"Upon closer examination, data-opolies can actually be more *dangerous than traditional monopolies. They can affect not only our wallets but our privacy, autonomy, democracy, and well-being."*

Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data

TECHNOLOGY & OPERATIONS | DIGITAL ARTICLE

Updating the definition of monopoly for our digital age.

Bold underlining for emphasis added by Bill Densmore

By Maurice E. Stucke
mstucke@utk.edu | 865-974-9816
Harvard Business Review | ©Harvard Business Publishing
Posted Online: MARCH 27, 2018

Maurice E. Stucke is a co-founder of The Konkurrenz Group and a law professor at the University of Tennessee. AB, 1987, Georgetown University | JD *magna cum laude*, 1994, Georgetown University. See additional article citations. A former trial attorney at the U.S. Department of Justice, Antitrust Division, he has co-authored two books, *Big Data and Competition Policy* (Oxford University Press 2016) and *Virtual Competition* (Harvard University Press 2016). His research on the digital economy has been featured in *The Economist*, *Guardian*, *Harvard Business Review*, *New York Review of Books*, *New Yorker*, *New York Times*, *Science*, *Times Higher Education*, *Wall Street Journal*, Wharton Business Radio, and *Wired*.

"It's no good fighting an election campaign on the facts," Cambridge Analytica's managing director told an undercover reporter, "because actually it's all about emotion." To target U.S. voters and appeal to their hopes, neuroses, and fears, the political consulting firm needed to train its algorithm to predict and map personality traits. That required lots of personal data. So, to build these psychographic profiles, Cambridge Analytica enlisted a Cambridge University professor, whose app collected data on about 50 million Facebook users and their friends. Facebook, at that time, allowed app developers to collect this personal data. Facebook argued that Cambridge Analytica and the professor violated its data polices. But this was not the first time its policies were violated. Nor is it likely to be the last.

This scandal came on the heels of Russia's using Facebook, Google, and Twitter "to sow discord in the U.S. political system, including the 2016 U.S. presidential election." It heightened concerns over today's tech giants and the influence they have.

That influence comes in part from data. **Facebook, Google, Amazon, and similar companies are "data-opolies." By that I mean companies that control a key platform which, like a coral reef, attracts to its ecosystem users, sellers, advertisers, software developers, apps, and accessory makers.** Apple and Google, for example, each control a popular mobile phone operating system platform (and key apps on that platform), Amazon controls the largest online merchant platform, and Facebook controls the largest social network platform. Through their leading platforms, a significant *volume* and *variety* of personal data flows. The *velocity* in acquiring and exploiting this personal data can help these companies obtain significant market power.

Is it OK for a few firms to possess so much data and thereby wield so much power? In the U.S., at least, antitrust officials so far seem ambivalent about these data-opolies. They're free, the thinking goes, so what's the harm? But that reasoning is misguided. Data-opolies pose tremendous risks, for consumers, workers, competition, and the overall health of our democracy. Here's why.

Why U.S. Antitrust Isn't Worried About Data-opolies

The European competition authorities have recently brought actions against four data-opolies: Google, Apple, Facebook, and Amazon (or GAFA for short). The European Commission, for example, fined Google a record €2.42 billion for leveraging its monopoly in search to advance its comparative shopping service. The Commission also preliminarily found Google to have abused its dominant position with both its Android mobile operating system and with AdSense. **Facebook, Germany's competition agency preliminarily found, abused its dominant position "by making the use of its social network conditional on its being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account."**

We will likely see more fines and other remedies in the next few years from the Europeans. But in the U.S., the data-opolies have largely escaped antitrust scrutiny, under both the Obama and Bush administrations. Notably, while the European Commission found Google's search bias to be anticompetitive, the U.S. Federal Trade Commission did not. From 2000 onward, the Department of Justice brought only one monopolization case in total, against anyone. (In contrast, the DOJ, between 1970 and 1972, brought 39 civil and 3 criminal cases against monopolies and oligopolies.)

The current head of the DOJ's Antitrust Division recognized the enforcement gap between the U.S. and Europe. He noted his agency's "particular concerns in digital markets." But absent "demonstrable harm to competition and consumers," the DOJ is "reluctant to impose special duties on digital platforms, out of [its] concern that special duties might stifle the very innovation that has created dynamic competition for the benefit of consumers."

So, the divergence in antitrust enforcement may reflect differences over these data-opolies' perceived harms**. Ordinarily the harm from monopolies are higher prices, less output, or reduced quality. It superficially appears that data-opolies pose little, if any risk, of these harms**. Unlike some pharmaceuticals, data-opolies do not charge consumers exorbitant prices. Most of Google's and Facebook's consumer products are ostensibly "free." The data-opolies' scale can also mean higher quality products. The more people use a particular search engine, the more the search engine's algorithm can learn users' preferences, the more relevant the search results will likely be, which in turn will likely attract others to the search engine, and the positive feedback continues.

As Robert Bork argued, there "is no coherent case for monopolization because a search engine, like Google, is free to consumers and they can switch to an alternative search engine with a click."

How Data-opolies Harm in Eight Potential Ways

But higher prices are not the only way for powerful companies to harm their consumers or the rest of society. Upon closer examination, data-opolies can pose at least eight potential harms.

Lower-quality products with less privacy. Companies, antitrust authorities increasingly recognize, can compete on privacy and protecting data. But without competition, data-opolies face less pressure. They can depress privacy protection *below* competitive levels and collect personal data *above* competitive levels. The collection of too much personal data can be the equivalent of charging an excessive price.

Data-opolies can also fail to disclose *what* data they collect and *how* they will use the data. They face little competitive pressure to change their opaque privacy policies. Even if a data-opoly improves its privacy statement, so what? The current notice-and-consent regime is meaningless when there are no viable competitive alternatives and the bargaining power is so unequal.

Surveillance and security risks. In a monopolized market, personal data is concentrated in a few firms. Consumers have limited outside options that offer better privacy protection. This raises additional risks, including:

- **Government capture.** The fewer the number of firms controlling the personal data, the greater the potential risk that a government will "capture" the firm. Companies need things from government; governments often want access to data. **When there are only a few firms, this can increase the likelihood of companies secretly cooperating with the government to provide access to data. China, for example, relies on its data-opolies to better monitor its population.**
- **Covert surveillance.** Even if the government cannot capture a data-opoly, its rich data-trove increases a government's incentive to circumvent the data-opoly's privacy protections to tap into the personal data. Even if the government can't strike a deal to access the data directly, it may be able to do so covertly.
- **Implications of a data policy violation/security breach.** Data-opolies have greater incentives to prevent a breach than do typical firms. **But with more personal data concentrated in fewer companies, hackers, marketers, political consultants, among others, have even greater incentives to find ways to circumvent or breach the dominant firm's security measures.** The concentration of data means that if one of them is breached, the harm done could be orders of magnitude greater than with a normal company. While consumers may be outraged, a dominant firm has less reason to worry of consumers' switching to rivals.

Wealth transfer to data-opolies. Even when their products and services are ostensibly "free," data-opolies can extract significant wealth in several ways that they otherwise couldn't in a competitive market:

- First, data-opolies can extract wealth by getting personal data without having to pay for the data's fair market value. **The personal data collected may be worth far more than the cost of providing the "free" service.** The fact that the service is "free" does not mean we are fairly compensated for our data. Thus, data-opolies have a strong economic incentive to maintain the status quo, in which users, as the MIT Technology Review put it, "have little idea how much personal data they have provided, how it is used, and what it is worth." If the public knew, and if they had viable alternatives, they might hold out for compensation.
- Second, something similar can happen but with the content users create. Data-opolies can extract wealth by getting creative content from users for free. **In a competitive market, users could conceivably demand compensation not only for their data but also their contributions to YouTube and Facebook. With no viable alternatives, they cannot.**
- Third, data-opolies can extract wealth from sellers upstream. One example is when data-opolies scrape valuable content from photographers, authors, musicians, and other websites and post it on their own platform. In this case, the wealth of the data-opolies comes at the expense of other businesses in their value chain.
- Fourth, data-opolies can extract our wealth indirectly, when their higher advertising fees are passed along in the prices for the advertised goods and services. If the data-opolies faced more competitors for their advertising services, ads could cost even less — and therefore so might the products being advertised.
- Finally, data-opolies can extract wealth from both sellers upstream and consumers downstream by facilitating or engaging in "behavioral discrimination," a form of price discrimination based on

past behavior — like, say, your internet browsing. They can use the personal data to get people to buy things they did not necessarily want at the highest price they are willing to pay.

As data-opolies expand their platforms to digital personal assistants, the Internet of Things, and smart technologies, the concern is that their data advantage will increase their competitive advantage and market power. As a result, the data-opolies' monopoly profits will likely increase, at our expense.

Loss of trust. Market economies rely on trust. For online markets to deliver their benefits, people must trust firms and their use of the personal data. But as technology evolves and more personal data is collected, we are increasingly aware that a few powerful firms are using our personal information for their own benefit, not ours. When data-opolies degrade privacy protections below competitive levels, some consumers will choose not "to share their data, to limit their data sharing with companies, or even to lie when providing information," as the UK's Competition and Markets Authority put it. Consumers may forgo the data-opolies' services, which they otherwise would have used if privacy competition were robust. This loss would represent what economists call a deadweight welfare loss. **In other words, as distrust increases, society overall becomes worse off.**

Significant costs on third parties. Additionally, data-opolies that control a key platform, like a mobile phone operating system, can cheaply exclude rivals by:

- steering users and advertisers to their own products and services to the detriment of rival sellers on the platform (and contrary to consumers' wishes)
- degrading an independent app's functionality
- reducing traffic to an independent app by making it harder to find on its search engine or app store

Data-opolies can also impose costs on companies seeking to protect our privacy interests. My book with Ariel Ezrachi, *Virtual Competition*, discusses, for example, Google's kicking the privacy app Disconnect out of its Android app store.

Less innovation in markets dominated by data-opolies. Data-opolies can chill innovation with a weapon that earlier monopolies lacked. Allen Grunes and I call it the "now-casting radar." Our book *Big Data and Competition Policy* explores how some platforms have a relative advantage in accessing and analyzing data to discern consumer trends well before others. Data-opolies can use their relative advantage to see what products or services are becoming more popular. With their now-casting radar, data-opolies can acquire or squelch these nascent competitive threats.

Social and moral concerns. Historically, antitrust has also been concerned with how monopolies can hinder individual autonomy. **Data-opolies can also hurt individual autonomy**. To start with, they can direct (and limit) opportunities for startups that subsist on their super-platform. This includes third-party sellers that rely on Amazon's platform to reach consumers, newspapers and journalists that depend on Facebook and Google to reach younger readers, and, as the European Commission's Google Shopping Case explores, companies that depend on traffic from Google's search engine.

But the autonomy concerns go beyond the constellation of app developers, sellers, journalists, musicians, writers, photographers, and artists dependent on the data-opoly to reach users. Every individual's autonomy is at stake. In January, the hedge fund Jana Partners joined the California State Teachers' Retirement pension fund to demand that Apple do more to address the effects of its devices on children. As The Economist noted, "You know you are in trouble if a Wall Street firm is lecturing you about morality." **The concern is that the data-opolies' products are purposefully addictive, and thereby eroding individuals' ability to make free choices.**

There is an interesting counterargument that's worth noting, based on the interplay between monopoly power and competition. On the one hand, in monopolized markets, consumers have fewer competitive options. So, arguably, there is less need to addict them. **On the other hand, data-opolies, like Facebook and Google, even without significant rivals, can increase profits by increasing our engagement with their products. So, data-opolies can have an incentive to exploit**

behavioral biases and imperfect willpower to addict users — whether watching YouTube videos or posting on Instagram.

Political concerns. Economic power often translates into political power. Unlike earlier monopolies, data-opolies, given how they interact with individuals, possess a more powerful tool: namely, the ability to affect the public debate and our perception of right and wrong.

Many people now receive their news from social media platforms. But the news isn't just passively transmitted. Data-opolies can affect how we feel and think. Facebook, for example, in an "emotional contagion" study, manipulated 689,003 users' emotions by altering their news feed. Other risks of this sort include:

- **Bias.** In filtering the information we receive based on our preferences, data-opolies can reduce the viewpoints we receive, thereby leading to "echo chambers" and "filter bubbles."
- **Censorship.** Data-opolies, through their platform, can control or block content that users receive, and enforce governmental censorship of political or religious information.
- **Manipulation.** Data-opolies can promote stories that further their particular business or political interests, instead of their relevance or quality.

Limiting the Power of Data-opolies

Upon closer examination, data-opolies can actually be *more* dangerous than traditional monopolies. They can affect not only our wallets but our privacy, autonomy, democracy, and well-being. Markets dominated by these data-opolies will not necessarily self-correct. Network effects, high switching costs for consumers (given the lack of data portability and user rights over their data), and weak privacy protection help data-opolies maintain their dominance.

Luckily, global antitrust enforcement can help. The Reagan administration, in espousing the then-popular Chicago School of economics beliefs, discounted concerns over monopolies. The Supreme Court, relying on faulty economic reasoning, surmised that charging monopoly prices was "an important element of the free market system." With the rise of a progressive, anti-monopoly New Brandeis School, the pendulum is swinging the other way. Given the emergence of data-opolies, this is a welcomed change.

Nonetheless, global antitrust enforcement, while a necessary tool to deter these harms, is not sufficient. Antitrust enforcers must coordinate with privacy and consumer protection officials to ensure that the conditions for effective privacy competition and an inclusive economy are in place.

■ END OF ARTICLE