer IoT products and services allows businesses to observe consumer habits and predict behaviour. It is a key input to developing AI. Those with access to data can better compete in AI-driven markets.

For personal data, the sector inquiry marks an important step in the growing convergence of competition considerations and privacy/data protection, which already finds form in regulators’ actions – note, for example, the ongoing legal battle in Germany between Facebook and the Bundeskartellamt over whether an infringement of data protection law by a dominant company could be and was an abuse of dominance. Note, also, the recent debate between Google and the Commission over the former’s proposed acquisition of Fitbit. On 14 July Google reportedly offered not to use Fitbit’s user data to inform its advertising business. The Commission will test the robustness of such remedies as part of its merger review, which it says is unrelated to the sector inquiry. Not only is the

Commission taking particular interest in the consumer data aspect of the deal; but also the European Data Protection Board (“EDPB”) requested, in February this year, that the merging parties conduct a privacy impact assessment before notifying the deal. This is the first time the EDPB has intervened in a such a case.

Relation with antitrust enforcement and digital markets policy development

The Commission’s sector inquiry page states that the Commission *“may – at a later stage – assess whether it needs to open specific investigations to ensure the respect of EU rules on restrictive agreements and abuse of dominant position.”* This is repeated in the Commission’s press release opening the inquiry: *“If, after analysing the results, the Commission identified specific competition concerns, it could open case investigations...”*

Previous sector inquiries have led to a number of investigations into specific companies. The Commission launched probes into geo-blocking following its 2017 e-commerce sector inquiry, which also prompted EU legislation to ban unjustified geo-blocking.

The sector inquiry cannot be separated from ongoing investigations such as Google/Fitbit (albeit in the mergers rather than antitrust field), nor does a sector inquiry formally prevent the Commission opening enforcement cases earlier. It is clear there is parallel policy-making, enforcement and inquiry work. Note, here, the recent and

and controversial announcement of (and consultation on) a proposed “New Competition Tool” – the outcome of its 2019 report on competition policy for the digital era – whereby antitrust enforcement in digital markets will be complemented by possible ex-ante regulation of digital platforms, including requirements for those with a “gatekeeper” role and the proposed tool which would aim to deal with structural competition problems across markets (e.g. tipping markets) which cannot be tackled or addressed in the most effective manner by current competition rules.

Consumer protection

There is a broader consumer protection agenda in play and the European Commission is not the only regulator to take an interest. National regulators – such as the Bundeskartellamt mentioned above – have also got involved.

In the UK, the Department of Culture, Media and Sport in January this year proposed new rules to protect consumers of IoT devices – first, by requiring internet-connected device passwords to be unique and not resettable to any universal factory setting; second, that manufacturers of consumer IoT devices must provide a public point of contact to enable vulnerabilities to be reported and acted on in a timely way; and thirdly, manufacturers of IoT devices must explicitly state the minimum length of time for which the device will receive security updates at the point of sale, either in store or online.

Although antitrust law and the tools of enforcement must be applied to changing circumstances, in particular, digital economies, this is a reminder that antitrust is part of a broader set of societal rules designed to protect consumers, and these rules may increasingly converge, as noted above for data protection.

The fact that new technology such as the IoT may present new or enhanced risks to consumers does not, of itself, necessitate a specific policy or legislative response. For example, it may be concluded that ongoing reform initiatives that are not specific to the technology or existing laws and regulations are sufficiently adaptable to deal with the challenges presented. For example, in 2015 the Alliance for Internet of Things Innovation concluded that - while IoT products presented special considerations for product liability and insurance - there was no need for new regulation or legislation. However, with rapid technology development in the IoT world, existing product liability laws - first adopted in the EU over three decades ago and always a work-in-progress – may need further revision to be workable.

It will be important to understand how antitrust practice towards the consumer IoT develops alongside other aspects of consumer protection law, including product liability and product safety law, particularly since the lack of international harmonisation across these fields is likely to create a patchwork of standards and rules.

Conclusion and practical steps

Promoters of IoT projects offer enormous benefits to consumers and society. IoT devices are proliferating, IoT projects are becoming more complex and spanning both public and private fields, and the vast acquisition of consumer data is contributing to the development of AI and predictive technology. These developments have raised antitrust, data protection and consumer concerns. The Commission's IoT sector inquiry is engaged in understanding the first of these, but policy-makers will not ignore the other two.

At this stage the following are some key issues for companies and their advisers to consider:

- **Resource commitments:** engaging with a sector inquiry and dealing with any follow-up action tends to involve the commitment of considerable resources; assess how to present the business' case effectively.
- **Questionnaires:** consider whether business documents could be misinterpreted and how best to defend them; consider how these responses may shape the authority's thinking.
- **Consistency:** note that information may be exchanged between Member States of the EU; consistency of message and positioning

is vital.

- **Third party complaints:** third party complaints will need to be addressed; anticipate how third parties (consumers, customers, suppliers and competitors) may be concerned about industry practices and how best to address those concerns.

- **Strategy:** there is no 'one size fits all' strategy that will be appropriate for all businesses affected. At the outset, a 'wait and see' approach may be justified until the shape and direction of the inquiry develops but this carries the risk that the later a company engages with an inquiry the more limited the prospects for influencing more fundamental issues such as the overall scope and key issues to be examined.

- **Opportunities:** consider whether there are any business-specific messages to get across or potential to work with trade bodies to improve the profile of the industry.

Consequently, stakeholders in this inquiry should – as stated above – engage early and deeply, taking into account this broader context. Although the precise form and scope of the Commission's inquiry is unclear at this stage, smart device and applications providers, telcos and related entities should

consider the possible competition issues arising, where their interests lie and what strategic direction they might adopt.

Professor Suzanne Rab
Barrister, Serle Court

Jeremy Robinson
Watson Farley & Williams

This article was prepared jointly with Jeremy Robinson of Watson Farley & Williams.