Comment

The limits of antitrust in privacy protection

Eugene Kimmelman*, Harold Feld** and Agustín Rossi***

Key Points

- Antitrust has been put forward as a tool to defend consumers' privacy.
- Antitrust should encourage non-price competition, and can be the right tool to fight anti-competitive hoarding of personal data.
- However, antitrust in general is not the right tool to address, nor the right conceptual framework to analyse, privacy harms.
- Instead, a comprehensive approach to consumer protection is needed.

Introduction

In the 21st century, it has become virtually impossible to meaningfully participate in society without revealing our personal data. Many of the most necessary, entertaining, and useful internet services demand personal data that are then used for targeted advertisements as a condition of use. Service providers follow us around the Internet and across devices to show us ads and to collect more data. Credit rating agencies and financial institutions determine our access to mortgages and car loans based on the data they relentlessly collect from as many sources as possible. And even supermarkets indefinitely collect and store our payment and delivery information and our shopping history.

Many consumers are unsatisfied with this state of affairs. Some find it abusive that their privacy is the price to pay for access to socially or economically unavoidable internet platforms. Others hate to be paying twice for their internet service, both with their money and with their personal information. And all are outraged by data breaches, hacks, revelations of corporate and state surveillance, and other social and political scandals. Consumers in the USA, the European Union (EU), and elsewhere want more control over their personal data, and they demand privacy protection.

Many solutions have been put forward to defend consumers' privacy. The proponents of antitrust as a privacy remedy provide a variety of rationales, often interrelated, which this paper will briefly explore.[1] One is that dominant platforms can impose abusive terms over their users who then have no way of leaving the service because network effects leave them effectively locked in. Another rationale is that antitrust promotes consumer welfare by ensuring consumer choice and that antitrust enforcement should guarantee that there is non-price competition including in different levels of privacy protection.[2] A third one suggests that companies should be held accountable under antitrust law when they mislead or deceive consumers about the personal data collection practises that helped them achieve monopoly power.[3] And finally, there are those who believe that the possession of personal data should be viewed as a potential barrier to future competition and considered during merger review, even when a merger wouldn't otherwise have significant vertical or horizontal competitive effects.[4]

The above arguments show that antitrust has an important, but narrow role in privacy protection. We agree that antitrust should encourage non-price competition, including different levels of privacy protection, and that antitrust can be the right tool to fight anti-competitive

* Eugene Kimmelman, Public Knowledge, Washington, DC 20036, USA
** Harold Feld, Public Knowledge, Washington, DC 20036, USA
*** Agustín Rossi, Public Knowledge, Washington, DC 20036, USA; Email: gus@publicknowledge.org

1 Allen P Grunes and Maurice E Stucke, 'No Mistake About It: The Important Role of Antitrust in the Era of Big Data' (Social Science Research Network, 2015) SSRN Scholarly Paper ID 2600051 <https://papers.ssrn.com/abstract=2600051> accessed 29 June 2018.

2 Robert H Lande, 'The Microsoft-Yahoo Merger: Yes, Privacy Is an Antitrust Concern'. FTC: Watch, February 2008. https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=1721&context=all_fac.

3 Maureen K Ohlhausen and Alexander Okuliar, 'Competition, Consumer Protection, and the Right (Approach) to Privacy' (2015) 80 Antitrust Law Journal 121, 135.

4 Ibid 136.

hoarding of personal data. However, antitrust in general is not the right tool to address, nor the right conceptual framework to analyse, privacy harms.

There are three reasons why the antitrust role in privacy protection should be limited and narrow: (i) advocating for antitrust action requires a significant investment of political energy and time that has a very uncertain and unclear return for privacy protection; (ii) antitrust action can have negative unintended consequences in the absence of an underpinning comprehensive privacy law, such as turning one privacy offender monopolist into several privacy offender competitors; and (iii) antitrust cannot remedy most harms caused by non-dominant players.

First, antitrust cases consume significant amounts of always limited political energy, time, and financial resources in exchange for the vague possibility of an effective increase in privacy protection. According to the Dechert Antitrust Merger Investigation Timing Tracker, on average a significant antitrust merger investigation in the USA took 10 months in 2017 and just a bit less in the EU.[5] And the most relevant cases against big companies that have sparked many demands for leveraging antitrust to protect consumers' privacy tend to take even longer: *United States v Microsoft* took over six years to be settled.[6] In Europe, the *Google Search* case has been open since 2010 and it is still subject to litigation. Simply put, the return on investment of relying on antitrust to protect consumer privacy is non-optimal.[7]

Nor is it the case, as some maintain, that the expense is reduced because many mergers are completed pursuant to settlement agreements and consent decrees that may include specific conditions to protect privacy. Not only are merger reviews time and resource intensive, but they require the relevant competition agency to subsequently invest adequate resources in enforcement. Settlement of an enforcement action, or a consent decree as part of a merger approval, can only be a primary tool for protecting privacy if thoroughly enforced on an ongoing bases like a regulatory regime.

Second, there are many possible negative unintended consequences of using antitrust to protect privacy in the absence of an underlying comprehensive privacy law. Privacy advocates might find that antitrust as a remedy backfires if, for example, the result of an antitrust action against a privacy harming company is that it is divided into several privacy harming companies, none with sufficient market power to be considered dominant. Competition may create incentives to differentiate by providing greater privacy protection, but could as easily promote more intense efforts to obtain personal data.

Third, as we explore in the third section of this paper, the consequences of the individual harm of a privacy violation are the same regardless of the size of the company involved. Non-dominant companies that fall out of the scope of most antitrust scrutiny can harm an individual as much as dominant players. Approaching data protection from the prism of antitrust, which focuses on dominant companies and specific behaviours such as collusion, blinds us from seeing that especially in the absence of an underlying comprehensive privacy protection statute, there are privacy harms committed every day by companies of all sizes and in all types of markets. Given the importance of privacy for people's dignity, political organization, and social life, the protection of personal data should be a goal on its own, standing independently of competition policy.

In this paper, we suggest that a comprehensive approach to consumer protection is needed to deal with the many challenges presented by dominance in Internet and telecommunication platforms and pervasive data collection practises. Policy-makers' and regulators' choice of policy tool should be guided by their intended policy goals and not vice versa. Consumer protection requires tools that can promote accountability and fairness in markets. This includes tools to promote competition, consumer protection, privacy protection, diversity of information, and other public interest values.

This article first explores the limits of antitrust. Then, it explains why privacy is not and has not been correlated with market power. Following, a toolkit of policies to protect privacy and consumers is presented.

What antitrust can actually do, and its limits

Calls to revive antitrust enforcement in the USA particularly in the digital communications and Internet industries are long overdue in light of evidence of increasingly concentrated markets and broader dangers to

5 Dechert LLP, 'DAMITT: How Long Does It Take to Conduct Significant U.S. Antitrust Merger Investigations?' (July 2018) <https://www.dechert.com/knowledge/hot-topic/damitt–how-long-does-it-take-to-conduct-significant-u-s–antitr.html> accessed 19 July 2018.

6 Antonio G Martínez, 'What Microsoft's Antitrust Case Teaches Us About Silicon Valley' (*Wired*, 2018) <https://www.wired.com/story/what-microsofts-antitrust-case-teaches-us-about-silicon-valley/> accessed 19 July 2018.

7 European Commission, 'Summary of Commission Decision of 27 June 2017 Relating to a Proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement' <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018XC0112(01)&from=EN> accessed 19 July 2018.

society such as privacy invasions and data breaches. However, these concerns are often presented in too simplistic a manner. While it is true that in theory, some idealized version of antitrust enforcement may be capable of handling all competitive issues as well as the unintended and undesirable consequences of commercial processing and collection of personal data, neither current antitrust jurisprudence nor contemporary economic analysis supports this vision.[8]

Antitrust analysis tends to be backward-looking, involving observed market outcomes that are considered to be the result of insufficient competition leading to conduct that is harmful to consumers. Structure is examined as the context that makes the conclusions about conduct more plausible. The lack of competition due to high levels of concentration, for example, may make it more likely that dominant platforms will be able to demand more personal data in order to sell more advertisements, but enforcement is triggered only when abuses can be demonstrated. This means that privacy advocates would have to demonstrate, within the existing parameters of antitrust law and practise, that a company is forcing consumers to agree to competition altering terms for the use of their personal data.[9]

Antitrust reviews of corporate mergers reverse this analytical flow because it is the one area where antitrust is forward-looking. That's because structural analysis is central to the complaint that a merger will so greatly increase market concentration as to pose a threat to consumers and competition.

In both antitrust enforcement and merger review, however, the antitrust authorities often prefer structural remedies such as divestiture of assets to shrink market power, rather than remedies that require them to regulate the conduct of companies in the marketplace. This means that market structure, conduct, and performance are focal points, yet basic market conditions receive less attention. In fact, antitrust enforcers do not generally address basic market conditions because they are beyond their legal mandate. In the case of privacy protection, it is unlikely that an antitrust authority will be capable of creating and enforcing generic behavioural requirements to protect consumers' privacy.

Some characteristics of an industry make it unlikely that private investment and market forces will produce socially optimal outcomes. In some cases, investors cannot project or capture the benefits of the production of a common good, such as developing strong cybersecurity practises that protect personal data but might be costly to adopt for one actor if other actors are not following suit. In other cases, consumers cannot project the benefits of more output, such as a so-called network effect, which makes the network more valuable to consumers, who can reach more people, and to marketers, who can identify niches to expand output. These and other basic market attributes may not influence antitrust enforcers one way or the other unless a particular company acts abusively as it takes advantage of network effects.

Today, when calls to strengthen the antitrust oversight over digital platforms increase it's important to remember that even in its 'golden age' of trust busting in the first half of the 20th century, antitrust was never seen as enough.[10] To the contrary, the same time period also saw the first wave of comprehensive consumer protection law to supplement antitrust. Louis Brandeis' arguments in favour of the creation of the Federal Trade Commission emphasized the need for additional authority to protect consumers as a necessary supplement to antitrust. Perhaps even more relevant, it was in the same year the Sherman Act passed that Brandeis wrote his seminal article 'The Right To Privacy'. As Brandeis emphasized, the right to privacy is a personal right as well as an economic right. Legislative recognition of personal privacy rights, he argued, was crucial to living in a society where technology increasingly made it impossible to simultaneously participate in society while preserving personal privacy.

In periods of lax antitrust enforcement, monopolies return

Historically, antitrust enforcement has periods of rigorous enforcement followed by periods of lax enforcement and concomitant reconsolidation. In these periods when antitrust is less rigorously enforced, strong privacy protections become even more critical. While it is certainly true that 'business friendly' administrations may choose to ignore both antitrust and consumer protection, history has shown that these two do not always move in tandem. For example, the Cable Act of 1984 not only largely deregulated the cable industry, but also created one of the strongest sectoral federal privacy statutes enacted by Congress. Additionally, in periods when infrastructure is regulated as a 'natural monopoly', government protection of the monopoly franchise

8 Gene Kimmelman and Mark Cooper, 'A Communications Oligopoly on Steroids—Why Antitrust Enforcement and Regulatory Oversight in Digital Communications Matter'.

9 Ibid.

10 Ibid.

is often accompanied by an increase in federal and state consumer protection oversight.

AT&T is a good example of this dynamic. During the period when AT&T was regulated as a 'natural monopoly', the Communications Act of 1934 imposed privacy obligations enforced by the FCC and by private right of action. As the FCC began to impose pro-competitive regulation to introduce competition into various segments of the telecommunications market (in tandem with the Department of Justice enforcement actions under the Sherman and Clayton Acts), it also began to impose new privacy regulations both to promote competition and to protect consumers. In 1996, with the Telecommunications Act Congress codified and expanded these privacy protections, citing both the pro-competitive and pro-consumer rationales.[11]

At the same time, antitrust enforcement was experiencing a period of decline. The eight regional telephone monopolies that emerged from the government's breakup of the old AT&T national monopoly in the 1980s merged into two dominant wireline and wireless giants, Verizon and AT&T. Similarly, local cable monopolies combined into regional powerhouses—Comcast and Charter—and developed cozy relationships with a similarly consolidating content industry. Lax antitrust enforcement combined with weak regulatory oversight resulted in the growth of what Kimmelman and Cooper call a 'tight oligopoly on steroids'.[12] By the standard definitions of antitrust and traditional economic analysis, a tight oligopoly has developed in the digital communications sector.

Regulatory policy was equally lax, deregulating services that were far from competitive based on the hope or hype that competition would grow in areas such as access to broadband services. As a result, today these four firms (Comcast, AT&T, Verizon, and Charter) enjoy geographic separation, technological specialization, and product segmentation that makes it easy to avoid competition. Nevertheless, this period also saw renewed emphasis on privacy protection. The same FCC that permitted consolidation in the telecom and cable industries also developed strong rules to implement the privacy provision of the 1996 Act, and—until the current administration—regularly expanded these rules to address changes in technology.[13] The FTC expanded its general consumer protection authority to include protecting privacy in the emerging internet economy.

The recent history of the telecommunications sector is a cautionary tale for privacy advocates tempted to leverage antitrust to achieve their goals, and a demonstration of the value of separately enforceable privacy regulation. In 1997, then Chairman of the FCC Reed Hundt declared it would be 'unthinkable' to allow AT&T to combine with a regional Bell operating company.[14] Less than a decade later, the FCC simultaneously approved the acquisition of AT&T by SBC and the acquisition of MCI, the next largest long-distance company, by Verizon. But despite this reconsolidation, consumers (and competitors) continued to enjoy the vigorous privacy protections imposed by the 1996 Act and FCC regulations. Regulation, in sum, should precisely be the main concern of privacy advocates.

Why privacy is not only a market power issue

In 2013, Target announced that the personally identifiable information of 70 millions of its customers had been compromised. Even assuming that Target has significant market power, it is difficult to see how antitrust could deal with harms of this sort. Single-firm conduct is typically only a violation of antitrust law to the extent that it unreasonably restrains competition—despite antitrust's focus on consumer welfare, it will not typically address negligent or risky behaviour by dominant firms, even when such behaviour harms consumers. But even this is beside the point as Target does not likely have enough market power to trigger an antitrust investigation.

Several examples of FCC enforcement of its privacy regulations likewise demonstrate the value of privacy regulation and the limitations of antitrust. Although many of the enforcement actions during the Obama Administration were taken against dominant firms such as AT&T and Verizon, some of the agency's most aggressive enforcement actions were taken against small firms that carelessly exposed sensitive personal information. In 2013, two small telephone service providers exposed sensitive personal information of more than 300,000 applicants to the 'Lifeline' federal subsidy program to access via the Internet without meaningful security protection.[15] These firms were not merely

11 Harold Feld and others, 'Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World' <https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper>.

12 Kimmelman and Cooper (n 8) 7.

13 Feld and others (n 11).

14 FCC, 'News Release: Combination of AT&T and an RBOC "Unthinkable"' <https://transition.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc7041.html> accessed 19 July 2018.

15 See TerraCom, Inc., and YourTel America, Inc. Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13342, para. 50 (24 October 2014). 'Lifeline' is a federal program that provides subsidies to low-income households to purchase telephone service. Not all applicants

non-dominant; they were objectively tiny. Nevertheless, the FCC successfully prosecuted the companies, ultimately entering into a consent decree that included a fine and remedial measures to prevent any future exposure of personal information.[16]

No one would argue that there is less of an obligation to protect the privacy of users of non-dominant platforms—or even of comparatively small platforms—than there is to protect the privacy of users of dominant platforms or that the harms suffered by the consumers of one are less than those suffered by consumers of others. If a small, non-dominant, social network shares a person's health status with third parties without meaningful consent, that person would be as much at risk of work, social, or healthcare discrimination as if the harm had come from a dominant platform. The consequences of discrimination and the limitations to user autonomy based on the disclosure of delicate personal information are the same regardless of the size of the company that violated the trust of the consumer.

Unfortunately, during the Trump Administration, Congress and the FCC have moved to further limit consumer privacy protection online rather than expand it. In March 2017, Congress repealed the Obama-era FCC regulations imposing privacy protection obligations on broadband service providers.[17] In December, as part of its repeal of network neutrality regulations, the Trump FCC explicitly abandoned any authority to protect consumer privacy online.[18] This represented a remarkable break with previous FCC pronouncement that even when deregulating broadband providers from 'economic regulation' it would still protect consumers and consumer privacy.

It is this recent history of inadequate privacy regulation in the USA that often leads advocates concerned with privacy to look to other available regulatory tools. Additionally, the nexus between accumulated personal information and the dominance of internet platforms is properly within the scope of antitrust review, and antitrust enforcement to remedy anticompetitive uses of personal information can, and should, also strive to maximize consumer welfare through vigorous protection of consumer privacy. Similarly, it is the appropriate province of antitrust law to recognize that one of the harms of market dominance may be the ability to coerce consumers into providing personal information in return for either 'essential' or 'unavoidable' services.[19] But this important function of antitrust and the valuable role it plays in protecting consumer privacy should not obscure the importance of stand-alone privacy regulation or the limitations of antitrust as a consumer protection tool.

Principles for effective comprehensive consumer privacy regulation

It is beyond the scope of this article to describe necessary regulation for strong, comprehensive privacy protection. Nevertheless, it is useful to emphasize the different roles of privacy regulation and antitrust by highlighting principles the authors believe should guide Congress and the states in developing effective privacy regulation in the digital age.

Consumers deserve the right to control the use of their personal information. Those who collect and store this personal information have a duty to protect it. When a breach of this trust occurs, the party that failed to properly secure the information should make the individual whole to the greatest extent possible.

Context matters. We all willingly trade information every day, but the circumstances of these decisions vary widely. Where an individual cannot avoid sharing information without forgoing critical services, the law must recognize a greater obligation to protect the information.

This should not be confused with the current arbitrary distinction made between 'sensitive' and 'non-sensitive' information. To illustrate the difference, consider the following example. Sexual orientation may be either sensitive or non-sensitive depending on whether the person is 'out' or 'closeted'. Context will indicate what level of protection should be applied to this information far better than an absolute rule. A celebrity who 'comes out' on social media clearly regards the information not merely as non-sensitive but public. By contrast, visitors of a private Facebook group for homosexuals in countries where homosexuality is illegal clearly regard the information about their sexuality as highly sensitive. Additionally, the 'sensitive' versus 'non-sensitive' dichotomy used by the FTC and proposed by others is

receive Lifeline subsidy, and telephone companies retain the application materials for a period of years even after participants have left the program or the specific carrier. The 300,000 individuals whose information was exposed was therefore considerably more than the number of individuals subscribing to the two companies at the time of the incident.

16 See '$10 Million Fine Proposed Against Terracom and YourTel for Privacy Breaches', 29 FCC Rcd 13325 (rel 24 October 2014).

17 Brian Fung, 'Republicans Voted to Roll Back Landmark FCC Privacy Rules. Here's What You Need to Know' *Washington Post* (Washington, DC, 28 March 2017) <https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/republicans-are-poised-to-roll-back-landmark-fcc-privacy-rules-heres-what-you-need-to-know/> accessed 19 July 2018.

18 Cecilia Kang, 'F.C.C. Repeals Net Neutrality Rules' *The New York Times* (20 January 2018) <https://www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.html> accessed 19 July 2018.

19 laura Moy, Statement of Laura Moy, Deputy Director Center on Privacy & Technology at Georgetown Law 2018.

increasingly unworkable in a world where it is increasingly easier to compile large amounts of 'non-sensitive' information to 'reverse engineer' sensitive information. The 2013 Target incident discussed above is an illustration of how compiling a record of 'non-sensitive' information to create a user profile revealing sensitive health information.

Americans need more privacy protection. Industry lobbyists have long sought to include federal preemption of state privacy and data breach laws as part of any new federal legislation. To the extent federal preemption is necessary to create a manageable national framework, it should be narrowly tailored to meet specific concerns.

Backward compatibility with existing federal privacy and data breach protections. The USA has relatively few federal statutes that directly impose privacy protections on industries. But while few in number, these laws form the basis for consumer privacy protection in critical industries such as health, communications, and financial protection. New federal protections for consumers should be 'backward compatible' with existing protections.

Any privacy legislation that follows these principles will protect consumers' autonomy, choice, and dignity regardless of the market share or size of the company that desires to collect or processes a person's personal information. In this section, we've argued that the best way to protect people's privacy is by enacting comprehensive privacy protection. Antitrust emphasizes specific anti-competitive behaviours and market power, and people deserve privacy protection regardless of the size of the company involved. In sum, if the policy goal is to protect consumer privacy, then the policy response should not be subordinated to the possibility of antitrust as a tool.

Conclusion: a toolbox of policies to protect privacy and consumers

In the 21st century, there are no magical solutions for protecting consumers. All the tools must be on the table in order to guarantee that consumers' rights, are not infringed in a rapidly changing economic environment with an increasing concentration of dominant players.

Antitrust enforcement and regulatory policy in the communications sector over the past 20 years demonstrate both the potential benefits of effectively aligned interventions and the enormous costs resulting from failed industry oversight. In such markets where historical monopolies, capital-intensive investments, and generally high levels of market concentration have only recently been challenged there is very little margin for error if policymakers want to harness the full economic potential of the communications sector in ways that boost sustainable economic growth that is fair and equitable.

Early 'hands off' antitrust and regulatory policy prevented new potential competitors from experimenting, solidified the dominance of telecommunications incumbents through regional expansion, and ossified the natural economic tendencies in these markets—thereby leading to massively inflated prices for consumers. More recently—and especially under the Obama administration—more aggressive intervention in proposed mergers and parallel regulatory actions designed to expand competitive opportunities for wireless, broadband, and broad-band-delivered video services broke some of the price-inflating cycle, unleashed substantial innovation in the video streaming market, and started to police against new potential abuses of dominance in data and transmission bottlenecks.[20]

The challenge in telecommunications and network industries that was recognized a century and a quarter ago remains relevant today. These industries benefit from immense economies of scale and scope that lead to large size and the threat of market power. We call them platforms today. They impact a wide range of economic and social activities that ride on these platforms and public policy should not destroy the economic benefits while it prevents the abuse of the inherent market power. The Progressive Era response was a nuanced mix of regulation and antitrust enforcement. The more dynamic the sectors of the communications industry, the more difficult and important is the need to find the right mix.

The key lesson in the communications sector is that vigorous regulation and antitrust enforcement can create the conditions for market success. But balance is the key. Technological innovation and convergence are no guarantee against the abuse of market power, but the effort to control the abuse of market power should not stifle innovation. If the Trump administration jettisons the enforcement practises of the past eight years, then the telecommunications sector is likely to see a wave of new consolidation and a dampening of the price cutting and innovative wireless and broadband services that have been slowly emerging. These markets will not remonopolize, but they will become a tighter oligopoly

20 Kimmelman and Cooper (n 8).

on stronger steroids even more dominated by two or three vertically integrated giants charging vastly inflated prices and asserting excessive power over the marketplace of ideas. Without adequate and forward-looking regulation, punctual antitrust enforcement and the breakup of dominant players might prove, and has proven to be, an insufficient tool to protect consumers.

As the Internet economy has developed, many Internet platform companies themselves, who were once the beneficiaries of an open and competitive Internet, now can stand in its way. Some of them have achieved a scale where their actions or inaction can have an inordinate effect on consumer welfare. Barriers to entry that result from data, from an entrenched user base, or from application lock-in may be just as real as those that incumbent broadband providers benefit from. When it comes both to broadband and internet platforms, it is vital for policymakers to act to address issues of market power, to ensure that consumers are protected, and to ensure that platforms promote public interest values like diversity, equity, and democratic discourse.

The question is how to act. The Internet economy is very complex, and the problems that can arise from a large operating system vendor, or a dominant social network, search engine, payment provider, or e-commerce platform, are not all the same. Some of the policy recommendations that groups such as Public Knowledge have long supported in one context (for example, common carriage) are not easily or correctly applied to internet platforms, while others (for example, privacy protections or rules against favouring economic affiliates) may be. In some instances, antitrust action or structural regulation may be the best approach; in others, consumer protection and other behavioural rules. All of those should be tools in the toolbox, but none of them should be put to work they are not designed for.

It has also become increasingly clear that many proposals for reform have tradeoffs. Navigating these can be tricky. Open platforms benefit competition, but sometimes at the expense of security. Interoperability requirements can help consumers switch from one provider to another, but can carry a privacy risk. Freedom of expression is a core social value, but that doesn't mean platforms should allow their tools to be used to attack other users, or that the First Amendment should be used as a shield by platform providers to avoid economic regulation. Decentralized, federated networks can prevent lock-in, but can be difficult to govern and improve. Understanding the risks and rewards of various policy approaches to platforms requires expertise in law, history, economics, and technology, as well as in the role platforms play in people's lives.

But informing our efforts we should keep a sense that, though dominant internet platforms may be relatively new, the issues they raise are not. Applying doctrines such as antitrust and traditional public interest and economic regulation to internet platforms requires paying attention to the ways that internet platforms are different, but that does not mean that none of the old rules apply or that time-tested tools should be discarded.

This new environment does mean, however, that we should be careful in our choice of tools. Advocacy and policy change efforts should be driven by policy goals, and not by our preference in tools. Antitrust should, in sum, be part of the toolkit necessary to protect the privacy of consumers. But we would be making a disservice to consumers and privacy if we would rely solely on antitrust to protect them.

doi:10.1093/idpl/ipy015