Information Technology and Innovation Foundation
1101 K Street NW, Suite 610
Washington, DC 20005

August 20, 2018

Donald Clark
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex C)
Washington, DC 20580

RE: Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201

Dear Secretary Clark,

The Information Technology & Innovation Foundation (ITIF) is pleased to submit these comments in response to the request for comment (RFC) from the Federal Trade Commission (FTC) on whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy.[1]

ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington, and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation, and productivity.

There is an inherent tension between regulators and innovators. Regulators seek to place limits on businesses to avoid risky scenarios that might result in harmful outcomes. In contrast, innovators take risks in their pursuit of new ideas. Unfortunately, as the economy has become more innovation-based, there has been considerably less focus on how regulatory agencies can both protect consumers from harm and avoid undermining incentives for innovation. ITIF offers these comments on how the FTC can better find this balance.

[1] "Hearings on Competition and Consumer Protection in the 21st Century," Federal Trade Commission, n.d. https://www.ftc.gov/policy/hearings-competition-consumer-protection.

COMPETITION AND CONSUMER PROTECTION ISSUES IN COMMUNICATION, INFORMATION, AND MEDIA TECHNOLOGY NETWORKS

Competition and consumer protection issues are rightly under the ambit of a generalist enforcement agency—the FTC. For most all consumer protection and competition issues, the FTC should treat Internet Service Providers (ISPs) no differently than other similar actors it oversees. We as a nation should generally work to move away from sector-specific competition and consumer protection regulations. Generalist enforcement agencies are resilient to capture, make for more efficient enforcement, and eliminate duplicate efforts across the government. The narrow exception is where the expertise and foresight of a sector-specific agency could improve outcomes.

With the Federal Communications Commission's (FCC) recent decision to classify broadband Internet access service as a lightly regulated "information service" under the Communications act, the FTC finds itself with an important new oversight role with respect to ISPs. The FTC is well-equipped to oversee ISPs and other participants in the Internet access system for most all competition and consumer protection issues, including privacy for all actors in the broader Internet system. However, ITIF has argued that the FCC is better suited to the role of enforcing network neutrality.[2] Congress should address the question of the proper agency to oversee broadband providers through legislation that also settles the controversy over the regulatory structure for broadband and net neutrality generally.[3] Should Congress agree that the FCC is better suited to enforce network neutrality issues, the FTC should cede this ground to the sector-specific agency.

In the meantime, while the FTC maintains oversight of these issues, we urge the FTC to take a relatively permissive stance when it comes to paid prioritization schemes, as many of these are likely to functionally enhance the performance of the Internet without making other users worse off.[4] As long as best-effort traffic continues to be the predominant use of broadband, as it likely will, the applications that legitimately benefit from prioritization (which is a narrower class than generally assumed) should not swamp the open Internet.

---

[2] Doug Brake, "Why We Need Net Neutrality Legislation and What it should Look Like" (Information Technology and Innovation Foundation, 2018), https://itif.org/publications/2018/05/07/why-we-need-net-neutrality-legislation-and-what-it-should-look.

[3] Ibid.

[4] Doug Brake, "Paid Prioritization: or Why We Should Stop Worrying and Enjoy the Fastlane" (Information Technology and Innovation Foundation, 2018), https://itif.org/publications/2018/07/30/paid-prioritization-why-we-should-stop-worrying-and-enjoy-fast-lane.

Real-time services that do not tolerate delay but also require reliable performance to justify investment development, such as robotics control, haptic feedback mechanisms, and high-quality VR or AR, do not work well over the open Internet as it functions today. Basic tradeoffs around delay and reliability are built into the basic protocols of the Internet—both reliability and low-latency can only be provided with traffic differentiation. Considering the varying demand for these resources from different applications, prioritization can be provided without an offsetting loss. For example, nobody really notices if an email packets arrive a tenth of a second later than it otherwise would, but that same delay in a video conference results in choppy video.

The FTC should step in if a provider functionally blocked or unduly slowed legal Internet traffic, or did not otherwise abide by its transparency disclosures. But prioritization techniques that provide better than best-effort traffic are unfairly maligned by net neutrality activists, and as long as paid prioritization is offered on a non-exclusive basis, with similar terms offered to similar users, the risks of over-enforcement outweigh the risks of under-enforcement.

Net neutrality is one key flashpoint, and a primary tussle between different actors in the broader Internet system. As a general matter, the FTC should hew toward traditional antitrust analysis, and treat broadband networks similar to other parts of the economy, analyzing the costs and benefits of enforcement and the impact to dynamic innovation before intervening generally. For example, under the previous administration the FCC attempted to place heightened privacy restrictions on ISPs as compared to other sectors, which was ill advised. ITIF welcomed the comments of FTC staff, who argued for similar treatment compared to other large networked platforms.

THE IDENTIFICATION AND MEASUREMENT OF MARKET POWER AND ENTRY BARRIERS, AND THE EVALUATION OF COLLUSIVE, EXCLUSIONARY, OR PREDATORY CONDUCT OR CONDUCT THAT VIOLATES THE CONSUMER PROTECTION STATUTES ENFORCED BY THE FTC, IN MARKETS FEATURING "PLATFORM" BUSINESSES

By now there is a well-established literature on the nature and role of market platforms. The consensus is that market platforms can offer both sellers and buyers tremendous benefits, largely by reducing the transaction costs of finding other parties to interact with.[5] In many cases a combination of efficiencies of scale and network effects push platform markets toward concentration. But that does not mean these markets will lack competition or innovation. In fact, the presence of even large platforms can increase both competition and innovation at the level that matters most; the case of an individual customer seeking the best supplier. In cases

[5] Joseph V. Kennedy, "Why Internet Platforms Don't Need Special Regulation," (Information Technology and Innovation Foundation, October 2015), https://itif.org/publications/2015/10/19/why-internet-platforms-don't-need-special-regulation.

where lack of competition due to anti-competitive conduct is a concern, normal antitrust principles and remedies still hold. But regulators need to carefully study the effect of both alleged anticompetitive behavior and proposed remedies on all sides of the platform before reaching conclusions on the best policy response.

Today, most discussion of antitrust issues and platform markets seems to focus on the largest Internet companies (Apple, Amazon, Facebook, Google, and Microsoft), but both medium and smaller Internet platforms play important roles in helping match suppliers and customers for a wide range of goods and services. However, platform businesses were and are important parts of the traditional economy. They include shopping malls, job placement services, and newspaper classified ads. If software and Internet companies present unique antitrust concerns, it is largely because of the growing value of on-line commerce in the economy and the rapidly changing nature of both the technology and (as a result) the business models firms pursue.

Does the platform business model have unique implications for antitrust and consumer protection law enforcement and policy?

The rapid increase in both usage and value for some platforms has produced a number of calls for greater regulation. The motivations behind these outcries vary, but they include fears of market power, exploitation of workers, concerns about data security and privacy, opposition from incumbent suppliers, and in the case of Europe, concerns about lagging regional competitiveness in the digital economy. By and large these calls for new regulatory action are misplaced. In fact, by showing how efficiently specific markets can work, Internet platforms often point out the need for reduced regulation of existing industries, such as taxis, lodging, and product marketing, so that they can do a better job responding to the demand that platforms create.

While Internet platforms are new, market platforms are not. But the former do play a unique role in the marketplace by bringing large groups of users together and reducing one of the most important barriers to economic activity: transaction costs. Because Internet platforms are different from traditional businesses, they often do not fit well into the normal regulatory system. Regulators therefore need to have a good understanding not only of platforms generally, but also of the role that specific platforms play in the market, including the source of the value they create, their relationship to customers and competitors, and the alternatives to them.

It is important for regulators to understand the benefits platforms can provide. A previous submission to the FTC listed five ways in which these firms add value:

1. Improving resource use;
2. Increasing competition;
3. Reducing transaction costs;
4. Reducing asymmetric information between buyers and sellers; and
5. Bringing new buyers and sellers into the market.[6]

With the growing importance of national and even international markets, many businesses, including platforms need to be large to maximize these benefits. Moreover, size brings considerable buyer and seller benefits.

While Internet platforms are just as capable of anticompetitive behavior and bad business practices as any other company, the traditional powers available to injured parties and government regulators can handle virtually all actual (as opposed to possible) harms. There is therefore little need at this point for new laws or regulatory actions aimed solely at platforms per se. However, in specific case such as pricing below marginal cost, regulators will need to adapt standard theory to account for the ways in which platforms add market value.

Critics and some regulators have expressed five general concerns about the role of Internet platforms. The first is that some of these platforms have become too powerful and are precluding platform competition in the marketplace. Second, some express concern that businesses are increasingly dependent on platforms for sales and therefore are subject to capricious and harmful action by the platform. Third, some regulators and privacy groups have worried about the misuse of consumer data and inadequate precautions to protect the massive amounts of data these companies collect. The fourth concern is that some platforms take advantage of their suppliers by classifying them as independent contractors rather than employees. Finally, some regulators and incumbent industries have expressed concern at the threat that platforms pose to competitors.

Note that only some of these concerns involve traditional antitrust concerns. In specific cases, these antitrust concerns can be legitimate, but the approach to them should continue to be driven by the standard metric of maximizing consumer welfare and economic efficiency. With regard to the first concern specifically, the nature of internet platforms is such that in many markets only one major platform will succeed in the marketplace at a time. The presence of network effects and efficiencies of scale often moot the traditional assumption of diminishing marginal returns and confer advantages on the platform that succeeds in capturing

---

[6] Christopher Koopman, Matthew Mitchell, and Adam Thierer, "The Sharing Economy: Issues Facing Platforms, Participants, and Regulators," (Public interest comment submitted to the Sharing Economy Workshop, Federal Trade Commission, May 26, 2015, 2-3), http://mercatus.org/sites/default/files/Koopman-Sharing-Economy-FTC-filing.pdf.

a larger share of the market. But a larger market share does not only benefit the platform. It also maximizes the social value for users.

With regard to the other concerns, the FTC should reject growing appeals to use antitrust tools to address noncompetitive harms. It should also resist calls to regulate bigness per se, as overall large firms generate significantly greater welfare gains than small firms do.[7]

The first four items are legitimate concerns about market problems. However, these problems already exist in more traditional industries. Although their existence can impose social costs, for the most part these problems are contained by market competition, civil litigation by injured parties, and targeted regulatory enforcement against specific abuses. Internet platforms do not pose unique challenges in this regard, because they are subject to these same checks and balances. Specifically, it is far from clear that new legislation is needed to deal with imagined problems. Existing laws give agencies sufficient powers to deal with any actual problems.

The fifth concern frankly deserves less or even no attention. It is for the most part the creative destruction that Joseph Schumpeter portrayed as driving market innovation and higher productivity.[8] Those who lose out to market competition, especially by new entrants who may not face the same regulatory burdens, often feel that the latter benefit from an unfair advantage. In fact, because of lobbying, public policy often tilts toward incumbent firms and has provided them with benefits for decades.[9] But this usually imposes costs that limit economic growth.[10]

Where there are legitimate antitrust concerns, long-standing laws, including the Sherman Act of 1890 and the Clayton Act of 1914, already give both the Department of Justice and the Federal Trade Commission regulatory authority to punish anticompetitive behaviors such as price fixing, collusion, and mergers, whether or not the particular company is a platform.

---

[7] Robert D. Atkinson and Michael Lind, *Big is Beautiful: Debunking the Myth of Small Business*, (Cambridge: MIT Press, 2018).

[8] Joseph A. Schumpeter, *Capitalism, Socialism, and Democracy,* (London: Routledge, 1942).

[9] Gordon Tullock, "The Welfare Costs of Tariffs, Monopolies, and Theft" *Western Economic Journal* 5, no. 3 (1967); 224-32, Anne Krueger, "The Political Economy of the Rent-Seeking Society," *American Economic Review* 64, no. 3, (1974); 291-303.

[10] Mancur Olson, "The Rise and Decline of Nations: Economic Growth, Stagflation, and Social Rigidities (New Haven: Yale University Press, 1982).

There are other reasons to think that the market power of Internet platforms may not represent a threat. The first is that, in most cases few of these markets require a major commitment from either buyers or sellers, and both sides have the option of doing something else with their time and money. This ensures that the value of participating in the market is likely to be at least equal to the costs. Otherwise people will simply stop using the platform.

Second, Internet platforms face competition from numerous sources, including established industries, direct competitors, and related services. For example, travelers do not have to go to New York if the price of lodging is too high. If they do go to New York, they have the option of staying at one of many hotels. If they wish to have a more private experience, a number of services in addition to Airbnb exist to link them to a bed-and-breakfast or other arrangement.[11]

Competition is especially strong for platforms that rely on advertising for a large portion of their revenues. To attract consumers, these sites usually have to offer their basic services for free or at a heavily discounted price, although they may also offer a premium option. Although advertisers must pay, the largest ones are very sophisticated about making sure the value of advertising exceeds its cost. They typically purchase advertising across a wide variety of media. A company such as Google must compete not only with other search engines, but also with other types of Internet platforms and with television and print media. Independent companies such as Visual IQ make their money by helping advertisers find out which outlets provide them with the best value.[12] In this regard, accurate market definition is critical. It is largely a mistake to consider the "search market" or the "social network" market as discreet markets. In these cases, most, if not all, of the firms in these markets (e.g., Google, Microsoft, Facebook, etc.) provide these services for free and the real market is the total ad market (digital and non-digital). And here, at least for now, there is little evidence that these companies have market power.

Antitrust regulators often look for evidence of unfair pricing by companies with market power. In some cases, companies may be accused of charging too high a price, thereby restricting production and appropriating a large amount of consumer surplus for themselves. At the other extreme, regulators often view any practice of setting prices below marginal cost as an attempt to gain market share and drive competitors out of business.

---

[11] For examples see VRBO, Homarama, and Homeaway. In addition, sites like Hometogo and Tripping help consumers compare offerings between these different sites.

[12] David S. Evans, "Attention to Rivalry Among Online Platforms and Its Implications for Antitrust Analysis," (Research paper 627, University of Chicago Institute for Law and Economics, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195340. Evans finds "there is little evidence that online markets tend to converge to monopoly because of network effects once the analysis focuses on attention as the proper dimension for evaluating competition. Nevertheless, it turns out that competition for attention is highly dynamic with rivals introducing new products and services, some involving drastic innovation, frequently." 3 (footnote omitted).

Ironically, platforms can be accused of doing both even when they are maximizing social welfare and earning low profits.[13]

Daniel Spulber and Christopher Yoo point to factors that are likely to continue increasing the competition that platforms face.[14] One is the continuation of technological changes in network architecture that reduce startup costs and boost both entry and exit by allowing assets to be used for a variety of purposes. Another is a continued increase in total demand or usage, which reduces the importance of fixed costs as a barrier to entry. Finally, they predict that the demand for continued innovation will erode any temporary market power and force companies to constantly invest in new features. Examples of powerful platforms that lost their dominance due to a lack of innovation include Prodigy, AOL, AltaVista, MySpace, and Friendster. New technologies like blockchain for instance, could conceivably pose competitive threats to at least some of the existing platforms. But even if there is little or no disruption over the next few decades of many of the existing platforms, there is no evidence that this implies a diminishment of consumer welfare.

Regulators also fear companies will collude to raise prices or limit competition. But collusion tends to be much more difficult in the case of multisided platforms. In order to be successful, platforms would have to collude on all sides of the market in order to benefit; otherwise competition on those sides of the market where demand is elastic or users multi-home is likely to erode any excess profits.[15] But platforms often face different competitors on different sides, reducing the shared interests among competitors and increasing the number of parties needed to collude. And as noted above, in some cases, one side of the platform is free (usually the consumer side) and on the other side (usually the sales side) there is already robust competition.

Regulators also need to consider the pro-competitive effect of platforms. By reducing entry barriers and making it easier for small, flexible suppliers to reach customers, platforms increase competition in markets

---

[13] David S. Evans and Richard Schmalensee, "The Industrial Organization of Markets with Two-Sided Platforms," (Working paper 11603, National Bureau of Economic Research, Cambridge, Massachusetts, September 2005), http://nber.org/papers/w11603.pdf.

[14] Daniel F. Spulber and Christopher S. Yoo, "Antitrust the Internet, and the Economics of Networks," (Institute for Law and Economics, University of Pennsylvania Law School, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2370050.

[15] David S. Evans and Richard Schmalensee, "The Industrial Organization of Markets with Two-Sided Platforms," 27.

such as books, rides, and home rentals. By reducing the fixed costs needed to participate in the market, platforms reduce prices and increase consumer choice.[16]

Antitrust regulators still need to be watchful, but they cannot merely assume that a platform is behaving in an illegal manner and harming consumers just because it is doing something that they don't like or understand. Instead, they need to make a detailed case-by-case determination about whether total social welfare, including all sides of the market, has been harmed. In the absence of a careful market study, standard antitrust tools may be of limited use. Two of the leading experts on multisided platforms conclude "it is not possible to know whether standard economic models, often relied on for antitrust analysis, apply to multi-sided platforms without explicitly considering the existence of multiple customer groups with interdependent demand."[17]

Regulators should also keep their focus on consumer, not producer welfare. Platforms that provide more choice to consumers and offer a lower price usually lead to some disruption on the producer side. For example, a company like Amazon competes with both small sellers and large sellers. But its success or lack thereof comes from its ability to either provide more choice, better consumer experience (e.g., faster delivery), or lower prices. If that hurts existing sellers, that is not an issue for competition policy authorities, unless the company gained that advantage unfairly.

The problems are even greater when considering the practical difficulties of regulation. Although the conclusions of regulatory analysis may depend heavily on the specific markets involved, the data about demand elasticities, market definition, degree of competition, and interdependence between different sides that is needed to make these judgments may not be available, especially in new markets characterized by rapid technological change. Because of limitations on regulators' ability to intervene wisely, their involvement may often reduce total welfare

Does or should the presence of "network effects" affect the Commission's analysis of competition and consumer protection issues in platform markets?

As explained above, the presence of network effects often pushes platforms toward concentration. This is not because firms are more prone to collude or because competition is less intense. It is because social value is increased as the size of the network grows. Regulatory attempts to artificially constrain the size of networks will reduce social welfare even if they increase competition. Moreover, such efforts may prove to be fruitless since the market contains a built-in tendency for concentration. For example, there is a reason there is one

---

[16] Liran Einev, Chiara Farranato and Jonathan Levin, "Peer to Peer Markets," (Working paper 21496, National Bureau of Economic Research, Cambridge, Massachusetts, August 2015), 11, http://www.nber.org/papers/221496.

[17] David S. Evans and Richard Schmalensee, "The Antitrust Analysis of Multi-Sided Platform Businesses," (Research paper 623, University of Chicago Institute for Law and Economics Olin, January 2013), 2, http://ssrn.com/abstract_id=2185373.

major social network (Facebook), one major professional network (LinkedIn), and one major micro-blog network (Twitter). Consumers benefit greatly from the network effects involved. For example, they don't have to post twice to share information with their friends.

In the rare cases where technology is relatively stagnant and where the firm sells, rather than gives away for free its services, regulation as a monopoly may be appropriate. But monopoly regulation tends to reinforce a lack of innovation rather than challenge it. Where innovation remains the norm, as is the case for most Internet platforms, concern about the anticompetitive aspects of network effects is often overdone. Continued innovation tends to ensure that consumer value is increasing even if profit margins are high. Moreover, the staying power of any one network tends to be exaggerated. Constant innovation raises the threat that incumbents will be displaced by the type of disruptive change that is so difficult for incumbents to prevent.

Antitrust regulators should concentrate on finding cases of clear anticompetitive behavior that clearly harms consumers or reduces economic efficiency. They should ensure that markets remain open to challengers with new technology. Beyond this, regulators should exercise great care to ensure that their actions do not unintentionally lower the value that network products provide to society.

THE INTERSECTION BETWEEN PRIVACY, BIG DATA, AND COMPETITION

Data as a dimension of competition, and/or as an impediment to entry into or expansion within a relevant market

With the increased power and decreased cost of collecting, transmitting, and storing data, as well as an increase in machine-readable data, more and more companies are using more and more data to help them provide goods and services. However, a number of commentators have begun to argue that, in the case of companies aggregating large amounts of data, competition policy should be extended to incorporate concerns about the collection and use of data beyond clear examples of anticompetitive behavior.[18] The general argument is that the mere act of collecting large amounts of data, such as the vast quantities of personal data collected by social-networking platforms, search engines, and e-commerce sites, gives companies an unfair competitive advantage and that competition policy needs to incorporate this analysis.[19]

---

[18] For the most comprehensive argument see Maurice E. Stucke and Allen P. Grunes, Big Data and Competition Policy (New York: Oxford University Press, 2016).

[19] Margrethe Vestager, "Big Data and Competition" (speech before the EDPS-BEUC Conference on Big Data, Brussels, September 29, 2016), http://ec.europa.eu/commission/2014- 2019/vestager/announcements/big-data-and-competition_en; European Commission, "Online Platforms and the Digital Single Market Opportunities and Challenges for Europe" (communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, May 25, 2016 COM(2016) 288), 13, http://eur-

To date, U.S. regulators have not adopted this line of reasoning, nor should they. While it is true that data can be used in anticompetitive ways, competition policy is capable of dealing with such abuses. In fact, when analyzing allegations of such behavior, it is often helpful to imagine whether agencies would object if the activity complained about involved some input of critical importance other than data. This helps clarify whether the threat to competition is truly due to control of an important resource or to ungrounded fears about the uniqueness of data.

Advocates for intensifying competition policy cite a variety of purported flaws in the current system. However, ITIF, as well as other defenders of the current approach seldom argue that there can be no anticompetitive behaviors when it comes to data. Rather, ITIF and others say that, in some cases, data use—rather than data collection—could trigger competitive concerns.[20] What defenders do argue is that, when it comes to competition policy, the focus should be on abusive behavior and not on structural issues, such as how much data a company holds. Extending competition review to examine the level of data companies hold will send a signal to companies that they should not do the hard work of collecting data, most of which is used to expand social and economic welfare.

The collection of large amounts of data does not by itself represent a threat to competition. Although use of data might in specific circumstances justify regulatory intervention, in most cases the acquisition and use of data does not reduce competition, and the existing legal framework, including traditional interpretations of existing statutes, gives competition and data protection regulators all the flexibility they need to protect

---

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288. See also UK Competition and Markets Authority (CMA), "Online Platforms and the EU Digital Single Market" (written evidence, (OPL0055), CMA, London, October 23, 2015), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internalmarket-subcommittee/online-platforms-and-the-eu-digital-single-market/written/23391.html. "To the extent that such data is of central importance to the offering but inaccessible to competitors, it may confer a form of 'unmatchable advantage,' making it hard for those competitors to compete"; Organization for Economic Co-operation and Development (OECD), Committee for Information, Computer and Communications Policy, "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by 'Big Data,'" (Paris: OECD, Directorate for Science, Technology and Industry, June 18, 2013), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2012)9/FINAL&docLanguage=En. "Data are a core asset that can create significant competitive advantage and drive innovation, sustainable growth, and development."

[20] Daniel Castro, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help," Center for Data Innovation, November 6, 2017, http://www2.datainnovation.org/2017-open-apis.pdf.

markets and consumers. On the contrary, large amounts of data, including personal information, are increasingly a vital input for some of the economy's most important innovations, including online platforms, medical diagnoses, digital assistants, language translation, urban planning, and public safety. Moreover, data is non-rivalrous: Multiple companies can collect, share, and use the same data simultaneously. That goes for consumers, too: When consumers "pay with data" to access a website, they still have the same amount of data after the transaction as before, allowing them to share the same data with multiple companies.

Finally, it is important to note that some of the platforms that collect large amounts of consumer data are natural monopolies: they gain significant market share because of economies of scale and scope, and what economists call "network effects." By providing platforms for users around the world to connect, their very size generates enormous economic benefits for society and consumers. These platforms serve two-sided markets, and many of these businesses, especially those provided free services, face competition on the advertising side.

Competition on privacy and data security attributes (between, for example, social media companies or app developers), and the importance of this competition to consumers and users;

Proponents of expanding the scope of antitrust review to incorporate how companies collect and use data make a variety of arguments. In a paper that largely rejects these claims when applied to concerns about privacy, FTC Commissioner Maureen Ohlhausen and attorney Alexander Okuliar list four arguments proponents make:

1. Privacy is a non-price dimension of competition that can be hurt if some companies have too much market power.
2. Antitrust authorities should not focus solely on the impact on competition in cases where competitive agreements also affect consumer protection but instead should include noncompetition effects in their balancing of costs and benefits.
3. Antitrust authorities should take action when companies achieve monopoly power by misleading consumers about their data-collection policies.
4. Competition law should look at privacy issues even if no competitive implications exist.[21]

[21] Maureen K. Ohlhausen and Alexander P. Okuliar, "Competition, Consumer Protection, and The Right [Approach] to Privacy," Antitrust Law Journal 80 (2015): 134–36. In rejecting attempts to incorporate privacy concerns into antitrust policy, the authors point to three major problems: 1) Antitrust deals with harm to competition, not to privacy harms; 2) Antitrust is concerned with market-wide effects whereas privacy policy focuses on the individual relationship between the

As Commissioner Ohlhausen points out, the U.S. Supreme Court has used a series of cases to make it clear that the primary criterion for antitrust enforcement is economic efficiency.[22] And this is how it should be. U.S. regulators cannot use their powers to address speculative threats to competition. They must present the courts with sufficient evidence to conclude that a merger would result in real harm to consumers. The European Commission faces similar restraints because companies can appeal its decisions in the courts. This rightly constrains the agencies' ability to adopt a different standard even if they wanted to.

It is, of course, true that some companies have tighter privacy policies than others. But consumers generally have a lax attitude toward privacy; they say they want more of it, but they voluntarily share a lot of personal information online and generally do not support websites that cost even a little more, even when they claim to have better privacy practices.[23] So there is no evidence a robust demand for enhanced privacy is going unmet, nor is there evidence that consumers have been harmed by the data practices of major platform companies.

More significantly, consumer-protection agencies have sufficient powers to ensure that companies honor any pledges they make about their data policies and comply with existing privacy regulations. They also have broad authority to address problems arising from the actual misuse of data. In the United States, a variety of laws protect privacy in specific market areas. Examples include the Children's Online Privacy Protection Act, the Health Insurance Portability and Accountability Act, and the Fair Credit Reporting Act. In the European Union, the protection of personal data is enshrined in the EU Charter of Fundamental Rights, and enforced via the ePrivacy directive and the General Data Protection Regulation (GDPR). These laws apply as much to data-rich tech giants as small start-ups. If policymakers are concerned with privacy, they are certainly capable of enacting stricter privacy laws as the EU has done, although if done improperly these regulations can have significant economic costs.[24]

Moreover, there is little evidence that providing users with more privacy gives a company a competitive advantage; otherwise more companies would be competing on this basis. So there is little reason to think that

---

company and the consumer; and 3) Antitrust remedies are inadequate to handle privacy concerns because companies can accomplish the same outcome through private contracts rather than a merger;

[22] Ohlhausen and Okuliar, "Competition, Consumer Protection, and The Right [Approach] to Privacy, 141–43.

[23] Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use," Information Technology & Innovation Foundation, July 2018, http://www2.itif.org/2018-trust-privacy.pdf.

[24] Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies" (Information Technology and Innovation Foundation, September 10, 2015), https://itif.org/publications/2015/09/10/privacy-panic-cycle-guide-public-fears-about-new-technologies.

more competition on privacy would occur even if markets were perfectly competitive. From the company's point of view, privacy restrictions limit possible data uses and therefore reduce revenues and the quality of service. And, despite what privacy advocates might wish, there is little evidence that consumers will pay an appreciable amount for restrictions on how their data can be used.[25]

The market for privacy is imperfect. Therefore, we should not expect it to solve all the privacy preferences of all users, since those preferences are so diverse. But this does not mean that decisions on antitrust issues should be driven by privacy concerns or that privacy laws are inadequate. There is no evidence that any lack of competition in providing services that feature greater privacy protections is due to entry barriers rather than a lack of consumer demand. Consumers may say they value privacy when surveyed, but the way they "vote with their clicks" suggests that they are more than satisfied with their current choices. Therefore, regulators should apply traditional competition analysis to the competitive aspects of a problem and use privacy laws to deal with privacy issues.

Privacy law relies heavily on the standard of informed consent to the use of personal data. But privacy advocates increasingly question the degree to which standard terms of use statements truly imply user consent.[26] It is true that few users read these documents and that to use these services one has to agree to the company's policies. But that does not mean that the documents serve no purpose. First, they provide a record of how the company intends to collect and use data. This can subject companies to public scrutiny and criticisms by those who think they are unfair. Unfortunately, the threat of legal action can motivate the company to draft extremely comprehensive terms that incorporate any possible future uses it might imagine. This makes it difficult for users to understand which uses are actually likely. Nevertheless, the terms of use can create a market for more private services by allowing private groups to study them and inform consumers about their contents and whether any abuses have occurred.

---

[25] Alistair R. Beresford, Dorthea Kübler, and Sören Preibusch, "Unwillingness to Pay for Privacy: A Field Experiment" (Social Science Research Center Berlin, June 2010), http://ftp.iza.org/dp5017.pdf.

[26] Stucke and Grunes, Big Data and Competition Policy, 326–27, "The consensus is that the current noticeand-consent regiment [sic] is inadequate to safeguard privacy. Individuals are generally unaware who has access to their personal information, what data is being used, how the data is being used, when the data is used, and the privacy implications of the data's use."

Second, these agreements serve as terms of the contract between the company and the users. Regulators have taken action against companies for violating their own terms.[27]

Third, it is hard to see any other alternative. Contracts of adhesion are widely accepted in many markets because they reduce transaction costs, especially in instances where it would be impractical to negotiate with every user or provide a menu of alternatives. Perhaps most important, the terms of use do not prevent legislators or privacy regulators from enacting binding laws on how companies protect and use data, irrespective of what the terms of use say. The main reason that this rarely happens is because there have been relatively few instances of companies engaging in clearly inappropriate behavior, and those have been handled by narrow disciplinary actions rather than broad regulation. Since Internet platforms have few valuable assets other than their brand and user base, they have an incentive to build a reputation for trust. This does not always overcome the temptations of profit or secrecy, but that is true for every industry. Past experience shows that users are willing to punish companies that misuse their data.[28]

Finally, any discussion of data and privacy has to recognize that there is no free lunch. Restrictive data policies reduce the economic value of data, and that means less revenues will be available for firms that rely on data for their business model. The result is either that free services will no longer be free, or that companies will have less resources to continue to innovate and improve the customer experience.

THE COMMISSION'S REMEDIAL AUTHORITY TO DETER UNFAIR AND DECEPTIVE CONDUCT IN PRIVACY AND DATA SECURITY MATTERS

The FTC provides an important function in protecting consumers and ensuring competition in many areas of the U.S. economy. In addition to having authority to investigate and combat unfair and deceptive practices, the FTC enforces multiple sector specific laws, such as the CAN-SPAM Act, the Children's Online Privacy Act, the Truth in Lending Act, the Equal Credit Opportunity Act, and the Fair Credit Reporting Act. While the FTC has done much to protect consumer privacy and security, there are opportunities to better protect consumers while at the same time encouraging innovation in today's digital economy.

---

[27] Lisa Kimmel and Janis Kestenbaum, "What's Up With WhatsApp? A Transatlantic View on Privacy and Merger Enforcement in Digital Markets," Antitrust, Fall 2014, 49, (citing both the Nielson Holdings/Arbitron and Reuters/Thompson mergers), https://www.crowell.com/files/Whats-Up-WithWhatsApp.pdf

[28] Laura M. Holson, "To Delete or Not to Delete: That's the Uber Question," The New York Times, November 21, 2014, http://www.nytimes.com/2014/11/23/fashion/uber-delete-emil-michaelscandal.html.

The FTC Should Limit Its Enforcement Actions for Unfair and Deceptive Conduct to Cases Where There Is Concrete Consumer Harm

The FTC's enforcement actions send important signals to businesses in the private sector about how they should allocate their resources to comply with laws and regulations. Ideally, these signals should encourage businesses to take actions that protect consumers and discourage businesses from taking actions that harm consumers; while not discouraging companies from taking risks that might generate innovation that is beneficial to consumers. Unfortunately, this has not always been the case as the FTC has taken action against companies even when lacking evidence of tangible consumer harm (see, for example, ITIF's discussion of the FTC's actions against Nomi Technologies despite finding no action of consumer injury).[29]

In the context of data, harm refers to the extent to which consumers are materially and negatively impacted by misuse of their personal information, which they could not have reasonably avoided themselves. Harms can come in several forms.[30] Autonomy violations result in harm for consumers when information they consider sensitive and would prefer to keep private becomes public through involuntary means. Harms that arise from autonomy violations are often reputational or interpersonal. Discrimination occurs when personal information is used to deny a person access to something, such as employment, housing, loans, and other goods.[31] Finally, economic harm occurs when a consumer suffers a financial loss or damage because of the misuse of their personal information. Most economic harms that result from personal information are identity theft, fraud, or larceny, which are not the primary focus of most privacy policies and regulation. A harm-based standard is important because cultural norms and standards over what individuals consider privacy-invasive and what they are willing to share changes over time, and this type of regulatory principle will adjust with changing expectations.

---

[29] Daniel Castro, "Testimony of Daniel Castro on Legislative Hearing on 17 FTC Bills," Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, May 24, 2016, http://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-CastroD-20160524.pdf.

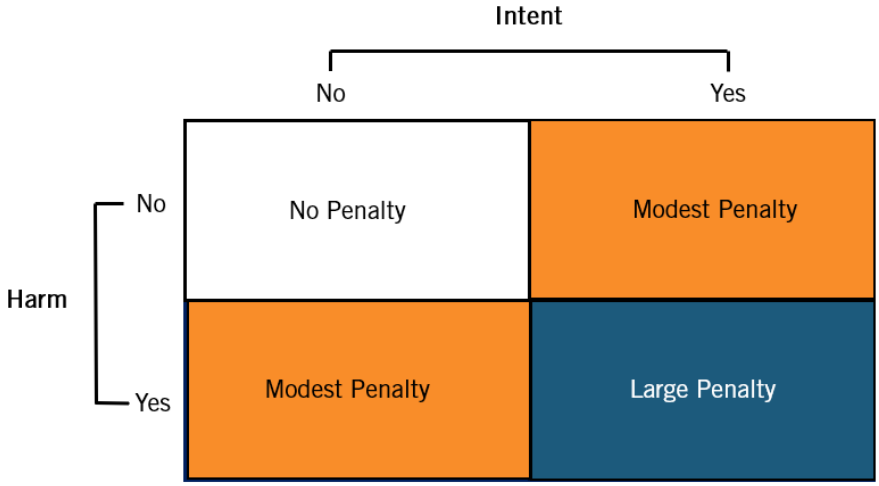
[30] Robert Atkinson, Daniel Castro and Alan McQuinn, "ITIF Filing to FTC on Informational Injury Workshop" (Information Technology and Innovation Foundation, October 27, 2017), https://itif.org/publications/2017/10/27/itif-filing-ftc-informational-injury-workshop.

[31] There are many types of discrimination, including based on age, class, disability, employment, language, gender, genetic information, national origin, pregnancy, race or ethnicity, religion, sex, sexual orientation, and more.

How and When the FTC Should Intervene With Unfair and Deceptive Conduct

As described in Figure 1, when deciding whether to take enforcement measures, ITIF recommends that the FTC consider two key factors: the extent to which a company acted intentionally or negligently, and the extent to which a company's action caused real, substantial consumer harm. Importantly, the FTC should not subject companies to punitive measures for actions they take in good faith that did not cause consumer harm because doing so would force companies to prioritize regulatory compliance rather than preventing consumer injury (e.g., hiring privacy lawyers to rewrite their online terms of service to minimize legal exposure from a data breach rather than hiring security experts to remedy cybersecurity vulnerabilities). In addition, the FTC should treat companies whose maleficence, negligence, willful neglect, or ineptitude results in harm to consumers differently than those that harm consumers through unintentional missteps as they strive to create innovations that benefit society. While penalties will be required in both scenarios, the FTC should save its most aggressive enforcement actions for the former.[32] Moreover, it is important for the FTC to understand that the digital economy, unlike business practices in the "analog" economy, is anything but mature. New technologies, consumer offerings, and business models are continuing to emerge. In such an environment, consumer protection regulation needs to ensure that it is not so strict and punitive as to harm innovation, especially in cases where there was no intent to do harm and where no harm was done.

Figure 1: Recommended level of regulatory penalty based on harm and intent/negligence.



[32] Daniel Castro, "Latest Privacy Kerfuffle Shows Limits of Proposed Privacy Legislation," *Innovation Files*, February 21, 2012, accessed August 8, 2018, http://www.innovationfiles.org/latest-privacy-kerfuffle-shows-limits-of-proposed-privacylegislation/.

The FTC should pay attention to harm and intent when using its enforcement authority against companies involved in unfair and deceptive conduct to avoid creating perverse incentives.[33] The FTC should use these criteria to decide on the appropriate response, where unintentional and harmless actions elicit the smallest penalty and intentional and harmful actions elicit the largest. Penalties should be designed to encourage companies to make sure they do not willfully commit infractions or impose real harm on users. Intent refers to the extent to which companies willfully choose to commit a certain act. For enforcement purposes, negligence, willful neglect, and ineptitude should also be considered intentional actions. By focusing on intent, the FTC can better determine which companies are acting in good faith to bring innovation to market and which are maliciously engaging in unfair or deceptive practices.

Consider the following the following four scenarios:

Scenario 1: A company makes a mistake that does not result in tangible consumer harm. In this instance, regulators should work to resolve the complaint, but not impose any penalties. For example, many tech companies publish written policies describing their products and services, but with the rapid pace of change, these descriptions can become out of sync with the latest versions. Certainly, companies should strive to keep these updated, but in the race to innovate, it is not surprising that on occasion something gets overlooked. When this happens, companies should not face punitive sanctions for actions that do not cause consumer harm and that are undertaken in good faith. Moreover, if the FTC pursues large penalties against companies for deviating from their stated policies, it may simply push companies to create broader, less transparent policies that exempt them from future liability and do not enhance consumer protections. Negligence should be considered intentional, thus harm caused by negligence does not fall into this category.

Consider the case the FTC brought against Nomi Technologies, a company that provided in-store retail analytics.[34] The FTC's complaint stated that Nomi included a partially incorrect statement in its privacy policy about how consumers could opt out of data collection at retail locations—an option that Nomi was under no legal obligation to provide.[35] Nomi's privacy policy stated, "Nomi pledges to… always allow consumers to opt out of Nomi's service on its website as well as *at any retailer using Nomi's technology*"

---

[33] Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene."

[34] Joshua Wright, "Dissenting Statement of Commissioner Joshua D. Wright," Federal Trade Commission, April 23, 2015, accessed August 8, 2018, http://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf.

[35] "In the Matter of Nomi Technologies, Inc.: Complaint," Federal Trade Commission, accessed August 8, 2015, http://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf.

(emphasis added).[36] This was an error because while it offered consumers the ability to opt out of data collection on its website from all of its retail partners, none of its retailers offered consumers a separate, in-store, opt-out mechanism. Importantly, the FTC provided no evidence that any consumers were even affected, let alone harmed. At the time, Chairwoman Ramirez and Commissioners McSweeny and Brill argued that some consumers interested in opting out may have visited Nomi's website but chose not to do so. However, the population of potentially affected consumers was miniscule. Only 3,840 consumers even downloaded Nomi's privacy policy.[37] Of that group, how many read the relevant portion of the policy, chose not to opt-out of all tracking using the website, visited at least one retail partner, carried a mobile phone, and wanted to opt-out at a particular store? No one at the FTC identified any consumers who fit this profile.

While the FTC did not impose any civil penalties on Nomi, by formally taking action when there was no injury to consumers, the FTC sent a signal that companies should spend more time on corporate lawyers and less time delivering value to consumers, including through developing privacy-enhancing technologies. This decision told companies like Nomi that they would be better off providing no privacy guarantees to their consumers; that way they will not fall victim to this sort of gotcha-style enforcement action. Rather than bringing a case and settlement against Nomi, the FTC should have shown some regulatory restraint by simply notifying the company of the problem and verifying that it had been corrected. It was a waste of valuable agency resources that could have better been spent pursuing cases involving actual consumer harm.[38]

Scenario 2: A company make an unintentional mistake that results in real, substantial harm to consumers. In this instance, regulators should again work with the company to fix the problem but impose only a modest penalty against the company to mitigate the damage that resulted from the company's error. The purpose of the penalty should be to make consumers whole again or to allocate resources to help prevent similar issues from happening again.

Consider the FTC's enforcement action against Amazon in 2011. At the time, the company faced a growing number of complaints that children had inadvertently accumulated excess charges by making in-app

---

[36] "In the Matter of Nomi Technologies, Inc.: Complaint," Federal Trade Commission.

[37] Wright, "Dissenting Statement of Commissioner Joshua D. Wright."

[38] Maureen Ohlhausen, "Dissenting Statement of Commissioner Maureen K. Ohlhausen," Federal Trade Commission, April 23, 2015, accessed August 8, 2018, http://www.ftc.gov/system/files/documents/public_statements/638361/150423nomiohlhausenstatement.pdf; Wright, "Dissenting Statement of Commissioner Joshua D. Wright," Federal Trade Commission.

purchases.[39] Amazon responded to the enforcement action by contesting the allegations in a letter to the FTC denying the charges and vowed to defend itself in court.[40] It appears these in-app charges were unintentional and Amazon has subsequently acted in good faith to fix the resulting problems.[41] The company first self-corrected in 2012 by requiring a password for in-app charges over $20.[42] When this did not fully solve the problem, the company continued updating its practices and controls to meet the special needs of some consumers.[43] In this case, a substantial penalty is unwarranted since it does not appear that Amazon intended to cause harm to its consumers or violate any laws. As the aforementioned framework describes, the FTC should push for a settlement that ensures that Amazon refunds any mistaken charges and that the described harms cease. The FTC should also recognize that in cases like Amazon's, where the company is adapting to consumer needs and has caused little consumer harm, the Commission should not displace a company's judgment on how best to serve its customers with its own.

Scenario 3: A company intentionally commits an infraction but no harm results from that action. In this case, the FTC should work to resolve the problem and levy a modest penalty against the company. The purpose of the penalty should be to punish those who act irresponsibly or negligently and incentivize better behavior. However, unlike in situations where consumers have been harmed, there is no need to use penalties to try to make consumers whole again.

---

[39] "FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges," Federal Trade Commission, July 10, 2014, accessed August 8, 2018 http://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars.

[40] Recently, a federal judge refused to dismiss the case, and it seems that it will be decided in court. Andrew C. DeVore, "Amazon Letter to FTC," *Scribd*, July 1, 2014, accessed August 8, 2018, http://www.scribd.com/doc/232376130/Amazon-letter-to-FTC, and Brian Fung, "The FTC just scored a victory in its suit against Amazon," *Washington Post*, December 2, 2014, accessed August 8, 2018, http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/02/the-ftc-just-scored-a-victory-in-its-suit-against-amazon/.

[41] "Set Parental Controls for In-App Purchases," *Amazon*, accessed August 8, 2018, http://www.amazon.com/gp/help/customer/display.html?nodeId=201357720, and DeVore, "Amazon Letter to FTC."

[42] Grant Gross, "Amazon allowed kids to spend millions on in-app purchases, FTC says," *IT World*, July 10, 2014, accessed August 8, 2018, http://www.itworld.com/article/2696340/it-management/amazon-allowed-kids-to-spend-millions-on-in-app-purchases--ftc-says.html.

[43] Ibid.

For example, Path is a social network that lets users share journal entries, photos, and location information between friends.[44] From the start, Path billed itself as a different kind of social network, one where a user could interact and share personal and private messages and photos with just their closest friends. But despite its privacy hook, Path's service initially violated the Children's Online Privacy Protection Act (COPPA) Rule—which requires operators who knowingly allow children under 13 to use their services to notify parents and obtain consent prior to collection, use, or disclosure of personal information from children under 13—by collecting personal information from approximately 3,000 preteens without first getting consent.[45] In 2013, the FTC brought a complaint against Path for knowingly collecting, using, and disclosing personal information from children, although it did not include any evidence of actual harm to users in its complaint.[46] Path settled with the FTC and paid an $800,000 civil penalty.[47] This case is an example of a company that purposefully gathered information on some of its users in violation of the law, although that violation caused little or no consumer harm. In this case, penalizing the company for violating the law was appropriate to help set an example for other companies.

Scenario 4: A company acts with intent, including negligence, and its actions harm consumers. In this case, the FTC should consider imposing significant penalties. Penalties should both make consumers whole and deter bad behavior in the future. In this way, regulation can help foster innovation within industry by strongly discouraging companies from engaging in practices that both violate the law and harm consumers. By setting an example, the FTC can also spur other companies seeking to minimize their risk and exposure to focus their compliance efforts and update their practices.

Consider the FTC's enforcement action in 2017 against Dish Network, a Colorado-based satellite television provider, for violating the FTC's Telemarketing Sales Rule (TSR), the Telephone Consumer Protection Act,

---

[44] Ellis Hamburger, "Path is back with a new messaging app that can talk to people and places," *The Verge*, June 20, 2014, accessed August 8, 2018, http://www.theverge.com/2014/6/20/5827452/path-is-back-path-talk-messaging-app-acquires-talkto-unlimited-friends-list-dave-morin.

[45] "United States of America, Plaintiff, v. Path, Inc., Defendant," Federal Trade Commission, February 1, 2013, accessed August 8, 2018, http://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc.

[46] "Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books," Federal Trade Commission, February 1, 2013, accessed August 8, 2018, https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.

[47] Ibid.

and state law.[48] The TSR is designed to improve consumer choice regarding telemarketing calls by creating the National Do Not Call (DNC) Registry, a database of phone numbers that consumers can add themselves to which indicates their preference not receive telemarketing calls.[49] The court found that Dish initiated, or caused its telemarketers to initiate, telephone calls to phone numbers on the DNC Registry over 66 million times, in violation of the TSR.[50] Indeed, telemarketers allegedly dialed a single consumer's phone number 15 times in 2010 and 2011, despite its inclusion on the DNC Registry.[51] As a result, Dish received the largest civil penalty ever obtained for a violation of the FTC Act—$168 million. This case is an example of a company that willfully violated the law and violated consumers clear choice to not receive telemarking calls. In this case, the FTC was right to seek an appropriately hefty penalty that both deters other companies from violating the TSR and ensures future compliance from Dish.

When weighing enforcement actions against companies, the FTC should consider several things. First, intentions matter. As companies, especially newer companies, race to innovate, mistakes will inevitably happen. If the FTC wants to foster innovation, it should ensure the punishment fits the crime. Moreover, consumers are better served by targeted rules and enforcement actions that address specific harms. If the FTC focuses on levying large fines and long-term consent decrees for actions that caused little to no harm, companies will focus less on releasing safe, useful products and services, and more on legal fees and internal audits. By following the framework discussed in these comments, the FTC can both protect consumer privacy and advance innovation.

---

[48] "FTC and DOJ Case Results in Historic Decision Awarding $280 Million in Civil Penalties against Dish Network and Strong Injunctive Relief for Do Not Call Violations," Federal Trade Commission, June 6, 2017, accessed August 14, 2018, https://www.ftc.gov/news-events/press-releases/2017/06/ftc-doj-case-results-historic-decision-awarding-280-million-civil.

[49] "Q&A for Telemarketers & Sellers About DNC Provisions in TSR," Federal Trade Commission, August 2016, accessed August 14, 2018, https://www.ftc.gov/tips-advice/business-center/guidance/qa-telemarketers-sellers-about-dnc-provisions-tsr.

[50] "FTC and DOJ Case Results in Historic Decision Awarding $280 Million in Civil Penalties against Dish Network and Strong Injunctive Relief for Do Not Call Violations," Federal Trade Commission.

[51] "Are you owed $1,200? Maybe, if you got a Dish Network telemarketing call," *CBS News*, May 7, 2018, accessed August 14, 2018, https://www.cbsnews.com/news/dish-network-do-not-call-lawsuit-eligible-to-collect-1200-per-call/.

EVALUATING THE COMPETITIVE EFFECTS OF CORPORATE ACQUISITIONS AND MERGERS

Whether the doctrine of potential competition is sufficient to identify and analyze the competitive effects (if any) associated with the acquisition of a firm that may be a nascent competitive threat;

The identification and evaluation of differentiated but potentially competing technologies, and of disruptive or generational changes in technology, and how such technologies affect competitive effects analysis

These two questions raise several more specific questions that regulators must ask themselves before they make decisions on either general policy or the appropriate response to an alleged anticompetitive action or merger.

What is the appropriate antitrust framework to evaluate acquisitions of nascent technologies?

The general approach that agencies adopt toward nascent technologies can matter a lot. Regulators should by and large welcome new technologies and encourage their growth even if they raise complicated policy issues or challenge the current regulatory framework. In addition, regulators should try to understand the role and nature of new technologies, including the value they potentially deliver and whether multiple versions of similar technology are likely to appear. This will require an appropriate increase in agency resources devoted to keeping talented staff and continuously educating them about the impact of new technology and innovations.

Regulators also need to realize that smaller companies can sometimes have an advantage in developing new technologies because of their focus and specialization. Investors need a way to monetize successes and compensate for risk. Restricting the role of acquisitions may therefore lower the supply of innovation. One way for government to foster the internal growth of small innovators is to revisit some of the Sarbanes-Oxley restrictions enacted in 2002. Regulatory changes that make Initial Public Offerings (IPOs) easier can reduce the pressure to sell.

Even with reforms to IPO laws, many small companies will prefer to be acquired. Larger companies often have the resources needed to take an innovation to scale. A case in point was Google's acquisition of start-up mapping company Keyhole in 2004. Google's very deep pockets, coupled with a willingness of the Google

founders to think boldly, let Keyhole—what became Google Maps—become orders of magnitude larger than anything the Keyhole founders imagined, all the while dropping the price to free.[52]

Moreover, as Wesley Cohen and Steven Keppler found, in large firms the benefits of one innovation are spread out across more units and products, boosting overall R&D efficiency.[53] Moreover, in some industries, such as pharmaceuticals and some internet industries, it is often not realistic to expect a new firm to grow internally. The ability to spend large sums on testing and distribution is vital. Platforms, which already benefit from network effects, may be especially suited to help new technology scale. But even firms in traditional industries can benefit from acquisitions, especially if they access larger distribution networks. A good nontechnical example is Coke's partnership and eventual purchase of the specialty drinks company Honest Tea. Coke vastly expanded the distribution of Honest Tea and gave its investors a profitable exit.

When evaluating mergers involving nascent technology, regulators should ask the following questions:

1. Whether the acquired firm desires to remain independent but is being pressured to sell by targeted competition. If owners of the small company genuinely believe that the acquisition represents their best opportunity for expanding a technology's use and maximizing the firm's value, regulators should be cautious about opposing it. On the other hand, if the firm has been the target of a focused effort to pressure owners to sell, regulators should take a closer look.
2. Whether the acquired firm has the resources to grow without being acquired. As mentioned, IPO reforms may be able to give firms a viable alternative to an acquisition without requiring a change in merger law. But unless nascent technology has an outlet to grow, it cannot have a large impact on markets and benefit consumers and economic growth.
3. Whether the acquirer is likely to use the new technology to enter a new market or stifle it in existing markets.
4. The degree to which users of the new technology must also use the acquirer's existing products in order to benefit from them. In the latter case, the potential for an anticompetitive effect is greater. In the former case, the acquiring firm's profits will depend on ensuring that the technology delivers significant benefits to users.

---

[52] Robert D. Atkinson, "Review of Never Lost Again: The Google Mapping Revolution That Sparked New Industries and Augmented Our Reality," New York Journal of Books, June 2018, https://www.nyjournalofbooks.com/book-review/never-lost-again.

[53] Wesley M. Cohen and Steven Klepper, "A Reprise of Size and R & D," *Economic Journal* 106, no. 437 (July 1996): 948, http://www.jstor.org/stable/2235365.

How should the FTC evaluate whether a nascent technology is likely to develop into a competitive threat in dynamic, high-tech markets?

Determining the value of nascent technology is extremely difficult. One reason is that success can depend on the company's business model and competency even more than on the specific technology. Many companies have had great technology but lacked the insight and leadership to develop and market it. Regulators should engage in discussions with all parties, including those both supportive and opposed to a merger, to increase their understanding of the significance and likely future of new technology. Interviews with professional investors can also provide independent views about future outcomes.

Regulators can also look to see whether similar technologies are being developed elsewhere. The existence of similar technology is a sign that its introduction will be broad based rather than limited to one company. This raises fewer antitrust concerns since customers will have more sources to benefit from the technology. It also indicates that the technology is likely to have a significant impact on the market.

Other signs regarding the degree of competitive threat are the amount of patent protection (more protection means that other sources for the technology may not be quickly available) and the internal resources of the owner of the technology. Regulators also need to look at regulatory barriers to nascent technology, including at the state and local level. Regulation can often be a greater barrier to innovation than any alleged anticompetitive behavior. When appropriate, the Commission should attack these regulatory barriers to competition.

What is the appropriate evidentiary standard for potential competition and loss of innovation cases?

Antitrust law should remain focused on consumer benefit, innovation and economic efficiency. Using the consumer welfare test, regulators should have to explain by a preponderance of the evidence why a proposed merger will either 1) eliminate a potential challenger who is both likely to become a significant competitor and develop and scale the technology in question as well or better than the combined firm; or 2) give the buyer a significant technological advantage in a market where there is little competition and where this reduced competition is likely to be used reduce consumer welfare. This latter point requires accurate market definition, because in the case of free internet services, for example, the relevant market is advertising. These two factors would establish a rebuttable presumption that the merger should not go forward. The company should then get a chance to rebut the government's case.

The main standard should remain consumer welfare (or more broadly, innovation and economic efficiency). There is currently an active debate about whether antitrust law should also try to accomplish other objectives such as privacy and job protection and whether regulators should oppose consolidation even when it presents no harm to consumers. The policies of the last 30 years have resulted in a consensus about the proper role of antitrust policy in the economy. Debate will continue about exactly how to apply the consumer welfare

standard and how to resolve difficult cases, but agencies should not throw out these accomplishments by introducing more uncertainty into how the law will be applied. Job loss and privacy in particular are not issues that should be included in competition policy. For the former, one major goal of competition is productivity growth. Mergers that result in greater productivity clearly boost economic growth and consumer welfare. Restricting business behavior, including mergers, because it might lead to job loss is to turn competition policy into a tool to restrict economic growth.

For the latter, privacy deserves no consideration in competition policy, including merger review. Privacy policy is already enforced by the FTC's Bureau of Consumer Protection. Moreover, if two firms with different privacy policies merge, the merged firm cannot apply the weaker, more permissive policy to all the data in the now combined firm, unless its policies already allows such a change or it obtains affirmative permission from its customers.

Regulators should also ask whether acquiring firms continuously invest in new technologies. Do they spend a high portion of value added on research and development (both with and without mergers)? Companies that focus heavily on innovation are unlikely to relapse into a stagnant defense of their existing market share. They are also more likely to maximize the social value of a nascent technology whether it is developed internally or is acquired through a merger. Another important variable is the degree to which the industry is susceptible to Schumpeterian competition. Is the potential for disruptive technological change high? If it is, companies that do not continuously seek to increase consumer value through innovation are likely to lose market share. Similarly, regulators should ask about the overall pace of technology in the industry. If it is high, then the impact of specific deals is likely to be less. The presence of constant innovation is usually more important than the level of short-term competition.

Mergers are more problematical if the acquisition of new technology enhances a company's presence in an existing, relatively mature market as opposed to boosting its competitiveness in a new market. Technology that lets a large company expand into new markets raises fewer problems because the company does not have a dominant position to protect and likely faces a number of challengers.

Should the Horizontal Merger Guidelines be revised to clarify potential/nascent competition analysis?

For most purposes the existing Guidelines are accurate. They represent consensus opinions rooted in decades of agency actions and court decisions. But updated Guidelines on specific issues, such as the role of nascent technology and innovative industries, can provide companies and courts with greater certainty about how the government will apply antitrust laws. This can increase the number of beneficial mergers and cut the number of bad ones. Guidelines also protect the agencies from outside pressure to challenge mergers that do not violate the guidelines.

Should data-driven dominance be factored into antitrust reviews of nascent technology acquisitions? If so, how?

Data should be looked at in antitrust cases. Like technology, an experienced workforce, physical capital and access to suppliers, it increasingly represents an important input into many markets. But before concluding that data gives a company an unfair competitive advantage, regulators should consider that:

1. The volume of data is often less important than the algorithms or business practices that derive value from it. As with nascent technologies, the mere possession of good data does not automatically result in market power or high profits. The data has to be used in a way that confers real value to users.
2. Large amounts of data are often available privately to any party that wants to buy it. The key constraint is translating the data into a competitive product.
3. Data often has a short shelf-life. Any market advantage it provides is temporary. Thus, companies that do not continuously offer the best services at the best prices will gradually lose market share.
4. Large amounts of data are often vital to the network effects and efficiencies of scale that maximize consumer value. Having more data increases social value. The tendency of many markets, including those dominated by platforms, is toward concentration. This is not due to anticompetitive actions. It is due to diminishing costs and increasing value as products capture a larger market share. Consumers are usually the main beneficiaries of this scale.
5. Data is nonrivalous. Sharing it with one party does not preclude a consumer from sharing it with others. And one party's use of data seldom infringes on another party's use of the same data.
6. Forced sharing of data raises important questions of consent and security. Moreover, the gathering and use of data needs to be protected by appropriate protections for intellectual property because without this the incentives to invest in data collection, development and innovation would be reduced.

THE CONSUMER WELFARE IMPLICATIONS ASSOCIATED WITH THE USE OF ALGORITHMIC DECISION TOOLS, ARTIFICIAL INTELLIGENCE, AND PREDICTIVE ANALYTICS

Some people are concerned that algorithmic decision-making will result in racial bias, such as financial institutions denying loans on the basis of race. However, in many cases, because flawed algorithms hurt the company using them, businesses have strong incentives to not use biased algorithms and regulators are unlikely to need to intervene. For example, banks making loans would be motivated to ensure their algorithms are not biased because, by definition, errors such as granting a loan to someone who should not receive one, or not granting a loan to someone who is qualified, costs banks money. In addition, even if some companies do not have a financial incentive to avoid biased algorithms, existing laws that prohibit such discrimination, such as the Fair Credit Reporting Act and the Equal Credit Opportunity Act, still apply.

Another argument regarding the inadequacy of privacy laws to protect consumer welfare is that the collection of large amounts of data allows companies to discriminate against consumers, including practicing price

discrimination, charging different consumers different prices depending upon the likelihood that they will buy a product.[54]

Indeed, there is some evidence that companies are getting quite good at doing this.[55] This is often combined with the worry that disadvantaged groups will end up paying higher prices. But there are two reasons why price discrimination might not be a bad thing. First, to the extent that a platform has market power and can only set one price, its incentive is to raise prices on everyone and decrease supply. This allows the company to capture more value from the product and lowers the total benefit to society. If the company can charge different prices to different users, this social loss is reduced. Some consumers might still pay higher prices, but buyers will not purchase a product unless it makes them better off. Second, the ability to charge different prices is not limited to raising prices. Companies also have an incentive to lower prices for consumers who are reluctant to purchase the good.[56] This effect might actually be progressive. The company will charge a higher price to those users whose demand is inelastic. To the extent that lower-income consumers are more price responsive, they will benefit from price discrimination.[57]

More broadly, the FTC should recognize that consumers as a whole are going to benefit from greater use of algorithms, particularly artificial intelligence (AI). Though there are concerns about the potential harms that could arise from the use of AI, such as AI exacerbating unconscious human bias, the proposals that have gained popularity among consumer advocates to address these harms would be at best largely ineffective and at worst cause more harm than good. The two most popular ideas—requiring companies to disclose the source code to their algorithms and explain how they make decisions—would cause more harm than good by regulating the business models and the inner workings of the algorithms of companies using AI, rather than holding these companies accountable for outcomes.

---

[54] Nathan Newman, "The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google," William Mitchell Law Review 40, no. 2 (2014), http://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1568&context=wmlr.

[55] Burton G. Malkiel, "The Invisible Digital Hand," The Wall Street Journal, updated November 28, 2016, http://www.wsj.com/articles/the-invisible-digital-hand-1479168252

[56] Manne and Sperry, "The Problems and Perils of Bootstrapping Privacy and Data Into an Antitrust Framework," 7. "It is inconsistent with basic economic logic to suggest that a business relying on metrics would want to serve only those who can pay more by charging them a lower price, while charging those who cannot afford it a larger one."

[57] The White House, Big Data and Differential Pricing (Washington, DC: The White House, February 2015), 17, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_None mbargo_v2.pdf.

The first idea— "algorithmic transparency"—would require companies to disclose the source code and data used in their AI systems. Beyond its simplicity, this idea lacks any real merits as a wide-scale solution. Many AI systems are too complex to fully understand by looking at source code alone. Some AI systems rely on millions of data points and thousands of lines of code, and decision models can change over time as they encounter new data. It is unrealistic to expect even the most motivated, resource-flush regulators or concerned citizens to be able to spot all potential malfeasance when that system's developers may be unable to do so either.[58]

Additionally, not all companies have an open-source business model. Requiring them to disclose their source code reduces their incentive to invest in developing new algorithms, because it invites competitors to copy them. Bad actors in China, which is fiercely competing with the United States for AI dominance but routinely flouts intellectual property rights, would likely use transparency requirements to steal source code.[59]

The other idea—"algorithmic explainability"—would require companies to explain to consumers how their algorithms make decisions. The problem with this proposal is that there is often an inescapable trade-off between explainability and accuracy in AI systems. An algorithm's accuracy typically scales with its complexity, so the more complex an algorithm is, the more difficult it is to explain. While this could change in the future as research into explainable AI matures—DARPA devoted $75 million in 2017 to this problem—for now, requirements for explainability would come at the cost of accuracy.[60] This is enormously dangerous. With autonomous vehicles, for example, is it more important to be able to explain an accident or avoid one? The cases where explanations are more important than accuracy are rare.

Fortunately, regulators have an alternative to these flawed approaches. Instead of pursuing heavy-handed regulations or ignoring these risks, they should adopt the tried-and-true approach of emphasizing light-touch regulation, with tailored rules for certain regulated sectors that fosters the growth of the algorithmic economy while minimizing potential harms. The challenge for regulators stems from the fact that innovation, by its very nature, involves risks and mistakes—the very things regulators inherently want to avoid. Yet, from a societal perspective, there is a significant difference between mistakes that harm consumers due to maleficence, negligence, willful neglect, or ineptitude on the part of the company, and those that harm

---

[58] Will Knight, "The Dark Secret at the Heart of AI," *MIT Technology Review*, April 11, 2017, https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/.

[59] Joe Uchill, "China Broke Hacking Pact Before New Tariff Fight," *Axios*, April 10, 2018, https://www.axios.com/china-broke-hacking-pact-before-new-tariff-tiff-d19f5604-f9ce-458a-a50a-2f906c8f12ab.html.

[60] Cliff Kuang, "Can A.I. Be Taught to Explain Itself?," *New York Times Magazine*, November 21, 2018, https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html.

consumers as a result of a company striving to innovate and benefit society. Likewise, there should be a distinction between a company's actions that violate regulations and cause significant harm to consumers or competitors, and those that cause little or no harm. If regulators apply the same kind of blanket penalties regardless of intent or harm, the result will be less innovation.[61]

To achieve a balance, regulators should take a harms-based approach to protecting individuals, using a sliding scale of enforcement actions against companies that cause harm through their use of algorithms, with unintentional and harmless actions eliciting little or no penalty while intentional and harmful actions are punished more severely. Regulators should focus their oversight on operators, the parties responsible for deploying algorithms, rather than developers, because operators make the most important decisions about how their algorithms impact society.

This oversight should be built around algorithmic accountability—the principle that an algorithmic system should employ a variety of controls to ensure the operator can verify algorithms work in accordance with its intentions and identify and rectify harmful outcomes. When an algorithm causes harm, regulators should use the principle of algorithmic accountability to evaluate whether the operator can demonstrate that, in deploying the algorithm, the operator was not acting with intent to harm or with negligence, and to determine if an operator acted responsibly in its efforts to minimize harms from the use of its algorithm. This assessment should guide their determination of whether, and to what degree, the algorithm's operator should be sanctioned. Defining algorithmic accountability in this way also gives operators an incentive to protect consumers from harm and the flexibility to manage their regulatory risk exposure without hampering their ability to innovate.

This approach would effectively guard against algorithms producing harmful outcomes, without subjecting the public- and private-sector organizations that use the algorithms to overly burdensome regulations that limit the benefits algorithms can offer.

Sincerely,

Rob Atkinson
President, Information Technology and Innovation Foundation

Daniel Castro
Vice President, Information Technology and Innovation Foundation

---

[61] Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene," (Information Technology and Innovation Foundation, February 2016), http://www2.itif.org/2015-how-when-regulators-intervene.pdf.

Doug Brake
Director, Broadband and Spectrum Policy, Information Technology and Innovation Foundation

Alan McQuinn
Senior Policy Analyst, Information Technology and Innovation Foundation

Josh New
Senior Policy Analyst, ITIF's Center for Data Innovation