Regulating Tech Platforms: A Blueprint for Reform

By Ganesh Sitaraman | April 2018

THE GREAT DEMOCRACY INITIATIVE

Reporters at the *New York Times* and the *Observer* recently uncovered that Cambridge Analytica/SLC, a firm that has been described as a "military-grade psychological warfare and psychological operations company," mined millions of Facebook users' profile data for the purpose of political meddling in the 2014 and 2016 elections.[1] This information caused an immediate firestorm, including a movement to delete Facebook accounts, calls for founder Mark Zuckerberg to testify before Congress, and demands for regulation of powerful tech companies to ensure data security and privacy.

Facebook is far from the only tech company facing controversy from activities stemming from its behemoth size and power. Last year, the European Commission fined Google more than €2.4 billion ($2.7 billion) for abusing its dominant position to harm competitors.[2] The Federal Trade Commission fined Uber for misleading drivers on pay.[3] Amazon and Apple have been fined for not paying the full amounts of taxes they owed.[4]

In the wake of the Cambridge Analytica disclosures, individuals across the political spectrum have called for government intervention. Even tech company CEOs now recognize that their companies need to be regulated. Apple's Tim Cook said "some well-crafted regulation is necessary." Facebook's Mark Zuckerberg acknowledged that the question isn't whether to regulate, but "How do you do it?"[5]

This newfound recognition that regulation is essential is an important development. But the U.S. approach to regulating tech platforms should not fixate only on Facebook's issues revealed by the Cambridge Analytica scandal. Such an approach could result in a patchwork of narrow, technical solutions to a problem that is rooted in broader, structural failures. Those include the government's failure to address market power and dominance among technology platforms, and its failure to create a regulatory structure that protects individual privacy. What we need is a regulatory framework that ensures both that technology platforms cannot use their market power to inhibit competition, and that consumers' data is secure and privacy is respected.

This paper provides such a framework. It makes four sets of recommendations for how to regulate tech platforms.

First, institute a federal process for designating platforms and ensuring platform neutrality.

Platforms have life-or-death power over those who seek to use them. A platform can exclude participants (people or businesses, depending on the platform), can disfavor their content, and, when vertically integrated with a competitor, can use their power to compete with and undermine participants. In other words, platforms aren't necessarily neutral or fair to their users. What we need is a process for designating certain businesses as platforms, which would trigger regulation to ensure that they do not use their power to harm competition or consumers.

Second, adopt comprehensive data privacy and security protections.

Platforms, and these days most companies, collect significant amounts of user data for sale or for improving their products. Individuals have little control over their own data, and the risks of data breaches, with consequences for privacy and security, are significant. The United States should adopt a modified version of the European Union's General Data Protection Regulation as a way to address these problems, and create fundamental changes in how companies gather, store, transfer, and use data.

Third, reinvigorate antitrust enforcement.

The confluence of data and platform power raises additional problems, which are compounded when firms merge or expand into multiple arenas. If a single company owns multiple platforms, it is able to harvest data from across those platforms, merge that data, and develop increasingly specific and troubling profiles of users. We need to reinvigorate antitrust enforcement to block and unwind mergers that have this data nexus as a feature.

Fourth, enact laws at the state level if the federal government will not act.

Federal regulation in these arenas might not be possible in the short term. As a result, states should regulate tech platforms in the absence of federal regulation. States themselves can impose a more limited requirement of platform neutrality and can establish data privacy protections.

Recommendation 1: Institute a Federal Process to Designate Platforms and Ensure Platform Neutrality

Platforms have significant power over their users – power that can be abused. Technology platforms are unlike many other companies in the economy. In many sectors, companies compete with one another to sell products or services, competing on price and quality. Technology platforms, in contrast, often play the role of middleman, connecting consumers with other sellers and advertisers. But in addition to playing this middleman role, tech companies are also known for competing directly with successful small businesses using their platforms.

Take, for example, Amazon's marketplace. The way we normally think of it, John Q. Public can make custom bracelets at home and sell them on the marketplace. But problems could arise because Amazon both runs the marketplace and has a vertically-integrated entity that competes on the marketplace, Amazon Basics. That means that if John Q. Public's bracelets do well, Amazon will notice because it collects data about its marketplace. Amazon Basics could then produce identical bracelets in China at a lower cost. Amazon can feature Amazon Basic's bracelets on page one of its search, and relegate John Q. Public's bracelets to page three. The result is that John Q. Public will go out of business, not because his product was worse, but because Amazon used its platform's data, its power over the marketplace, and its vertically-integrated company to put him out of business. This fear isn't theoretical: Some companies have alleged that Amazon has done exactly this to them.[6]

The same kind of thing can happen with Google's search function. Consider the conflict between Google and Yelp, which aggregates customer reviews of restaurants and other businesses. Because Google has a separate line of business reviewing and recommending businesses, Google can prioritize its content over Yelp's when a user searches for a business review – and even when they search for "Yelp" and a business review.[7] This too isn't theoretical. In the summer of 2017, the EU antitrust authorities fined Google $2.7 billion for prioritizing its shopping comparison product instead of neutrally treating its comparison product and those of competitors.[8] In an account featured in the *New York Times Magazine* in early 2018, a startup tech company alleged that Google had de-prioritized their search tool. The alleged reason was that Google feared that if the startup gained traction it might eventually threaten Google's primacy over search.[9]

The problem in these cases emerges due to two factors: vertical integration and market power. Vertical integration gives a platform motive to discriminate against its users, because the platform (e.g. a marketplace or search engine) also owns a vertically-integrated business that operates on the platform alongside other companies (e.g. Yelp). This means that the platform can favor its vertically-integrated business over others; the platform isn't neutral even though users expect it to be. The market power problem is that platforms have the means to

discriminate because of their dominance. Many people think platforms are dominant because of network effects – that the more people using the platform, the better the service gets. While this is partly true, it is an incomplete explanation. Platforms can also become dominant if they discriminate against, exclude, and threaten possible competitors. If a search engine doesn't allow a potential competitor to be searchable, for example, the competitors might never have a chance to compete.

As cutting-edge as today's technologies seem, these problems – and the principles for regulating them – are actually quite old. Throughout history, policymakers confronted a variety of industries engaged in similar practices to those of contemporary tech platforms. They recognized that these practices were destructive, and to address them, they developed a set of basic principles that operate across a variety of sectors and domains of law: nondiscriminatory access, separation or "quarantine" of the business, and (depending on the context) regulation of rates.

As cutting-edge as today's technologies seem, these problems – and the principles for regulating them – are actually quite old.

A few examples will help illustrate. Imagine that you're in the late 19th century. Railroad service is competitive, with many train companies (each of which owns its own track) operating on the East and West coasts. But the railroad terminal in St. Louis is owned by a single train company, and any other train company that wants to send its trains from the eastern United States to the West must take that route. If the company that owns the terminal refuses to let any other company use it, there would be no competition on the routes through St. Louis. The train company would be a monopolist that could price-gouge consumers and provide poor service. Because of the extremely high capital costs of building a new terminal and re-routing tracks to it, competition might be impossible.

Historically, antitrust law solved this problem with what is called the essential facilities doctrine. Under the essential facilities doctrine, a company engages in anticompetitive behavior if (a) it controls an essential facility as a monopolist, (b) a competitor is unable to duplicate the essential facility in any practical or reliable sense, (c) the company denies use of the facility to the competitor, and (d) it is reasonably feasible for the company to offer access to the facility to the competitor.[10] Therefore, if the railroad company could offer nondiscriminatory access to the terminal, it must do so. This doesn't mean that the company can't recoup its costs by charging a fee (it can, though that rate has to be reasonable), nor does it mean that the company can't limit access to the terminal to prevent congestion. But it can't price-discriminate or bar access altogether.[11] To some, the doctrine is controversial; after all, the company did undertake the capital costs to

build the terminal. But the doctrine doesn't prevent the company from recouping its cost, and it offers a strong benefit to society in facilitating interstate commerce. While there is uncertainty and debate over its applicability in the wake of a recent Supreme Court case, the doctrine illustrates the basic considerations at issue.[12] It recognizes that monopolists have the extraordinary power to choke off all commerce (and in this case, transportation), and that no entity should be so powerful as to be able to exploit and pressure consumers, citizens, or the government.

Another example comes from the common law of public accommodations, or as it is sometimes known, the law of innkeepers and common carriers. Under the common law, innkeepers and common carriers were required to accept all comers, meaning that they could not discriminate against customers. The justification for the rule is simple and is similar to the one undergirding the essential facilities doctrine. Think back to the early Republic, when travel between cities took weeks and there were few roads and few places to stay along those roads. If an innkeeper could discriminate against travelers, then it would undermine the ability of anyone to travel. People would not be able to travel from one place to another (unless for a day-trip) if they could not reliably find access to overnight lodging. The nondiscriminatory access rule recognized that innkeepers serve an important public function on highways and hold extraordinary power over the free flow of commerce in the country.[13]

A third example comes from public utilities regulation, which can apply when a particular service is a national monopoly or networked industry. In the telephone industry, for example, it was extremely costly to provide phone lines to every household, and the network was more valuable the more people are on it (because they can communicate with each other). As a result, it makes sense to have a single provider of telephone service. But if telephone service is a monopoly, what's to stop the monopolist from raising rates? What's to stop the monopolist from using its power over phone lines to weasel its way into other adjacent sectors? Electricity and water are similar. It is costly to build pipes and power lines – and we don't really want multiple sets of competing pipes and power lines everywhere – but that means that a monopolist over these essential services can exploit users.

The answer in these sectors was public utilities regulation. The basic idea is that market power is necessary in some sectors, but instead of government providing the service directly, the government would regulate the private monopolist. First, it would separate or "quarantine" the business line that had monopoly power from the rest of the company, restricting a company to only owning the monopoly element and thereby preventing them from exploiting other adjacent sectors. Second, there would be regulation of rates and terms, to prevent the monopolist from jacking up prices on captive consumers. Third, there was usually a protected franchise. The utility was given exclusive domain over its sector, so that competitors could not detract from the utility's business.[14] The reason for this is that the utility was mandated to offer nondiscriminatory access, and if there were

competitors skimming off the most valuable customers, it wouldn't be financially possible for the utility to serve everyone.

The similarities between these approaches – quarantine, nondiscriminatory access, regulation of rates – provide principles for how to regulate tech platforms. Platforms should be required to offer nondiscriminatory access to their services (marketplace, search, or whatnot) and vertically integrated business lines must be divested from the platform. This separation, or quarantine, prevents exploiting power over search (including the power of data collection) to give preferential treatment to their own business lines.[15] The nondiscriminatory access provision is a complementary obligation to treat all users with fair and neutral terms. Rate regulation seems like an ancient idea, and one limited to sleepy public utilities like electricity. But in some cases, it is a necessary corollary to nondiscrimination and quarantine. If a platform charges users, and it becomes so dominant as effectively serving as a monopoly, then the platform might raise rates on users. Competitors won't be able to challenge the platform because they might not be able to get the network benefits needed to make their alternative platform valuable.

Factors for Designating a Platform

- Extent to which the entity serves as an exchange or marketplace for transaction of goods and services
- Extent to which the entity is essential for downstream productive uses
- Extent to which the entity derives value from direct or indirect network effects
- Extent to which the entity serves as basic infrastructure or foundation for customizable applications by third parties
- Extent to which the entity utilizes or could utilize its platform as a competitor, or could deny access or engage in discriminatory access

Both the Federal Trade Commission and Congress could act to implement these principles. The FTC already has significant authorities and could act in accordance with these principles on a case-by-case basis or by issuing regulations. Because the FTC has the power to regulate unfair methods of competition and unfair or deceptive practices, it could, for example, determine that discriminatory platforms are engaged in an unfair method of competition or an unfair practice.[16] If the FTC is unwilling to act, Congress could also pass legislation implementing these principles.

Here's how it would work. First, we need to determine what exactly constitutes a platform. The core problem is that there is no singular definition that will cover every possible case in which regulation is justified and exclude every possible case in which regulation is not justified. For example, a farmer's market might be considered a "platform" because it is a venue run by an organization that hosts a variety of sellers (the farmers). This is conceptually indistinguishable from Amazon Marketplace. Intuitively, most people would think it unfair for the farmer's market to charge one tomato grower twice as much as another for the

same size stall. Yet no one thinks that the federal government should regulate local farmers markets.

One way to avoid this problem is to designate some entities or lines of business as "platforms." An entity would be a "platform" based on a multifactor test that requires weighing a variety of relevant factors, including (among other things) whether the company is an exchange or marketplace, whether it benefits from network effects, whether it serves as a foundation for customizable applications for third parties, and whether it could use its platform to deny access if it was vertically integrated.[17]
If Congress wanted to adopt this approach by legislation, designations could happen in two ways. First, Congress would empower the Federal Trade Commission (FTC) to designate platforms, similar to how the Financial Stability Oversight Council can designate systemically important financial institutions. The FTC would consider the variety of factors and make a determination that an entity or business line is a platform. Second, because the FTC has limited resources and because uncompetitive practices might be distributed widely across the economy, third parties – state attorneys general and individual citizens – would be able to petition in court and get the entity designated as a platform. In these latter cases, a judge would weigh the various factors and determine whether the entity is a platform subject to regulation.

The consequences of designation follow from the traditional principles of regulation discussed above. If the FTC regulates, the platform would be cleaved from the rest of the business (quarantine) and subject to a non-discrimination duty. In other words, the platform would not be allowed to have business-lines beyond the platform itself. The FTC would also have the power to regulate rates, though it would not necessarily need to exercise this power. In cases in which third parties bring a suit to designate a platform, the court would be limited to the quarantine and non-discrimination remedies, in addition to imposing treble damages as a penalty for illegal, anticompetitive behavior. Third party designations would not trigger rate regulation but third parties could still sue platforms that engage in rate discrimination.

Recommendation 2: Institute Personal Data Privacy Protections

The widespread availability of personal data raises concerns about individual privacy from corporate and government intrusion, the possibility of hacks and identity theft, and the power companies might gain over time from controlling so much information about individuals. Companies (and the government) can identify how often someone goes to church, whether they look at pornography, whether they have a physical or mental illness, whether they are gay or straight. The risks to security range from hackers seeking financial information to foreign governments rigging elections. Individual privacy is often violated, as data is collected and transferred – potentially multiple times – without any meaningful notice or consent. Consumers have little choice but to offer up their data, lest they

are locked out of essential online services. Data hoarding can also inhibit competition, as companies with massive amounts of data produce customizable products and services, making it hard for new entrants to compete. Again, it isn't just network effects that make platforms work: data collection enables market power and dominance.

Even the benefits of data collection come with downsides. On the one hand, data collection and analysis mean companies can better predict what TV shows or movies we might like to watch. But at the same time, personalization based on data collection narrows our worldviews, exposes us to fewer ideas, and threatens to deepen tribalism and social fracturing.

Given the risks from the mass collection of data, it is striking that there aren't comprehensive regulations on how companies should store, protect, and use personal data. Instead, we have a notice-and-consent regime that is practically toothless because people simply click through large, complicated terms-and-conditions without the ability to fully understand their meaning, negotiate the terms, or make choices about the use of their data.

> ***It isn't just network effects that make platforms work: data collection enables market power and dominance.***

How should we balance the consumer and societal benefits of data use with the need to protect against unfair and intrusive data harvesting? The goals in regulating data should be to set basic standards for data collection and use, to empower citizens to control how data is used, and to ensure that data collection doesn't lead to uncompetitive markets. Regulation is particularly appropriate because government's role is to protect consumers and ensure competition and because there are significant social and political threats that attend data harvesting. But critically, data protections should not be technical patches; data protections should be structurally designed to fundamentally shift the incentives of private companies and the government, so that their actions will protect consumers rather than exploit them.

At the federal level, both the Federal Trade Commission (FTC) and Congress could act along these lines. The FTC already has considerable power to impose data privacy and security regulations under its authorities to regulate unfair or deceptive practices and unfair methods of competition. At present, the FTC has issued "fair information practice principles," but these principles are guidelines rather than binding regulations. If the FTC does not act, Congress has the constitutional authority to pass legislation on data privacy and security regulations.

While identifying and drafting a comprehensive set of data privacy and security regulations might seem daunting, the European Union has recently adopted a

comprehensive approach to data privacy and usage known as the General Data Protection Regulation (GDPR). The GDPR contains a variety of principles, many of which can and should be adopted into American law.

Data Ownership and Consent. Many companies that citizens rely on to read the news and participate in democracy and the economy require giving blanket authorization for surveillance, data collection, and exploitation. Complex, unintelligible terms and conditions pages with a single checkbox are the norm for "consent," and individuals end up consenting indefinitely and consenting to data transfers to third parties. Instead, individuals should have the right to understand what data a company might collect and to opt-in to choose what specific data is given up (rather than being forced into blanket authorizations), to determine who is using their data (e.g. restricting third party transfers), to pick for what purposes the data are used, and to approve of how long the data are used and stored. Individuals should be able to withdraw consent easily, and they should also be able to access platforms without being required to give up any data.

Right to Access. Individuals should have a right to know what data a company has on them. Individuals should be able to get this access for free in an electronic format, and it should include an account of what the data are being used for and to whom it is being sold or transferred, and they should be able to correct data that is incorrect. This is common in other similar sectors. Credit reporting companies, for example, used to have secret databases on individuals, but individuals now have a right to inspect that data and analysis on that data.[18]

Data Erasure. Companies often keep data indefinitely, which means that the data are constantly at risk of exposure to hacks. This can continue even if individuals no longer want to use the company's product or want to switch to a competitor. Individuals should have the right to have a company delete all of their data and stop using it. If the company has transferred data to third parties (with the individual's consent), the company should have to inform the third parties of the withdrawn consent and the third parties will be obligated to delete the data.

Data Portability. When a single platform has so much data on an individual and can customize the experience, it becomes harder for the individual to switch to a competing service. This is problematic because it entrenches the power of those platforms, prevents competition, and slows the development of beneficial innovations (including privacy and security). Individuals should have the right to get their data in a format that is portable, so it can be migrated to and used on a different platform or networked ecosystem. For example, if an individual wants to shift from using Gmail to using Outlook or Yahoo!Mail, the individual should be able to download emails in a portable format.

Other Principles and Provisions. In addition, a comprehensive approach to data privacy protections should require that companies design products so that

privacy and data protection are embedded into the system. For example, companies should adopt a posture of data minimization – collecting only the data necessary for the specified task and deleting data immediately when it is not necessary. In the event of breaches, companies should be required to notify individuals with 72 hours. In order to ensure compliance, penalties for violating the rules should be significant. The EU's GDPR adopts a penalty of the greater of 4 percent annual global revenue or €20 million. The enormity of the penalty is designed to force companies to adopt the regulations – and to operate carefully with respect to personal data.

Adopting principles along the lines of the EU's GDPR, with some slight adaptations to the American context, has significant benefits. First, the GDPR is a fully designed system. The GDPR's components cover the full range of data protections. The individual components also interact with each other to create a system for data regulation. For example, the provisions for privacy by design intersects with severe penalties to encourage companies to build protective systems in the first instance. The requirements also intersect to encourage competition; if someone designs a more privacy-focused platform, data portability means it is easy for users to migrate to the competitor.

Second, adopting a version of the GDPR would align the regulations on data between the United States and the European Union, making it easier for companies to comply. Instead of having two different standards, companies would only have to comply with a single standard. This should, in turn, make it more likely that start-ups and new companies can compete across both continents because the regulatory barriers to entry will be lower. Often, proposals for "regulatory harmonization" lead to a race to the bottom that can deregulate a sector. Here, aligning the standards will actually improve privacy, not weaken it.

Recommendation 3: Reinvigorate Antitrust Enforcement

When tech platforms merge, they don't just create a bigger company. Mergers allow a company to collect and combine data from different platforms. For example, when Facebook bought WhatsApp and Instagram it significantly expanded the amount of data under its control. Mergers between platforms compound many of the risks that come from data collection (outlined above).

Mergers can also prevent the rise of potential competitors to tech platforms. For example, WhatsApp and Instagram might eventually have expanded their operations and become full-scale competitors to Facebook. Yet, instead of competition, the acquisitions made Facebook even more dominant. In some cases, data and the merger problem also work in tandem. If a platform like Google or Amazon has data on what up-and-coming companies are starting to gain traction (for example, because it can monitor the frequency of searches for those companies), it can purchase start-ups before anyone even knows they might become a competitor. The result, once again, is less competition.

Strong antitrust enforcement from the Department of Justice and the Federal Trade Commission is therefore essential. As a starting point, the antitrust agencies need to revise their historically lax approach to scrutinizing technology platform mergers. For example, the agencies permitted Facebook to acquire WhatsApp and Instagram. Legislators also need to engage in more serious oversight of the antitrust agencies and, if the regulators do not act, should consider new legislation in order to ensure a more robust antitrust enforcement regime.

Recommendation 4: States Should Also Take Action

While action at the federal level is certainly possible, it does not seem likely in the short-term. But that doesn't mean that states can't take action. States can act both on platform neutrality and on data protections.

First, on the question of platform power and neutrality, states can pass laws requiring that any platform operating in its jurisdiction that offers a good or service must offer nondiscriminatory access to that platform (i.e. no preferential treatment of their own vertically integrated business lines). The common carrier and innkeeper regulations discussed above are a matter of state common law. In addition, states have the general power to regulate commercial activity. Under these principles and powers to regulate commerce within their state and protect their citizens from unfair and dangerous practices, states could require that any platform offering goods or services (like Google Search or Amazon) must do so in a neutral fashion, without any preferential treatment of their own vertically integrated business lines.

In practice, for example, a state could pass a law declaring that if an online platform recognizes that an IP address is coming from within the state, it would have to offer a non-discriminatory search process. States could implement this akin to the recommendations above, with an administrative designation process for defining platforms, or it could simply apply the rule to online platforms including online marketplaces and search tools.

Second, states could put into place data privacy regulations on their own. Under the states' general police powers, states have the ability to protect their citizens from harm. States could therefore require that companies must follow data privacy regulations, along the lines of the GDPR or the FTC's fair information practice principles. Akin to requiring platform neutrality, states could require either that consumers using the platform from an IP address within the state need to have their data protected or that companies enable consumers to inform the company where they are located, with that determination triggering the protections.

Third, states could require that any contractor with the state needs to follow various fair practices – including around data and platform neutrality. This

would mean that if companies want the state's business, they would have to conform to these practices in order to meet the state's procurement requirements. Large states – like California or New York – would have particular power to push companies to adopt these standards, or if they are unwilling, to spark the creation of new companies who will. The state procurement approach is not without precedent. The Governor of Montana, for example, recently issued an executive order requiring that state contractors meet net neutrality principles, and Oregon recently passed a state law banning the state government from working with companies that do not follow net neutrality.[19]

Conclusion

From Facebook's Mark Zuckerberg to Apple's Tim Cook, even the heads of major tech companies recognize that regulation is necessary in their industry. The question is how to do it. This paper provides an initial set of answers: platform neutrality, data protections, and antitrust enforcement. The FTC, Congress, and the states can all play a role in reform. It is time for them to act.

Endnotes

[1] Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, How Trump Consultants Exploited the Facebook Data of Millions, N.Y. Times, Mar. 17, 2018; Carole Cadwalladr & Emma Graham-Harrison, Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach, Observer, Mar. 17, 2018; Jackie Flynn Mogensen, A Groundbreaking Case May Force Controversial Data Firm Cambridge Analytica to Reveal Trump Secrets, MotherJones, Dec. 19, 2017.

[2] European Commission, Press Release: Antitrust: Commission fines Google 2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service, June 27, 2017, http://europa.eu/rapid/press-release_IP-17-1784_en.htm.

[33] Federal Trade Commission, Press Release: Uber Agrees to Pay $20 Million to Settle FTC Charges that it Recruited Prospective Drives with Exaggerated Earnings Claims, Jan. 19, 2017, https://www.ftc.gov/news-events/press-releases/2017/01/uber-agrees-pay-20-million-settle-ftc-charges-it-recruited.

[4] Shona Ghosh & Rob Price, Amazon Has Been Order to Pay Europe 250 Million Over Unpaid Back Taxes, Business Insider, Oct. 4, 2017.

[5] Bloomberg News, Apple's Tim Cook Calls for More Regulations on Data Privacy, Mar. 23, 2018; Nicholas Thompson, Mark Zuckerberg Talks to Wired about Facebook's Privacy Problem, Mar. 21, 2018.

[6] Lina M. Khan, Amazon's Antitrust Paradox, 126 Yale L.J. 710, 780-83 (2017).

[7] Conor Dougherty, Yelp's Six Year Grudge Against Google, N.Y. Times, July 1, 2017.

[8] Mark Scott, Google Fined Record $2.7 Billion in E.U. Antitrust Hearing, N.Y. Times. June 27, 2017.

[9] Charles Duhigg, The Case Against Google, N.Y. Times Mag., Feb 20, 2018.

[10] MCI v. AT&T, 708 F.2d 1081, 1132-1133 (7th Cir. 1983).

[11] This hypothetical is a modification of U.S. v. Terminal R.R. Ass'n, 224 U.S. 383 (1912).

[12] The case is Verizon Comm's v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398 (2004).

[13] For overviews of this body of law, including the English inheritance, see, e.g., Joseph William Singer, No Right to Exclude: Public Accomodations and Private Property, 90 Nw. U. L. Rev. 1283 (1996); Alfred Avins, What is a Place of "Public" Accommodation?, 52 Marquette L. Rev. 1, 1-7 (1968).

[14] For an overview, see Peter W. Huber et al., Telecommunications Law (2d. ed., 1999); Richard A. Epstein, Common Carriers, The New Palgrave Dictionary of Economics and the Law (1998).

[15] For discussions of the separations principle, see Tim Wu, The Master Switch (2010); Lina M. Khan, The Separation of Platforms and Commerce, Colum. L. Rev. (forthcoming 2019).

[16] The FTC's authority under Section 5 is broader than the antitrust laws. FTC v. Sperry & Hutchinson Trading Stamp Co., 405 U.S. 233 (1972).

[17] A full set of factors might include: The extent to which the entity serves as an exchange or marketplace for transaction of goods and services; the extent to which the entity is essential for downstream productive uses; the extent to which the entity derives value from direct or indirect network effects; the extent to which the entity serves as basic infrastructure or foundation for customizable applications by third parties; the extent to which the entity utilizes or could utilize its platform as a competitor [vertical integration], or could deny access or engage in inequitable or discriminatory access to the platform; the extent to which it is not reasonably or practically possible for a competitor to duplicate the facility; the extent to which it is feasible to provide access; the nature, scope, interconnection, and mix of the activities of the company; and any

other competition-related factors deemed appropriate. Another approach would limit FTC authority to the largest entities in terms of size or concentration in industry.

[18] Fair Credit Reporting Act, 15 U.S.C. §1681.

[19] Executive Order No. 3-2018, State of Montana, Jan. 22, 2018, https://governor.mt.gov/Portals/16/docs/2018EOs/EO-03-2018_Net%20Freedom.pdf?ver=2018-01-22-122048-023; Tom James, The Register Guard: Governor Signs Net Neutrality Bill, April 10, 2018.