

Transcending the Cloud

**A Legal Guide to the Risks and Rewards
of Cloud Computing**

Tying Up the Cloud:
A Study in Antitrust Issues
in Cloud Computing

ReedSmith

reedsmith.com



Tying Up the Cloud: A Study in Antitrust Issues in Cloud Computing

Chapter Author

[Jeremy D. Feinstein](mailto:jfeinstein@reedsmith.com), Partner – jfeinstein@reedsmith.com

The cloud computing era represents a significant shift in relationships in the information technology field. This shift will raise many antitrust questions, among other legal issues. Many antitrust questions will not become apparent until cloud computing business models become better established, but some issues are readily apparent even at the threshold. For instance:

- After a customer selects a particular cloud provider, can the customer be “locked in” to particular products and services within that cloud?
- When will a cloud provider be permitted to exclude other service providers or software providers from participating in a cloud?

This article provides some preliminary thoughts on these questions and considerations that should be taken into account by organizations providing and considering purchasing cloud computing services. Although definitive answers to these questions always require a specific factual context, the discussion below identifies some fundamental antitrust principles that apply and may help prospective cloud purchasers understand their rights and avoid potential traps by negotiating prudent contract terms when entering into a cloud computing arrangement. The key for prospective cloud purchasers (*i.e.*, users of cloud computing services) is to obtain complete and accurate disclosures of a cloud provider’s after-market policies *prior* to the initial decision to enter the cloud. After the initial purchase of cloud computing services, customers may find that their bargaining power is dramatically reduced by switching, compatibility, interoperability or even early termination costs.

A Starting Point: Power in the Cloud Services Market

Antitrust questions that are raised, and the range of possible answers that should be considered, will depend in significant part on (a) the definition of the “relevant market” in which a given cloud provider competes and (b) the determination whether the cloud provider has the ability to influence prices or output in that market as a whole—an ability referred to as “market power.” A relevant market encompasses all products that prospective purchasers in a particular geographic area would consider reasonable substitutes for each other. The relevant market includes not just existing substitutes, but also those that might enter the market within a relatively short time in response to a sustained rise in prices. Antitrust law places many more limitations on the activities of companies deemed to have power within a relevant market than on the activities of companies that lack such power.¹

Application of these basic antitrust concepts suggests that, at least at this very early stage in the development of cloud computing, it would be very challenging to prove that a cloud provider had “market power” in a putative market for the sale of cloud computing services. First, the market is arguably worldwide: the very idea of portable cloud services implies that a cloud provider in Canada could compete with a cloud provider in Australia for customers in the United States. Second, at least for now, the relevant market arguably cannot be limited to the provision of “cloud computing services” alone because for most companies and most business purposes “old fashioned” hardware and software systems and third party hosting arrangements, though lacking many of the benefits afforded by cloud computing, still remain reasonable substitutes for clouds. Third, the number of potential new entrants into the

hypothetical market for cloud computing services is still uncertain, and could prove to be very large.² Cumulatively, these factors suggest that until cloud computing develops a bit further, the provision of cloud services will be a market with many actual and potential competitors, reducing the chances of particular providers attaining real market power.

One possible exception to this could be hypothetical future clouds that are explicitly focused on delivering products or services already powerful in their fields, such as clouds for Apple iTunes, Microsoft Office, or the Google search engine. These cloud scenarios may not remain hypothetical for long.³ Enterprising plaintiffs might assert that the cloud providers have market power in putative markets for the provision of these specific cloud services, just as they might assert such power independent of the cloud context. But even for distinctive examples like these, it is not clear that the cloud context will change the power analysis much from the pre-cloud era, and in fact the cloud context may be dilutive: a new spreadsheet program seeking to compete with Excel, for example, might have an easier time doing so “in the clouds” than it would have in the past, where placement on “traditional” desktop and laptop hardware was a prerequisite for entry.

After-Market Analysis: Power Within A Cloud

A more likely scenario in which cloud providers may face credible near-term allegations of market power is in “after-markets” for products and services within their own clouds. The antitrust concept at work here is that there could be separate markets for the “provision of cloud computing capabilities” and the “provision of services or software products within a cloud.” A cloud computing vendor might face substantial competition from other clouds in a “primary market” where the customer chooses among various cloud providers, while at the same time facing little or no competition in “after-markets” for selling particular services to customers already in its cloud.

The possibility of cloud service providers exerting power within their clouds is certainly not limited to services involving already well-established brand names. Cloud computing customers may come to value or require any number of after-market services in their clouds, and cloud providers may attempt to dictate or limit customer choices with respect to such services. For instance, a cloud provider might insist that any cloud customer utilizing its data storage services also purchase and utilize the provider’s own proprietary virus detection software. Would such a limitation injure the cloud customers, or other

potential vendors of virus detection software, in a way that the antitrust laws might redress?

The well-known Supreme Court case of *Eastman Kodak Co. v. Image Technical Services*, 504 U.S. 451 (1992), is the most authoritative example of after-market antitrust analysis, and the principles it articulated remain highly instructive. *Eastman Kodak* is worth considering in detail because it provides a virtual checklist of potential after-market risks that companies purchasing cloud computing services should be mindful of when they choose a vendor.

When Is An After-Market A Relevant Market? Lock-ins, switching costs, and information barriers.

In *Eastman Kodak*, the plaintiffs were a group of independent servicers (ISOs) of sophisticated copiers made by Kodak. Kodak faced strong competition and lacked market power in the primary market for the sale of copiers. At the same time, Kodak faced only no competition in the after-market for the sale of replacement parts for Kodak copiers (which parts were only available from Kodak or its licensees) and only modest competition from the ISOs for the sale of repair services. When Kodak attempted to further increase its share of the services after-market by selling replacement parts only to customers who also purchased repair services from Kodak, the ISOs sued Kodak under monopolization and tying theories.

The Supreme Court held that the ISOs’ proposed relevant after-market for the servicing of Kodak copiers was sufficient to survive summary judgment. The Court emphasized that the determination of the relevant market must be made from the perspective of a consumer (here, the purchasers of Kodak copiers), and should include only those products or services that consumers view as interchangeable.

Kodak argued that there was no true distinction between the primary market for copiers and the alleged after-markets for parts and services. Kodak’s theory was that consumers could engage in “lifecycle pricing” analysis, and thus the costs of its parts and services policies would inform the consumer’s primary purchase decision of what copier to buy. Consequently, Kodak contended that its lack of power in the primary product market should end the issue as a matter of law.

The Supreme Court did not find this persuasive. It concluded instead that Kodak’s theory, “although perhaps intuitively appealing, may not accurately explain the behavior of the primary and derivative markets for complex

“durable goods” because of information barriers and switching costs. The Court observed that the information needed to engage in lifecycle pricing of Kodak copiers was difficult or impossible to acquire at the time of purchase, and in any event was subject to change during the lifespan of the copier. Thus, the court viewed the initial purchase decision as separate from subsequent decisions to purchase parts or servicing.

Once a customer had made the substantial capital investment in purchasing a Kodak copier, the cost of switching to another copier would be quite high. Thus, Kodak customers were effectively “locked-in” to the parts and servicing prices (and price increases) imposed by Kodak. The Court concluded that “the relevant [service] market from the Kodak equipment owner’s perspective is composed only of those companies that service Kodak machines,” and that the ISOs were therefore entitled to a trial on the question of whether Kodak abused its power in that market.

Lessons of Eastman Kodak

Eastman Kodak teaches several valuable lessons for prospective purchasers of cloud services who wish to protect their interests (and to do so with less cost than a protracted antitrust suit). First, the switching costs for corporate customers who purchase cloud service are likely to be substantial, and every prospective purchaser should carefully evaluate whether these costs will be high enough to effectively create a “lock-in” with their cloud provider. For example, customers should consider:

- Whether the cloud offers specialized software or services that, once adopted by the customer, would be difficult to obtain from another source
- How large an investment of time and money will be required to train employees to use the cloud’s user interface and software
- How quickly and at what cost could data stored in the cloud be retrieved and placed in another cloud or on the customer’s own storage systems
- What data security concerns would be implicated and what notifications might be required if the company later decided to move its data to a different cloud

Second, if switching costs will be high enough to create a lock-in effect once a particular cloud is selected, prospective purchasers need to obtain as much information as they can *before* they purchase cloud services about how the cloud service provider will handle after-market services.

Prospective purchasers should press a cloud service provider, at a minimum, to:

- Identify all software/services that are or might be included in the price of cloud services
- Explain its policies regarding customers’ right to disaggregate services that it does not want
- Identify any software/services that are mandatory
- Explain its policies regarding customers’ rights to add or substitute the software/services of providers of their own choosing, including providers who may provide software or service competing directly with software/services of the cloud provider
- Explain its policies regarding future price changes (and perhaps whether a long-term price agreement is available, if that is otherwise in the business interest of the customer)

A customer that takes these steps may reduce its chances of being taken advantage of in after-markets for cloud services.

Addressing Misconduct In After-Markets

What if the prophylactic steps described above fail, and a cloud provider adopts policies in after-markets that its existing customers dislike or that exclude competitors? Litigation based on *Eastman Kodak*-type theories would be an option for customers, as well as for potentially competitive service providers in cloud services after-markets who believe, like the ISOs in *Eastman Kodak*, that they are being harmed. In such a setting, a plaintiff would need to claim that the cloud provider’s conduct unreasonably impaired competition in a relevant market in some fashion, not just that it injured the plaintiff in particular.

There are many antitrust theories that an after-market plaintiff might employ, of course, but two of the most likely would be tying claims and exclusive dealing claims. A full discussion of how these theories might apply to cloud computing fact patterns would be premature, but set forth below are a few preliminary thoughts on each.

Tying in after-markets

To bring a tying claim, a plaintiff must show that there are two separate products, that the defendant has “tied” them by conditioning the sale of one on the purchase of the other, and that the defendant has market power in the tying product. *See generally Jefferson Parish Hospital Dist.*

No. 2 v. Hyde, 466 U.S. 2 (1984). Tying claims are a natural fit for after-markets, where the seller of the primary product often has a large share of after-market products and services, too. In the *Eastman Kodak* case, Kodak allegedly tied the sale of replacement parts to the concurrent purchase of Kodak's repair services, which allegedly had the effect of preventing customers from dealing with the plaintiff ISOs.

As already noted, a similar scenario could arise in the cloud context if a cloud provider insisted that it would only sell its data storage services to those of its cloud customers who also purchase the provider's own proprietary virus detection software. A cloud provider would have a much better chance of defending such a policy if it were disclosed to customers prior to their entry into the cloud—with such facts, a cloud provider might be able to convince a court that the virus detection software was not "tied" to anything but was simply part of the original package of services that the customer knowingly chose to purchase. If this policy were adopted after customers were already "locked-in" to the cloud, however, the analysis might proceed in a manner similar to *Eastman Kodak*. That is, if the cloud provider were deemed to have market power in the after-market for the sale of data storage service within its own cloud, conditioning the sale of that service on the purchase of other products or services might expose the provider to an antitrust trial in which the anticompetitive injuries (if any) caused by this policy would be evaluated.⁴

Exclusive dealing in after-markets

Exclusive deals between cloud providers and particular product or service vendors are also a foreseeable source of conflict. Suppose our hypothetical were altered slightly, and instead of tying distinct products together, a cloud provider announced to existing locked-in customers that it had reached an agreement with another firm (say, Symantec) to be the exclusive virus detection software vendor for the cloud. Cloud customers need not purchase Symantec's software at all, but if they want to deploy virus detection software in the cloud, it must be Symantec's. Would cloud customers or competing virus detection software vendors have an antitrust claim based on this new policy?

Exclusive dealing agreements are frequently lawful, but they can violate antitrust laws if they foreclose competitors' access to a substantial share—some courts have suggested 40 percent is in the right ballpark—of the relevant market for their products. This suggests that

Symantec's competitors would be unlikely to have a viable claim based on the facts above. No single cloud, at least in the near term, could come close to containing such a large share of the market for the sale of virus detection software.

As to the cloud customers, a threshold question, again, is whether the exclusivity was pre-announced. If IBM offers cloud services and announces from the outset that only IBM software products will be permitted in the cloud, it would be difficult to understand a subsequent claim by a customer that they were harmed by this exclusivity policy. A customer that wants to use Microsoft software should pick a different cloud. If the cloud vendor had reserved a contractual right to control software within the cloud, similar logic might apply. But if cloud customers are already "locked in" and are taken by surprise by an exclusive deal, the analysis might be different. Much like the copier purchasers in *Eastman Kodak*, for a locked-in cloud customer, competition in the relevant after-markets for cloud services consists of the products and services that the cloud provider allows to operate in the cloud. If the cloud provider reached an agreement to exclude competition in those markets, the locked-in customers might have a plausible claim for antitrust injuries (higher prices, reduced quality) resulting from the deal.

Conclusion

Prospective cloud services purchasers need to protect themselves by seeking complete and accurate disclosures of a cloud provider's after-market policies *prior* to the initial decision to enter the cloud—or to contract with a particular provider. Ideally, purchasers who anticipate a lock-in effect, similar to long term outsourcing contracts, should negotiate for terms that limit the ability of the cloud provider to change the rules of the cloud service offerings and pricing in the middle of the contract term. After the initial purchase of cloud computing services, customers may find that their bargaining power is dramatically reduced by the switching costs they may need to incur to both get out of the existing relationship and migrating to a new one—whether in whole or in part. Although many aspects of the cloud computing industry and its players are still in their infancy in terms of technology and economic models, the well-established principles of antitrust law that are increasingly being enforced by governments around the world still very much apply and will likely have a decisive role in how the industry ultimately unfolds both in the short and long term.

— Biography of Author —



[Jeremy D. Feinstein](#), Partner – Pittsburgh +1 412 288 7972 · jfeinstein@reedsmith.com

Jeremy is a trial lawyer with a focus on antitrust, RICO, unfair competition, business tort, and civil class action matters. He has handled major matters, both civil and criminal, for health insurance companies, financial services corporations, long-term care facilities, medical device manufacturers, and universities. His trial experience includes cases concerning monopolization, tying, and predatory pricing, lender liability, food safety, foster care and election law. He was named a “Pennsylvania Rising Star” by *Pennsylvania Super Lawyers* in 2006.

— Cloud Computing Task Force Leader —



Joseph I. Rosenbaum
Partner and Chair, Advertising Technology & Media Law Group
rosenbaum@reedsmith.com
+1 212 702 1303

— Endnotes —

- ¹ See generally, *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 602-03 (1985) (discussing market definition and power). A few types of inherently anticompetitive conduct, such as price fixing or agreements to divide markets, are treated as illegal “per se,” meaning that they are illegal regardless of any showing of possession of market power in a relevant market by the participants. The conduct discussed in this paper, however, is unlikely to be viewed as illegal per se, and instead will be analyzed under the Rule of Reason, in which the competitive effects of the conduct on customers and participants in the relevant market are considered.
- ² The primary requirement for entry appears to be substantial available processing capacity. Phone companies, cable companies, universities and other such entities that typically have enormous computer processing capabilities all might be characterized, at least for now, as potential entrants into the market for provision of cloud services.
- ³ See, e.g., *Office Heads Into The Clouds: Microsoft Releases New Software Amid Cheap Online Alternative From Google*, WALL ST. JOURNAL, May 13, 2010, at B7; *The Digital Download Is Dead*, SLATE MAGAZINE, May 21, 2010, <http://www.slate.com/id/2254532/> (discussing theoretical competition between a future iTunes cloud and a Google/Android cloud music service).
- ⁴ This analysis assumes that data storage and virus protection software are separate products for antitrust purposes (*i.e.* that consumers at least sometimes demand one without the other).