"[P]erhaps the biggest tension is between stimulating competition to promote innovation and regulating the data flows that power the platform economy."

The Push to Regulate Digital Markets and Services

PAWEL POPIEL

In the eyes of policymakers and much of the public, major digital platform companies were once synonymous with the democratization of communication, economic growth, technological efficiency and convenience, and endless, disruptive innovation. Even in the face of apparent crises, like Edward Snowden's 2013 disclosures about platforms' collaboration with various national security agencies in global surveillance programs, the services they offer and the markets in which they operate had remained largely free from external scrutiny. Yet now they have become the targets of countless and growing international regulatory inquiries, proposed and passed legislation, and public opprobrium over issues ranging from the viral spread of disinformation to their entrenched market power.

The public backlash against dominant platform companies signals a political awakening to their services' quiet but ongoing entrenchment in key political processes, their expansive reach into and power over a growing number of markets, and their transformation into social infrastructures on which we increasingly depend for accessing the news, communicating with others, seeking jobs, engaging in commerce, and many more daily activities. This international backlash follows major political shifts to which platforms' content flows may have directly contributed, including the 2016 US election of Donald Trump as president and the UK Brexit referendum the same year, as well as atrocities like the Rohingya genocide in Myanmar. Such events revealed the political stakes of the speech flowing across these digital services. The global COVID-19 pandemic only further illuminated growing public dependencies on digital platforms in times of crisis, as did their parent companies' ensuing record-breaking profits.

Although regulatory oversight previously had been scant, policy efforts to regulate digital platform services since 2016 have grown in analytical sophistication, acquired political momentum, and started to produce legislative and regulatory interventions. They have also involved significant cross-border collaboration and dialogue between regulators. But the emerging policy frameworks—which tend to focus on the triptych of content, data, and market power concerns—show degrees of variation, by region and by policy domain, and reflect different normative and policy goals.

While the biggest technology companies operating infrastructural platform services—Alibaba, Alphabet, Amazon, Apple, Baidu, Meta, Microsoft, Tencent—operate internationally, their governance and regulation is increasingly defined regionally and locally. Whereas the Chinese platforms are largely state-controlled, Western platform companies have strong incentives to oppose and shape regulatory policy endeavors. Accordingly, many of the largest US-based tech companies deploy substantial resources to lobby policymakers and influence public discourse on platform regulation to maintain their dominant positions. The confluence of varying normative commitments underlying policy goals, numerous policy focuses, and active efforts by platform companies to shape policy discussions produces tensions and trade-offs that characterize the growing international responses to digital platform services.

RATIONALES FOR REGULATION

To understand the assumptions, goals, and normative commitments motivating the efforts to regulate platforms, it is worthwhile to look at their

PAWEL POPIEL *is a postdoctoral fellow at the University of Pennsylvania's Annenberg School for Communication.*

origins. Like earlier information and communication technologies—from broadcast radio to cable television and the commercial Internet—the emergence of platforms contested existing regulatory frameworks. These paradigms, which govern digital information and communication flows, were drafted before platform services became central to online activities from communication to commerce. Often, these frameworks were tethered to clear distinctions between broadcast, telecommunications, and computing technologies and their uses.

As new technologies and business models blurred these distinctions through processes of digitization (the conversion of analog information to digital formats) and technological convergence (such as between telecommunications and computing), policy blind spots and gaps emerged. For instance, telecommunications services were treated as neutral conduits, responsible for delivering content and maximizing public access to their services, but not liable for the information flowing through their pipes. Yet content "publishers" like news media organizations could face liability for certain classes of defamatory or otherwise problematic speech. Communication platforms like YouTube and Facebook blurred these key regulatory distinctions. Neither content producers nor neutral conduits, these platforms benefit from liability exemptions for the speech that flows across their services, while carefully curating it using largely algorithmic sorting processes.

The emergence of platforms contested existing regulatory frameworks.

Such policy gaps went unaddressed for over a decade. The concerns platforms raised had not gained public salience, partly due to regulatory reticence, and partly as a result of maneuvering by major tech companies. Positioning themselves as engines of innovation and rapid economic growth, platforms were embraced by policymakers as fast-moving disrupters of markets, from media to shopping and taxi services. The affordances they provided, such as allowing users to bypass legacy news organizations to share news and political information, were perceived as naturally decentralizing and democratizing communication flows. Reflecting a prevalent neoliberal policy slant, their presumed breakneck pace and relentless innovation came to be seen, particularly in the United States, as ungovernable. Regulation was often invoked as the antithesis of tech-driven innovation.

The largest of these firms were embraced by the public. They also partnered with governments on issues ranging from cybersecurity to developing technology policy. When Snowden exposed the tight-knit collaborations between Internet companies, including digital platform incumbents, and national security agencies in the United States, the UK, and other Western countries, governments bore the brunt of public outrage, rather than the tech sector.

Cracks in tech dominance were becoming visible, as digital privacy issues drew more public attention and regulators imposed a handful of fines for privacy and competition violations. But the current, more concentrated backlash emerged amid a series of political shifts that alarmed many policy elites, raising concerns about the stability of democratic institutions in the face of right-wing populism. These included Trump's election, the victory of the "Leave" campaign in the Brexit referendum on exiting the European Union, and a series of other right-wing populist election wins from Europe to Latin America. The extent to which platforms contributed to these political outcomes is far from empirically clear. But early research suggesting that political disinformation on platforms played a decisive role—offering a tidy technological answer to complex political and economic developments—attracted policymakers' attention.

The scrutiny of platforms as potential sites of disinformation that destabilize elections intensified following 2018 revelations about political consulting firm Cambridge Analytica, which provided services to the Trump presidential campaign and was key to the success of the Brexit "Leave" campaign. It was reported that the firm had obtained Facebook user data without users' consent, and then used it to train algorithms to target other Facebook users with political ads.

These events revealed that the same affordances that democratized and decentralized communication also enabled the use of behavioral advertising algorithms to fragment and select voting blocks for disinformation campaigns. Subsequent high-profile controversies—such as one sparked by Facebook's failure to stop a white supremacist's livestream of his March 2019 terrorist attack on

two mosques in Christchurch, New Zealand, from going viral on its platform—demonstrated the public consequences of platforms' content moderation practices.

As governments grappled with imposing public obligations on platforms for the content they host and curate, a second critique emerged in policy circles focused on incumbent tech companies' growing market power. Frustrated with ineffective regulatory fines that were often written off as a mere cost of doing business and so failed to deter anticompetitive behavior, as well as with competition regulators' lax scrutiny of big tech mergers and acquisitions, these critics pointed to platform incumbents' central gatekeeping positions in key markets.

Amazon's dominance in e-commerce, Facebook and Google's duopoly in digital advertising and gatekeeping in digital news distribution, and Apple and Google's dominance in mobile app stores represented classic market power concerns that contested discourses about the tech sector's ceaseless creative destruction and decentralization. These concerns were especially pronounced since many of the services dominated by these companies fulfill key public functions, like information and news provision, and consequently resemble social utilities or social infrastructure. At the same time, the value of these services stems from the very network effects that, coupled with efficiencies related to economies of scope and scale, contribute to these companies' dominance. These dynamics became especially clear during the pandemic, which revealed the public dependence on dominant platforms for everything from health information to grocery shopping, fueling record-breaking profits. In response, a robust international policy debate focused on reforming competition laws and their enforcement to effectively address platforms' market power.

The twin concerns about problematic content and market dominance are linked with concerns about data collection, quantification, and commodification. User data powers content moderation and curation algorithms and informs business strategies to dominate markets. But big data quantification poses its own distinct set of concerns, including algorithmic discrimination based on socially salient categories like race and gender, and the impact on user autonomy in online and increasingly offline spaces. Data-powered labor management systems, like those employed by Amazon in its warehouses or those at the heart of the gig economy typified by companies like Uber or Postmates, contribute to greater labor precarity, worker atomization, and workplace surveillance. The opacity, complexity, and inscrutability of algorithms powering the platform economy, their growing entanglement with the public sector and the military, and the problems with data storage and processing (from cybersecurity to carbon footprints) all raise a host of concerns with which policymakers are only beginning to grapple.

EMERGING FRAMEWORKS

The policy frameworks for digital platform markets emerging internationally share overarching themes in their focus on content, data, and market power concerns. Due to the transnational scope of the biggest platform companies and close international dialogue among regulators—particularly those in the United States, Australia, and Europe—some proposed policy interventions overlap and align, especially in the domain of competition policy. Data concerns either fall under the purview of existing frameworks, like the EU's General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD), or are considered in relation to competition concerns. But greater variation exists in the highly politicized and user-facing area of content regulation, which reflects different countries' speech norms and policy goals.

In a striking reversal of the hands-off approach that had lasted more than a decade, competition policy interventions have lately attracted significant attention from policymakers. A growing number of high-profile antitrust investigations are under way or have concluded in the EU, the United States, the UK, China, India, South Korea, Japan, and other countries. They tackle a range of anticompetitive practices, such as illegal tying and bundling (Google tying app developers to its app store and payment services) and self-preferencing (Amazon privileging its own products over those of smaller competitors on its e-commerce site). Aside from being time-consuming and resource-intensive, such investigations must also grapple with legal and regulatory frameworks that fail to capture competitive dynamics in platform markets.

Consequently, proliferating inquiries and draft legislation focus on updating these frameworks to make tech mergers and acquisitions more costly and difficult; to mandate data portability and interoperability to facilitate competition on and

with platforms; and to separate lines of business to prevent platforms from leveraging dominance in one area to acquire it in another (as with app store dominance and payment services), among other structural interventions. The prominence of these policy solutions over other approaches stems partly from concerns about the size of the largest platform companies and partly from the belief that other concerns, including the circulation of disinformation and threats to privacy, are downstream from market power. Put differently, there is a widely held faith that greater competition will help induce better content moderation and data practices.

Many countries' consumer protection regulators effectively serve as the front line against data-related harms. These include cybersecurity threats and improper data collection practices, such as obtaining and processing data without user consent. But aside from occasional fines for egregious abuses, data protection frameworks vary in the range of protections they offer users. Expansive legislation like the EU's GDPR and Brazil's LGPD seeks to minimize commercial data collection, establish basic user rights with respect to companies that collect and process their data, and impose often complex opt-in consent regimes to empower user choice. Comparatively, countries like the United States offer minimal data protection, requiring users to actively opt out if they do not want their data collected, which is often unrealistic given the dominant platform companies' extensive reach over the commercial Internet.

The variation in data protection also can be found at the subnational level, as in the case of the state of California, which passed its own privacy law that exceeds federal US protections, hewing closer to the obligations set out in the GDPR. Going even further, cities like Barcelona have launched public, municipally governed data trusts that pool user data and empower residents to decide how their data is managed. Such initiatives respond to the growing recognition that big data provides population-level insights whose consequences extend beyond the individual. For example, Cambridge Analytica's political ad targeting reached Facebook users whose data was not obtained by the firm, but who shared characteristics with those whose data was collected. Trusts operate on the logic that individual consent requirements do not address such harms, whereas accountable public governance of datasets and their uses might do so.

As big data, with its potential for monetization, becomes increasingly central to the global economy, many countries have made efforts to harmonize their data protection frameworks with the GDPR by offering consumer protections, while facilitating international business and capital flows. Aside from draft bills that seek to curb practices like behavioral advertising, however, most policy proposals related to platforms' data processing focus on wresting data flows from the most dominant players. Interventions like data portability (the ability to move one's data from one platform service to another) and interoperability (providing platform access to competitors) dovetail with competition policy goals rather than privacy protections. They seek to make it easier for users to move from one platform service to another and for competitors to develop complementary services (such as competing messaging services that can exchange messages with WhatsApp users), with the overarching goal of incentivizing innovation and competition.

Regulation was often depicted as the antithesis of tech-driven innovation.

CONTENT CONTROL

Since the information and communications sectors play a fundamentally political role in society, shaping the conditions that determine who can access information resources and participate in the public sphere, dealing with speech issues in these sectors is inevitably a highly contested, political process. The greatest policy variation exists in policies addressing the most politicized concerns related to the content flowing across platform services, from hate speech to disinformation. The range reflects different approaches to regulating public speech.

For example, Germany's controversial 2018 Network Enforcement Act imposes strict liability and massive fines on platforms for failure to quickly remove content that violates national laws, such as those banning hate speech. In its landmark Digital Services Act (DSA), currently pending final approval by member state governments, the EU has drafted a less aggressive approach, leaving room for member states to add further requirements. This legislation imposes content obligations on the largest online platforms, such as developing codes of conduct with civil society, providing transparency about how their algorithmic

recommender systems sort user content, and offering avenues for users to contest content moderation decisions. Thus, the DSA provides baseline user protections, while limiting direct government regulation of speech flowing across platforms.

On the surface, US law, including the First Amendment to the Constitution and Section 230 of the Communications Decency Act, which exempts intermediaries from liability, ensures that platforms cannot be held liable for most content flowing across their services. Most efforts to tackle problematic content originate from platforms, often in response to civil society or public pressure. But debates about content moderation are increasingly fractured by politics, particularly since Twitter and Facebook deplatformed Trump following his comments in the aftermath of the January 2021 attack on the US Capitol by his supporters. Right-wing politicians invoked Trump's removal as evidence of social media censorship of conservative speech, even as an internal Twitter study found that the platform disproportionately amplifies conservative over liberal content.

In 2021, the state of Texas passed a law making it illegal for dominant platform companies to take down content posted by any state resident based on their political viewpoint. Though the Texas law faces legal challenges, a similar effort to prevent deplatforming is ongoing in Florida. Such initiatives are thinly veiled governmental incursions on speech flows for political reasons, intended to thwart private content moderation. Although they purport to prevent censorship, they ultimately undermine efforts to remove hate speech and related problematic content associated with the far right. As a result, they fall on a spectrum of other highly political efforts to control content flows—from Poland's proposed social media law calling for the creation of what would effectively be a government-run speech council to oversee platform content moderation, to the Chinese approach involving strict censorship of content considered politically harmful.

The 2021 passage of Australia's News Bargaining Code points to another approach to dealing with problematic content like disinformation—by bolstering traditional news media. The law targets the sizable advertising revenues that dominant technology platforms enjoy due to users' increasing reliance on their services for access to content produced by news outlets. For years, platforms like Facebook have been able to cannibalize these revenues at the expense of the already struggling news sector. Under the new law, dominant platform companies must negotiate agreements with Australian news media organizations to fairly share these revenues. Such bargaining approaches are also in various stages of consideration in countries like Brazil, Canada, India, and the United States. Ultimately, they seek to rebalance the power dynamics between platforms (and the digital markets they dominate) and news publishers.

THE POLITICS OF REGULATING PLATFORMS

These initiatives signal a widespread push to rein in the entrenched power of the largest tech companies. But as of this writing, only a small number of laws addressing platform markets have passed, and most efforts are still at the inquiry or draft bill stage. As a result, the effects of these proposed interventions are unclear. Any legislation that has been enacted is especially consequential and is scrutinized by policy observers in other countries.

The EU has maintained a first mover role in regulating digital platforms, strengthened by its expansive regulatory infrastructure. Its impending DSA, which focuses on online safety and illegal content, and the Digital Markets Act (DMA), intended to stimulate competition in concentrated platform markets, articulate a set of sweeping reforms whose enforcement and effects will be closely watched. In the US Congress, a recently passed update to a narrow merger law and a slew of draft bills indicate similar goals, particularly regarding platform competition. Although the draft bills face uncertain prospects in a highly polarized political climate, the United States has incentives to partially harmonize its approach with the EU's in order to offset China's economic power and its firewalled but immense platform sector.

These efforts to regulate digital platforms are political in at least two senses. First, they reflect the underlying normative and ideological commitments that shape regulatory approaches to the platform economy. Second, more overtly, these initiatives are often products of a clash of political interests, not least those of dominant platform companies themselves. This produces tensions and trade-offs in regulating digital markets.

Collectively, the proposed interventions signal a commitment to a privately run platform economy, regulated through competition and varying public obligations. They reflect the common belief that regulated market mechanisms will induce

better content moderation practices, stronger privacy protections, and more publicly responsive business models. The scant evidence for this belief is mixed. TikTok, Facebook's biggest competitor, has content moderation problems similar to those of other platforms and offers similar privacy protections (while raising policymakers' concerns about surveillance and cybersecurity as a result of its being based in China). Other competitors, like alt-right social media platforms Parler and Trump's Truth Social, have weaker content moderation mechanisms.

In effect, the largest platform services seem best poised to offer the kind of resource-heavy content moderation systems that can address the online harms that policymakers target. But this is at odds with policymakers' competition goals. None of the regulatory initiatives attempts to fund new mixed-ownership or public platforms, or to protect existing ones as alternatives to dominant privately owned giants. Doing so could incentivize more democratic platform governance structures.

Efforts to address the declining news industry by empowering news organizations to negotiate larger shares of digital advertising revenues from digital platforms introduce similar tensions. These agreements presuppose the existence of a small number of large platforms, potentially undermining greater competition in platformed news distribution. They also naturalize user data flows that produce digital advertising profits, and thus may be at odds with stronger data protection.

Indeed, perhaps the biggest tension is between stimulating competition to promote innovation and regulating the data flows that power the platform economy. Despite baseline privacy protections in existing and proposed laws, most policy initiatives do not contest private governance of data infrastructures. Though doing so could be socially beneficial, policymakers tend to treat user data as a key input for competition and innovation, and are wary of excessive restrictions that may unduly dampen the digital economy. Consequently, pro-competitive interventions like mandated interoperability and data portability empower user rights with respect to selecting services that access and process their data, but they do not fundamentally challenge existing data flows.

As these data flows become increasingly complex and entangled, complicated consent regimes may do little to help users manage their data or to address population-level effects of big data analytics. Moreover, governments may have incentives to access these data flows for surveillance purposes, which could also limit strong data protections. For instance, the Indian government proposed a draft data protection law designed to keep user data within its borders to fuel its expanding data economy, but withdrew the draft in August 2022 after public protests over provisions enabling state access to the data.

Influence Operations

Aside from policymakers, no entities are as invested in the outcome of these policy developments as the platform companies themselves. Though a range of actors participate in these policy debates, dominant platform companies bring immense lobbying and public relations resources to bear on them. They also recruit high-profile attorneys, economists, and former regulators to help them navigate the regulatory landscape and tactically exert soft power within often tightly knit policy networks.

This influence is far from absolute, as shown by the growing international scrutiny and the passage of laws in jurisdictions like the EU. Despite a highly publicized decision by Meta to pull news from its main social media service in Australia in response to the country's proposed news bargaining code, the law passed, and the company resumed offering these services. Yet tech giants retain the ability to obtain legislative and regulatory concessions, suggesting that the battle over regulating the platform economy is increasingly about tactical victories rather than paradigm shifts.

Having accepted that regulation is inevitable, dominant platform companies attempt to limit its scope, especially by challenging competition policy interventions that they view as an existential threat. First, they exploit the West's tensions with China by invoking growing competition from Chinese platforms and attendant cybersecurity threats, positioning themselves as the frontline defense against these dangers.

Second, they capitalize on regulators' inability to actively monitor platform activity at scale, presenting themselves as key co-regulatory partners that offer algorithmic solutions to policymakers' concerns over content and other issues. They argue for the relative ease of regulating a few centralized intermediaries, as opposed to a long tail of many dispersed, smaller services.

Meta CEO Mark Zuckerberg and the company's president of global affairs, Nick Clegg, have both

repeatedly stressed the benefits of working with a dominant Facebook to tackle content concerns in the digital public sphere—and the coordination costs of doing the same with many smaller platforms. Likewise, both Apple and Google emphasize the advantages of their size in rooting out malicious apps from their app stores. These arguments may not slow the growing number of interventions like data portability, interoperability, and stronger merger restrictions, but they could persuade policymakers to centralize content regulation via co-regulatory arrangements with a few large players, preserving the scale of dominant platform services.

BALANCING INTERESTS

Ultimately, as the 2020 report *Canada's Communication Future* put it, many policy initiatives to govern the platform economy aim to forestall the possibility "that users may seek ways to disconnect, or may demand strict rules that could stifle innovation." The emerging policy frameworks attempt to balance market competition in the service of innovation with varying data protections that do not excessively restrict monetizable data flows. Concurrently, news bargaining agreements and stricter content rules for dominant platform services all exist in tension with the desire to decentralize the platform economy.

It is far too early to speculate about the effectiveness of these interventions, many of which have not yet materialized as legislation. But the idea of a single, global Internet with unfettered information flows, which featured in Western geopolitical discourse for over two decades, is no longer a topic of policy debate, much less a reflection of reality. Policy approaches to regulating platform markets differ by region and by policy domain.

On the one hand, efforts to regulate content at the app layer of the Internet in response to concerns over political disinformation, health misinformation, and related phenomena vary internationally, reflecting a mosaic of normative concerns and political commitments. On the other hand, there is evidence of coordination on the competition policy front, along with economic pressures to harmonize baseline data protections. As regulators attempt to balance these protections against pressures to cultivate regional data markets and facilitate international data flows, familiar questions persist about whose interests will define regulated platform economies: public or private? ■