Your World First

C/M/S/ Law . Tax

Artificial Intelligence

Could a software developer be deemed a cartel facilitator?

Competition authorities are concerned about the use of AI software to implement anti-competitive arrangements. It is foreseeable that an AI software developer is drawn into a future cartel investigation. Indeed, one software provider already has skirted with the possibility of enforcement by the Competition and Markets Authority (CMA), having purportedly facilitated a price-fixing agreement through the online re-pricing software they provided to their clients. This article considers what (nearly) happened in this case, how an AI software developer might be found to have facilitated a cartel and what steps could be taken by developers prior to or during an engagement to address this risk?.

The perils of cartels

Cartel facilitation is not a new concept. It is where an organisation, including one not active in the market concerned, knowingly contributes to the implementation of an anti-competitive agreement.

It can bring within its scope parties such as trade associations or manufacturers who facilitate a cartel between competing resellers of their products. Third party consultants, independent brokers and advisers can also be implicated.

For third parties operating outside of the market, an allegation of cartel facilitation presents the worst of both worlds - finding yourself locked in a costly investigation (and possibly being sanctioned for your role) despite not benefitting from the cartel itself.

The one that got away?

In the CMA's Online sales of posters and frames case, resellers Trod and GB eye agreed that they would not undercut each other's prices for posters and frames sold on Amazon's UK website. The CMA imposed fines on Trod, while GB eye received immunity for reporting the cartel arrangement to the CMA.

The CMA found that, after a short period of trying to implement their anticompetitive arrangement manually, GB eye used automated repricing software (developed by a third party), which was configured to give effect to the arrangement. Trod followed suit with its own pricing software.

While Trod and GB eye were clearly direct participants in the cartel, it appears that the software developer may have also been involved in discussions about the parties' underlying goals and may therefore have facilitated the agreement between Trod and GB eye). In its published decision, the CMA did not rule out that an offence had been committed by the software provider, but decided that opening a separate line of investigation was not a priority.

There is no guarantee that, should a future case present itself or should such software become more prevalent, the CMA's assessment would not lead it to open a formal investigation. Indeed, the CMA has always demonstrated an appetite for novel cases. Furthermore, in 2018, the CMA appointed a new Chief Data and Digital Insights Officer to help the CMA better understand 'how firms use data and algorithms in their business models and what implications this might have for competition and consumers'. Therefore, the authority appears to have specifically tooled up for such an investigation.

How might an AI software developer end up facilitating a cartel?

An authority must establish at least three elements to show that a software developer facilitated a cartel:

- First, the software developer had some knowledge of (or should have reasonably foreseen) the existence of the anti-competitive arrangement. This does not require actual knowledge. Being in a position where you ought to have inferred the existence of collusion is sufficient.
- Second, the software developer contributed to the common objectives pursued by the colluding parties, i.e. the services were not merely peripheral. The more central the role, the more likely this element will be met. If the AI software is the means through which the anti-competitive end is being achieved – this ought to be easily met.
- Third, the software developer must have either intended to make such a contribution or should reasonably have foreseen its participation would have that effect and the developer was prepared to take the risk. Again, there is an alternate objective test where intention can be imputed. In other words, a see no evil, hear no evil approach will not be an adequate defence.

Where the above elements are in place, clearly there is a greater risk to the software developer that enforcement action will be taken against it.

What steps can be taken?

At a minimum, we would suggest the following five steps to address the risk of being inadvertently implicated in a cartel arrangement:

1. First and foremost, ignorance is no defence when it comes to cartel facilitation. So step one is to ensure that key development staff and client facing sales teams have some basic understanding of competition law. They need to be able to sniff out instructions that present a risk to the business.
2. For each client engagement, consider the context and risks at hand. For example, are you being jointly instructed by two or more competitors in the market? Are you being asked to liaise with a third party developer representing another market player? Does the software involve data being supplied by third parties and what are their roles in the marketplace?
3. Where a risk does present itself, a process will be required to report such instances up to senior management or a compliance officer. Such a scenario will require delicate client-handling. The process will need to establish whether the project presents a material risk, and a considered judgment weighing up the risks may prove necessary.
4. Where a decision is taken to proceed (i.e. the risk is manageable), set clear parameters for the project and for future discussions between development staff and the client. Where the service will be of a continuing nature, or where there are material changes to the brief, staff ought be alert to potentially problematic changes.
5. Explore the use of contractual protections and clear representations from the clients as to any raw data sources and the installation or use of the software. Note that an indemnity may prove ineffective due to the application of a legal doctrine preventing a party from claiming damages for a loss which has arisen as a result of their own wrongful act and from a public policy perspective.

The above measures should provide some comfort to software developers that their projects are not likely to result in enforcement action against them, with all of the costs and reputational implications that can bring.

The next test case?

In the CMA's first case involving online automated pricing software, the CMA decided not to proceed with its enforcement action against the software developers – despite it being found to have played some role in facilitating the underlying anti-competitive arrangement. The CMA has since appointed staff with specific capabilities in establishing such offences. Avoiding being the CMA's next 'test case' ought to be in the back of all software developers' minds.

Contacts

Kabir Garyali
Senior Associate
T +44 20 7524 6579
E kabir.garyali@cms-cmno.com

Further information, including a list of our offices, can be found at **cms.law**