Introduction

WHEN THE INTERNET became widely commercialized in the 1990s, it arrived with the promise of freedom: freedom for individuals to access information, exercise their voices, engage in debates, and shape societies. Early internet pioneers saw online platforms as the guardians and amplifiers of those freedoms, enhancing democracy by providing an inclusive platform for promoting diverse voices around the world. Today, this techno-optimist promise of an enhanced human experience has, at least in part, been realized: the internet has indeed democratized access to content and vastly expanded individuals' ability to receive, create, and disseminate all kinds of data, fundamentally transforming human beings' relationship with both information and with each other. This enhanced access to information and conversations has redefined the very fabric of human experience and undoubtedly generated immeasurable benefits for individuals and societies. And as the internet evolves in the years ahead, it will almost certainly continue to deliver significant new benefits in ways individuals and societies cannot yet even imagine.

Alongside these many benefits, however, the internet has also altered societies and individual lives to their detriment. While the internet has cultivated human connections and civic engagement, it has also been a channel for exposing vast segments of society to different forms of harmful content. Internet sites often serve as platforms for disinformation, bullying, hatred, and repulsive content, undermining the safety and dignity of individuals while dividing societies and destabilizing democracies. Algorithms designed to tailor online content to each user's preferences have fueled polarization and fragmentation, cultivating more extremist ideas and further eroding societal cohesion.[1] Instead of only increasing freedom, enhancing democracy, and nurturing an egalitarian and inclusive communitarian culture, the internet has also been used repeatedly to diminish these values, creating an ecosystem in which surveillance capitalism can thrive and societal divides deepen.[2]

Mitigating the individual and societal harms that arise from the internet is just one piece of the broader governance challenge facing regulators of today's digital economy. Digital transformation has ushered in an exceedingly concentrated economy where a few powerful companies control vast economic wealth and political power, restricting competition and widening the gap between winners and losers in the digital economy. The five largest tech companies—Amazon, Apple, Google, Meta, and Microsoft—collectively recorded over $1 trillion in revenue in 2020, while earning an income of $197 billion and having a market capitalization of $7.5 trillion by the end of 2020.[3] In 2021, the combined market capitalization of Apple, Alphabet, Meta, and Amazon exceeded the value of the over 2,000 companies listed on the Tokyo Stock Exchange; Apple and Meta together were worth more than the one hundred companies with the highest market cap listed on the London Stock Exchange; and Amazon alone eclipsed the entire German DAX Index, which represents around 80 percent of the market cap of companies publicly listed in Germany.[4] No doubt these tech companies would not have grown this big without developing products and services that consumers around the world value. But the law has also been on their side. For example, weak antitrust enforcement has amplified these companies' growth, allowing them to amass even more power through a staggering number of acquisitions. Over the past three decades, Amazon, Apple, Google, Meta, and Microsoft combined have acquired 770 startups.[5] According to Apple's CEO Tim Cook, Apple alone has acquired approximately one company every three to four weeks for the past six years.[6] Looking at this recent history, the power of these companies seems to only be growing stronger and more concentrated as the industry matures, with few obvious limits to how that power is deployed.

There are several reasons to be concerned about this concentration of economic, political, and cultural power in a few large tech companies.[7] First, this handful of companies controls a large proportion of the sector's wealth, allowing them to buy any competitor that threatens their market power. Second, their economic power buys them political influence that can be deployed to lobby for favorable regulation to further entrench that power. Third, these same companies increasingly control public discourse by moderating content on platforms where societal conversations, including political speech, take place. This allows them to exercise power over online infrastructures for democracy and public discourse. Fourth, these companies control much of the personal data that every user generates on a daily basis, which they have every incentive to extract for economic gain. These stores of data vest them with power over individual users. The cumulative effect of these different dimensions of power is to make these companies central to modern economic, political, and

social life. The power vested in these companies is so vast that it increasingly competes with the power exercised by nation states, a phenomenon that has raised significant concerns among governments around the world.

Because of this accumulation of power, decisions by tech companies on how to wield their influence are becoming more consequential and controversial, opening up important questions about how societies and individual lives are being shaped by this multifaceted power. For example, when tech companies moderate content on their platforms, they face significant challenges in seeking to curtail harmful speech without suppressing free speech. To be sure, these companies err constantly in their efforts to achieve this balance—both in failing to restrict harmful speech in some cases and in censoring speech that has public value in others. Despite their efforts to take down detrimental content, major platforms such as Facebook, YouTube, and Twitter overflow with content that is hateful, dangerous, and often illegal. Perhaps most disturbingly, the platforms still host terrorist propaganda and abhorrent violence all too frequently. For example, in 2019, a perpetrator who carried out a hate-motivated massacre of fifty people in a mosque in Christchurch, New Zealand, livestreamed his killings on Facebook.[8] This tragedy received a large number of views on Facebook and various other online platforms, where the footage was replayed while the companies struggled to take down the various copies of the video appearing online. On the other hand, there are numerous examples where platforms' content removal efforts have been overzealous. In 2011, YouTube removed a video of a thirteen-year-old boy killed in the war in Syria in accordance with its policy prohibiting display of "dead bodies."[9] The image of the boy's dead body was shocking. But the image was meant to shock. The video was posted to awaken the international community to the horrors of the unfolding war, with the hope of galvanizing a global condemnation of the repressive Syrian regime. But as these examples reveal, drawing lines between permissible and impermissible speech in ways that are socially acceptable is exceedingly difficult. Yet, despite the delicate nature of content moderation, many government regulators have largely abdicated these types of decisions to the platforms themselves.

In addition to the flawed outcomes from content moderation, the methods used in content moderation can be disconcerting as well. For example, alongside their reliance on algorithms, all platforms use human moderators that deploy so-called community guidelines to decide what content stays up and what is removed. But as revealed by the German newspaper *Sueddeutsche Zeitung* in a 2018 story,[10] there is a massive human toll borne by these moderators who work on the frontlines "cleaning" the internet. In return for meager pay and few employment protections, content moderators

are exposed to a constant stream of graphic violence and cruelty. The story reported that a single Facebook moderator in Germany, for instance, was expected to handle 1,300 reports a day.[11] A 2014 article published in *Wired* documented the work of Facebook's content moderators in the Philippines, who clean the platform of illegal content while being paid $1–4 per hour for their work. These moderators are exposed hour after hour to the worst possible content posted to these internet platforms. One Google moderator estimated having to filter through 15,000 images a day, including images of child pornography, beheadings, and animal abuse.[12] In 2020, Meta settled a lawsuit brought by over 10,000 of its content moderators, agreeing to pay $52 million in mental health compensation.[13] Content moderators pay an enormous psychological price in helping to keep the platforms safer and more civil for users around the world, but their plight also lays bare the distance between the highly compensated and powerful tech executives in Silicon Valley and the behind-the-scenes labor employed to scour the internet for harmful content. This human toll further calls into question the early, techno-optimist vision of the internet as an emancipatory force that would inevitably dismantle existing institutions of power and lead to a "more humane and fair" world.[14]

Another reason to be concerned about the concentration of power among a few tech companies relates to their collection of user data as part of their business model and the impact of that data collection on user privacy. This "surveillance capitalism" describes how tech companies extract vast data on their users' private lives and commercialize that information through targeted advertising, which threatens those people's rights to privacy and individual self-determination.[15] At worst, users' personal data can be harnessed to serve not only commercial, but also political goals. The Cambridge Analytica scandal—where a British political consulting firm acquired Facebook users' private data and used it in political campaigns—illustrates this problem in no uncertain terms.[16] In this case, internet users' private data was deployed with the goal of influencing the election in favor of President Trump. This or any similar attempt to manipulate voters compromises individuals' decisional privacy and undermines their trust in democracy.[17]

Internet users are not only vulnerable to surveillance by private tech companies, but also to digital surveillance by governments who rely on tech companies and their digital tools to further their national security or law enforcement objectives. The Chinese government's surveillance of its citizens, including its deployment of facial recognition technology, is particularly far-reaching. Hundreds of millions of surveillance cameras are already installed across China where the government can now match the video footage to

personal data collected elsewhere, identifying individuals in real time and potentially predicting or even preventing political resistance before it even happens.[18] The government has rolled out AI-driven surveillance programs such as Sharp Eyes,[19] the goal of which is to create an "omnipresent, fully integrated, always working and fully controllable" nationwide surveillance system, built and supported by Chinese tech companies.[20] Yet it is not only authoritarian governments that deploy the internet as a tool for surveillance. Democratic governments, including the United States, also conduct extensive surveillance operations, as former US National Security Agency (NSA) contractor Edward Snowden revealed as part of the unprecedented leak of sensitive US intelligence data in 2013. Those Snowden revelations exposed how the NSA had engaged in a mass surveillance of individuals by harvesting data available through Facebook.[21] Without proper oversight, it is both tempting and feasible for any government to utilize the surveillance capabilities of tech companies to advance their political goals or national security objectives, even when that surveillance undermines individuals' civil liberties.

Many of these concerns are now amplified with the rapid advances in artificial intelligence (AI). The innovations in so-called generative AI technologies, in particular, have the potential to revolutionize the way we work and interact with information and each other. At best, generative AI will allow humans to reach new frontiers of knowledge and productivity, leading to unprecedented levels of economic growth and societal progress. At the same time, the pace of AI development is unsettling technologists, citizens, and regulators alike. AI is already used to power both private and government surveillance and to manipulate human behavior, but those activities can now reach new heights with larger training datasets and more sophisticated AI tools. A growing fear is that these technologies will give powerful tools for bad actors to exploit and defraud people or commit other illegal acts. They might also soon be used by anyone to unleash waves of disinformation. Even ardent techno-enthusiasts are now issuing dire warnings on how unregulated AI can lead to these and many other uncontrollable harms, posing severe threats to individuals and societies. The direst predictions presage the AI's ability to obliterate labor markets and make humans obsolete or—under the most hyperbolic scenario—even destroy humanity.

As people have become increasingly aware of the risks and potentially harmful effects associated with the use of these digital tools and with tech companies' vast economic power and social impact, it is not surprising that calls for greater regulation of these companies are growing. Recently, several governments have begun to respond to these popular demands by asserting

their regulatory powers, leading prominent news outlets to proclaim how "A Global Tipping Point for Reining In Tech Has Arrived,"[22] and to describe how "Big Tech Braces for a Wave of Regulation."[23] For the past decade, the European Union has been leading this fight, frequently leveraging its antitrust laws, data protection laws, and other regulatory instruments to reclaim control over the industry.[24] But the EU is no longer the lone crusader in taking on the leading tech giants. The Chinese government has initiated an unprecedented crackdown on its tech sector in the name of advancing "common prosperity" and in order to ensure that tech giants do not overpower the Chinese state.[25] The tide may finally be turning even in the US, where Congress is reassessing the need to rewrite US antitrust laws, enact a federal privacy law, or revisit the Communications Decency Act of 1996, which shields internet platforms from liability for the content they host.[26] However, even if the problems associated with the tech industry have led to a broadening consensus that the digital economy needs to be regulated, there is no consensus among governments on what that regulation should look like.

Digital Empires: Three Competing Regulatory Models

Today, there are three dominant digital powers—the US, China, and the EU—who can metaphorically be thought of as "digital empires." These modern empires of the internet era are the leading technology, economic, and regulatory powers, each with the ambition and capability to shape the global digital order toward their interests and values. They have each developed a distinct governance model for their domestic digital economies, consistent with their different ideological commitments. Not unlike the empires of the past, they have further exported their domestic models in an effort to expand their respective spheres of influence, thus pulling other countries into the orbits of the American, Chinese, or European digital empires. The digital empires find their closest analogue, not in the former territorial empires, but in various informal empires of the twentieth century that projected economic, military, and cultural power across their borders, creating power asymmetries that vested them with influence over foreign societies. Today's digital empires are primarily exporting their tech companies, technologies, and rules governing those technologies, thus shaping countries and individuals that fall under their influence toward the norms and values they espouse.

Each digital empire holds a different vision for the digital economy, which is reflected in the regulatory models they have adopted at home and

promoted abroad. These three leading regulatory models could be thought of as representing three "varieties of digital capitalism"—drawing on different theories about the relationship between markets, the state, and individual and collective rights.[27] As described throughout this book, the US has pioneered a largely *market-driven* model, China a *state-driven* model, and the EU a *rights-driven* model. Each of these regulatory models involves societal choices that rest on diverging economic theories, political ideologies, and cultural identities. In deciding how to regulate the digital economy, governments in the three jurisdictions have all had to balance their support of technological innovation with the implications those technologies have for civil liberties, the distribution of wealth, international trade, social stability, and national security, among other key policy concerns. This balancing effort has led to some similarities but also notable differences across the leading regulatory models. As each model is associated with contested policy choices that subject them to criticism—each for different reasons—there is no global consensus on which of the three dominant regulatory models best serves the goal of building a vibrant and resilient digital economy and society.

The US has traditionally followed a *market-driven* regulatory model, which has provided the foundation for the global digital economy as it exists today.[28] The American regulatory approach centers on protecting free speech, the free internet, and incentives to innovate.[29] It is characterized by its discernible techno-optimism and relentless pursuit of innovation. The US government has historically viewed the internet as a source of economic prosperity and political freedom and, consequently, as a tool for societal transformation and progress. The American market-driven model exhibits uncompromising faith in markets and embraces a limited role for the government. According to this techno-libertarian view, government intervention not only compromises the efficient operation of markets; it also undermines individual liberty. Thus, while the US's commitment to innovation and growth provides the economic rationale against government intervention, its commitment to individual liberty and freedom is often invoked as a political reason to limit the government's role. Minimizing government interference is seen as essential to producing a vibrant democratic society characterized by free speech and the engagement of diverse voices in civic life. From this perspective, the government is only expected to step in to protect national security—on cybersecurity issues, for example, the US government has a role to play alongside tech companies.

Few would dispute that many of the prized innovations that shape our everyday lives today can be traced to Silicon Valley—innovations that the American market-driven model has directly facilitated. At the same time, privacy advocates and other critics argue that this zealous pursuit of innovation

has come at the expense of protecting individual internet users' rights. The EU has joined these advocates in arguing that, absent regulatory safeguards, public and private surveillance thrive under the US model and severely compromise individuals' rights to privacy and political autonomy. Seen from this vantage point, a world governed by tech companies' business models subjects internet users to behavioral advertising and manipulation that subvert individual choice, liberty, and self-governance.[30] By allowing for this, the US model thus compromises individuals' abilities to exercise their agency and participate in democracy. Several recent high-profile scandals illustrate the problem, including the Snowden revelations and the Cambridge Analytica scandal mentioned above. The EU and other critics of the market-driven regulatory model can also point out how Facebook, Twitter, YouTube, and other platforms have repeatedly failed to remove dangerous disinformation on topics ranging from the COVID-19 pandemic to democratic elections. And they can replay the images of the January 6, 2021, insurrection at the US Capitol, which originated in a rampant social media–fueled disinformation campaign about a stolen election.[31] Consequently, when looking strictly at innovation and economic growth, the American market-driven model can be praised for its ability to nurture tech companies, but that economic benefit comes at the expense of risking fundamental rights, human dignity, political autonomy, and democracy.

In contrast to the American market-driven regulatory model, the Chinese regulatory model rests on a *state-driven* vision for the digital economy.[32] The Chinese government seeks to maximize the country's technological dominance while maintaining social harmony and control over its citizens' communications.[33] China is determined to leverage technology to fuel its economic growth and development. It is currently engaged in an unprecedented state-led effort geared toward becoming the world's leading technology superpower. In addition to pursuing this economic goal, the government is focused on tightening the political grip of the Chinese Communist Party (CCP) by deploying the internet as a tool for control, surveillance, and propaganda. To achieve these goals, the CCP has harnessed the power of its private tech companies: in return for the initially lax regulatory approach that helped them grow and flourish, Chinese tech companies have acted as the CCP's surrogates, performing the surveillance and control functions of the state over their users. However, the Chinese government is increasingly adopting the view that the largest tech companies have grown too powerful. It has recently leveraged its antitrust laws to rein in domestic giants such as Alibaba and Tencent—the opening salvo of an unprecedented assault on its domestic tech industry. Yet even this newest turn in digital regulation serves the fundamental goal of the

Chinese government: cementing the state's control of the digital economy as a defining feature of China's regulatory model.

Like the US, China has been tremendously successful in fostering technological innovations, allowing leading tech companies such as Alibaba, Tencent, and Huawei to emerge. At the same time, the Chinese state-driven regulatory model has also come under increasing criticism in democratic countries, as the Chinese government systematically harnesses the internet as a tool for censorship and political control. Many foreign governments, including the US and the EU, condemn the Chinese government's policy of banning and filtering online content on a large scale—a policy colloquially known as the Great Firewall. Many foreign companies have become a direct casualty of this policy, including Google, Meta, and Twitter, which have largely abandoned the Chinese market due to the government's extensive censorship policies.[34] China's large-scale deployment of facial recognition techniques for law enforcement purposes is also widely condemned abroad.[35] Its social credit scheme, which rates citizens for their trustworthiness based on issues such as paying taxes or committing a crime, is similarly met with deep suspicion.[36] These examples illustrate how the Chinese government has converted the internet from a tool for advancing democracy to an instrument in service of autocracy. Thus, China's practice of deploying data as a tool for social control represents a stark departure from the shared European and American view where the internet is seen as key to promoting individual liberty and advancing freedom in society. Through its model, China has shown the world how freedom is not inherent in the character of the internet, but rather vulnerable to political choices by those with the power to limit that freedom.

The European regulatory model differs from both the American and Chinese models in being distinctly *rights-driven*.[37] The EU embraces a human-centric approach to regulating the digital economy where fundamental rights and the notion of a fair marketplace form the foundation for regulation.[38] According to this view, regulatory intervention is needed to uphold the fundamental rights of individuals, preserve the democratic structures of society, and ensure a fair distribution of the benefits from the digital economy. Technology must be harnessed toward human empowerment and with the aim of safeguarding the political autonomy of digital citizens. In contrast to the US model, which focuses on protecting free speech as *the* fundamental right, the EU model seeks to balance the right to free speech with a host of other fundamental rights, including human dignity and the right to privacy. In contrast to the Chinese model—which also reserves a strong role for the state in steering the digital economy—the EU model is geared at enhancing, not curtailing, the rights of citizens vis-à-vis both tech companies and the state.

The EU's regulatory model also emphasizes that digital transformation needs to be firmly anchored in the rule of law and democratic governance. Whereas the American market-driven model often emphasizes how governments do not understand technology and should hence refrain from regulating it, the European rights-driven model is more concerned that tech companies do not understand the pillars of constitutional democracy or the fundamental rights of internet users.[39] As a result, under the European regulatory model, the government must steer the digital economy with the goal of protecting those rights they view as foundations of a liberal democratic society.

Civil rights advocates often praise the EU for its commitment to fundamental rights, dignity, and democracy, including its efforts to steer the digital economy toward those values through regulation. At the same time, many industry advocates and companies in both the EU and foreign markets—particularly the US—view the European rights-driven regulatory model in a less positive light. They describe it as overly protective, compromising tech companies' incentives to innovate, and thereby curtailing the technological and economic progress that societies depend on. Few successful tech giants are emerging from Europe, which is often attributed to the EU's protective regulations that interfere with tech companies' innovative zeal.[40] Many US politicians, tech companies and other proponents of the free speech ideals underlying the American regulatory model also allege that the European rights-driven model risks undermining free speech and stifling public debate. In particular, US tech companies like Google have argued that the EU's approach toward content moderation—including its online hate speech rules and the "right to be forgotten" provision in the EU's General Data Protection Regulation (GDPR)—could to lead to harmful censorship.[41] In other words, these critics argue that the EU overdoes its rights-driven regulation, damaging economic progress and political freedom in the process.

Even this cursory overview of the three leading regulatory models reveals significant distinctions among them. However, the models also have elements in common. Despite prioritizing the market, the state, or individual and collective rights differently, each model ultimately maintains aspects of each. Markets do not always win in the US; the state does not control everything in China; and the rights of internet users do not always prevail over other policy imperatives in the EU. Nevertheless, when faced with critical policy trade-offs and the balancing of various interests in regulating the digital economy, each jurisdiction often falls back on those foundational principles that are intrinsic to their distinctive regulatory models: the US tends to draw on its pro-market instincts to limit government intervention, China responds in ways that ensure the government's interests are protected, and the EU acts in a manner

that elevates the rights of digital citizens to the heart of its policymaking. It is these persistent differences across the three models that fuel tension and conflict, paving the way for the contested battles that have become a defining feature of today's digital economy.

Imperial Rivalries: A Battle Fought on Two Levels

Due to the global nature of the digital economy, these leading regulatory models extend across jurisdictions, impacting foreign societies and shaping lives of foreign individuals. As a result, these models frequently collide in the international domain, leading to fierce battles both within and across the digital empires. These imperial rivalries are thus central to the evolution of the global digital order, revealing how that order is shaped not only by the empires themselves but by their mutual contest for influence. These rivalries take place at two levels. First, there is a *horizontal battle among different governments*, as illustrated by the conflicts among the US, China, and the EU over the norms and values that govern the digital economy. However, this horizontal battle among the governments is shaped by—and often fought through—*vertical battles between governments and the tech companies* that these governments are seeking to regulate. These vertical battles have evolved differently in each jurisdiction, consistent with the differences in the three regulatory models. Various horizontal and vertical battles are further deeply intertwined, constraining the strategies that any government can deploy in each battle. For example, the US government is reluctant to regulate its tech companies too aggressively for fear of stifling these companies' ability to innovate as such a strategy could, in turn, weaken the US in its horizontal rivalry over technological supremacy against China. Such interconnections across the various horizontal and vertical battles often lead to a strategy of restraint, bringing about periods of de-escalation alternated with periods of escalation. This dynamic sustains a persistent, yet ultimately manageable, conflict that prevents a full-blown tech war from emerging but also keeps a lasting truce at bay.

A Contest Among Governments: The Horizontal Battles Between the US, China, and the EU

Most of the public commentary on the great power contest in the digital sphere focuses on technological rivalry between the US and China as the leading technology powers.[42] This narrative often dismisses the EU as a bystander, caught between the two powers battling for technological supremacy

while struggling to create a vibrant tech industry of its own.[43] However, the EU has asserted itself in this contest as the most powerful regulator of the digital economy, giving it unique leverage to shift the digital economy toward its values. This often elicits strong criticism, especially from US tech companies and the US government, and leads to heated regulatory battles between the US and the EU.[44] As a result, this book frames the horizontal battle for the digital economy as one taking place between the US, China, and the EU.

In their contest for influence over the digital economy the US, China, and the EU each approach their horizontal battles with their distinct policy goals in mind. For the US, the primary objective has been to advance open markets and internet freedoms, at home and abroad.[45] This policy agenda blends the economic interests of US tech companies seeking to expand internationally with the foreign policy interests of the US government promoting democracy and freedom abroad. In pursuit of this agenda, the US has challenged foreign regulations that compromise the economic interests of its tech companies and condemned various attempts at online censorship that undermine free speech and political freedoms around the world. More recently, the US has turned its focus to technological competition with a determination to ensure its leadership over China. For China, this horizontal battle has initially been a defensive one. The Chinese government has focused on regime survival, political control, and its right to make its own rules for the "sovereign internet." A key concern has been to protect the Chinese market and citizens from harmful foreign influences.[46] But the Chinese government is also increasingly fighting an offensive battle for technological supremacy, both to become more self-reliant in a volatile world but also to prevail over the US in the two superpowers' contest for greater relative economic, geopolitical, and even military power.[47] For Europe, the battle has primarily focused on safeguarding the fundamental rights of European citizens in a globalized world.[48] The EU is seeking to rein in surveillance capitalism and protect European citizens from being exploited by US tech giants. But the EU is also seeking to protect Europeans from American and Chinese government surveillance, which has become easier to conduct in the digitalized world. In addition to this defensive agenda, the EU is now increasingly seeking to bolster its "digital sovereignty" in an effort to shed its dependencies on American and Chinese technologies by building its own technological capabilities.[49]

This horizontal conflict has morphed into several battles, the most prominent one being the unfolding US–China tech war.[50] This battle has reinvigorated the US export control regime, as the US government is restricting outflows of critical technologies from the US to China.[51] It has also galvanized a vigorous investment screening process in the US, limiting

Chinese investors' ability to acquire control of US technologies.[52] China has responded in kind, further constraining US tech companies' access to its domestic market while placing additional limits preventing its own critical technology assets, including sensitive data, from leaving China.[53] Even the stock market is now the target of mutual decoupling, with both China and the US tightening their rules that apply to foreign listings.[54] Both powers have also engaged in a relentless capacity-building effort to gain new technological capabilities while reducing their dependencies on each other. This battle has fueled a subsidy race in semiconductors, batteries, and artificial intelligence, setting off techno-nationalist impulses in other governments as well.

In addition to battling China for the mastery of new technologies, the US is battling Europe over the regulations that govern those technologies.[55] This transatlantic regulatory battle has focused on data flows, with the US and the EU asserting different views on the way individuals' right to privacy can, or cannot, be reconciled with the needs for government surveillance for law enforcement or national security purposes.[56] Another key tension relates to the taxation of the digital giants, with the Europeans insisting on their right to tax some of the revenue that large American tech companies generate in Europe.[57] Europeans have also forcefully leveraged their antitrust laws to constrain the business practices of US companies.[58] In these battles, Europeans are concerned about US tech firms' alleged overreach, while Americans are concerned about European regulators' alleged overreach. The US views the EU's regulatory efforts as both excessive and protectionist, unfairly targeting European companies' more successful American rivals. The EU has responded by insisting on its sovereign right to preserve a competitive and fair marketplace while ensuring that the fundamental rights of Europeans are protected. Thus, at the heart of the US–EU regulatory battle are the questions of who gets to set the rules for the digital economy and what kind of digital society emerges from those rules.

Vertical Battles Between Governments and Tech Companies

The US, China, and the EU are not only engaged in horizontal battles with each other. They are simultaneously fighting vertical battles vis-à-vis the tech companies operating in their markets—tech companies who wield private power so vast and so global that they have been compared to emerging empires themselves.[59] Two features render these vertical battles particularly complex today. First, tech companies are both targets as well as tools for governments. Governments seek to restrain these companies while

simultaneously deploying them in fighting horizontal battles, turning the vertical relationship into a delicate balancing act. For example, China relies on its tech companies to conduct surveillance and enforce censorship, the US harnesses its tech sector to pursue its national security goals, and the EU delegates to these companies the task of enforcing many of its data privacy and content moderation norms. The US, China, and the EU further need these companies to promote economic growth and technological progress in order to enhance their relative economic and geopolitical standing in their horizontal battles. This suggests that tech companies should be seen as both allies and enemies to the governments, helping them to achieve some policy goals while undermining others. The challenge for the governments therefore is to inflict some regulatory constraints on these companies without undermining their roles as forceful instruments in other battles where governments rely on their powerful capabilities.

Second, these vertical battles are complicated by the nature of the global marketplace, where tech companies have multiple masters.[60] These companies often face conflicting demands from different governments, making it impossible for them to comply with all of those demands at the same time. In a nearly decade-long battle that began in 2013, Microsoft was asked by US law enforcement officials to hand over personal data stored on its servers in Europe while simultaneously facing demands by European regulators not to hand over such data under the EU's data protection rules.[61] In 2021, Apple and Google bowed to the demands of the Russian government and removed an app designed by allies of opposition leader Aleksei Navalny to coordinate protest voting in Russian elections, their commitment to freedom and democracy at home notwithstanding.[62] Now, leading tech companies are navigating the Russian invasion of Ukraine, facing conflicting demands from Ukraine, Russia, the EU, and the US on how to handle the disinformation and propaganda on their platforms that are shaping the narrative about the war.[63]

US tech companies operating in China face a particularly difficult balancing act.[64] For example, Apple has been a vocal advocate of data privacy and civil liberties in the US and EU. However, the company has made several concessions in return for being able to operate in China. It has agreed to store the data of its Chinese users locally in a datacenter in Guiyang, where Chinese state employees manage the stored data. Apple also proactively censors its Chinese App Store with the help of algorithms and employees who flag and block apps that do not meet the approval of the Chinese leadership. In another example, in 2017, Google took steps to build a censored search engine for China in an effort to retain its right to operate in the country, only to back down the following year in response to growing criticism in the US that the

company was capitulating to China's censorship demands.[65] More recently, Chinese tech companies abroad have also had to navigate the difficult terrain of regulators' conflicting demands. In 2020, TikTok, a social media company owned by the Chinese company ByteDance, was attempting to comply with the US government's requirement that the company must find a US buyer—under the threat of being banned from the US market—only to learn that the Chinese government responded by prohibiting all artificial intelligence exports, thereby threatening the very sale that the US government required.[66] Similarly, the Chinese ride-hailing company DiDi Chuxing found itself caught between the conflicting demands of the Chinese and US governments regarding the disclosure requirements associated with Chinese companies' initial public offerings (IPOs) in the US. The US Securities and Exchange Commission asked DiDi to hand over data, which the Chinese government maintained could not leave China. This led the company to ultimately delist its shares from the New York Stock Exchange.[67] These examples illustrate how distinct vertical battles often collide, leaving companies with the difficult—and at times impossible—task of choosing which government's demands to comply with.

How the Horizontal and Vertical Battles Intersect and Encourage Restraint

The horizontal and vertical battles intersect in important ways, forcing governments to simultaneously reconcile various, and at times conflicting, imperatives. This interplay across the battles—both horizontal and vertical—leaves governments more constrained in terms of the regulatory policies they can pursue and often forces them toward a strategy of restraint. In the horizontal battles, governments are locked in conflict, yet the countries also need each other. For example, the US government wants to restrict China's technological ambitions, but it needs to preserve US companies' access to the large and lucrative market that China offers. The US export control regime illustrates this tension well. The US requires an export license for many sensitive technologies that US companies want to export to China; in practice, the government often grants those licenses to mitigate the costs imposed on US companies exporting those technologies to China.[68] The US also opposes many EU regulations targeting US tech companies but has an incentive to de-escalate any transatlantic tensions as it needs the EU to join forces with the US government in its battle against China.[69]

Governments are similarly constrained in their vertical battles against tech companies, which are necessary instruments for the governments to

win their horizontal battles. For example, the US government needs strong tech companies to stay ahead of China in the AI race and preserve its overall technological dominance. When the US Congress recently debated more assertive antitrust action, leading US tech companies warned that their ability to compete with the Chinese tech giants would be compromised should their business practices be curtailed by overzealous regulatory action.[70] European regulators also face a delicate balancing act. The EU's ability to set the rules for the global digital economy depends on multinational tech giants concluding that the costs of complying with European rules remain lower than the costs of pulling out of the European market—and that the benefits associated with globalizing EU rules outweigh the benefits of offering customized products in different markets. Should the EU overshoot its mark, these companies might conclude that they will abandon the European market, seeking profits elsewhere.[71] Such a move would fundamentally dissolve the EU's power to shape the digital economy, also undermining the EU's standing in its horizontal battles. Thus, we observe more moderation and de-escalation than we would if vertical and horizontal battles proceeded in isolation from one another.

This interplay across the various battles forces all players toward a strategy of restraint, keeping the battles alive yet de-escalating conflicts and making them more manageable. These interdependencies also explain why we are less likely to see outcomes as stark or extreme as those often predicted in the public conversation about the future of the digital economy.[72] This public commentary often envisions binary outcomes—arguing that the world is forced to choose between the US and China;[73] that the future will feature a global internet or a fragmented "splinternet";[74] or that either governments or tech companies will set the rules.[75] However, this binary way of framing the questions often blinds us to the more complex dynamics that shape the global digital economy. A closer examination of the interdependencies across the key battles suggests that the internet will not be global, nor will we witness full decoupling; China will not triumph over the US, nor will the US triumph over China; governments will not declare a complete victory over tech companies, but neither will tech companies detach themselves from government regulation. Instead, the digital world will likely be characterized by what Mark Leonard, the Director of the European Council of Foreign Relations, calls "the age of unpeace": a geopolitical order where states are too interconnected to fight an all-out war but too discordant to live in genuine peace.[76] In this highly connected and conflict-ridden world, battles will be costly and differences lasting, yet ultimately manageable—producing victories that will be relative as opposed to absolute.

Imperial Expansion: Global Consequences of the Regulatory Models

In addition to engaging in rivalries with each other, the three digital empires are also competing for global influence by exporting their regulatory models to other countries. This way, the US, China, and the EU are each seeking to shift the rest of the world closer to the norms and values inherent in their market-driven, state-driven, and rights-driven models. As a result, the question is not only whether the US or China prevails in their tech war against each other but, even more fundamentally, whether the global digital economy ultimately evolves toward the norms underlying the American market-driven or the Chinese state-driven model. Similarly, the success of the EU model will be judged not only by its ability to curtail US tech companies' market power in the US–EU regulatory battles, but also by its ability to shape the global digital order toward the values that are fundamental to the European rights-driven regulatory model.

When these regulatory models are exported to foreign jurisdictions, they generate both "positive externalities" and "negative externalities" in those jurisdictions. Those externalities are positive, for example, when foreign citizens use US companies' digital technologies to enhance their productivity or to access conversations they find valuable; when foreign governments improve public safety with the help of Chinese surveillance technologies to the benefit of their citizens; or when foreign privacy advocates witness data protection standards elevated around the world thanks to the global effect of the EU's regulation. However, those externalities can also be negative, affecting foreign societies in harmful ways, and evoking of negative connotations associated with expansionist digital empires.[77] Although these three digital empires may not be self-consciously imperial in search for domination over unwilling populations and governments, critics may accuse, for example, the US of "free-trade imperialism," China of "surveillance imperialism," or the EU of "regulatory imperialism." These allegations reflect a perception that the digital empires' global expansion often leads to power asymmetries between the center and the periphery of those empires.

The American market-driven regulatory model is increasingly becoming a source of global concern. Because of the global nature of the digital economy, the effects of the US model are felt everywhere, every day. Limited privacy protections, lenient antitrust laws, and the generally hands-off approach to internet platforms in the US have enabled and nourished a world dominated by large American tech giants. These tech giants are now shaping the lives of digital citizens across all continents. WhatsApp allows its two billion users

across 180 countries to send 100 billion messages a day.[78] Google operates in over 200 countries, where internet users make over five billion Google searches a day.[79] Nobody can deny that these tech giants are fostering global connections among individuals and providing valuable services to internet users around the world.

But these companies are also often shaping foreign societies in deeply disturbing ways. For example, the growing criticism that US companies have pursued technological innovation and commercial rewards at the expense of individual and collective rights of citizens is a global one. To illuminate how the failings of the American regulatory model are felt around the world, consider the role that Meta played in the Brexit campaign that led the United Kingdom to leave the EU in 2020. Its Facebook algorithms amplified the more emotional and controversial messages that were associated with the pro-Brexit campaign, overshadowing the less inflammatory social media messaging of the Remain campaign.[80] During the lead-up to the Brexit vote, Twitter also enabled Russian meddling in the referendum. More than 150,000 Russian Twitter accounts posted about Brexit in the days leading up to the referendum, mostly encouraging people to vote to leave the EU.[81] In another disturbing episode involving Myanmar, Meta admitted in 2018 that it failed to intervene and remove content posted by military and radical Buddhist groups. These groups utilized the Facebook platform to spread hate and racially motivated discrimination against the Rohingya minority, including messages using dehumanizing language and calling for the destruction of Rohingya as a people.[82] Instead of removing posts that were fueling hatred toward the country's Muslim minority, Meta provided a platform for advocating racist attacks and ethnic cleansing.[83] These disturbing developments around the world can be traced to the business models of US tech companies—but also to the US regulatory model that enables those business models to emerge and continue to thrive.

The Chinese state-driven regulatory model is also increasingly having global implications, elevating foreign governments and citizens' concerns about the influence that Chinese tech companies—and the CCP that is widely believed to exert control over those tech companies—have over foreign societies. It is common knowledge that the Chinese government is deploying the internet as a tool for control and surveillance.[84] Much of this surveillance is domestic, geared at controlling political dissent and maintaining social stability within China. However, there is a growing concern among democratic governments and civil rights advocates that Chinese digital authoritarianism is also entrenching around the world as Chinese companies build digital infrastructures in many jurisdictions as part of the country's expansive "Digital Silk Road" project.[85]

One example of such concerns materializing involves the headquarters of the African Union (AU) located in Addis Ababa, Ethiopia.[86] The Chinese government built and financed the building complex hosting the AU, and the Chinese information and communications technology giant Huawei was contracted to provide most of the IT solutions for the building. But in January 2018, the leading French newspaper *Le Monde* reported that it had uncovered a multiyear hacking operation of the headquarters.[87] The report disclosed that, between January 2012 and January 2017, servers inside the AU building transferred data every night between 12:00 a.m. and 2:00 a.m. to unknown servers hosted in Shanghai. After this data theft was discovered, a further investigation revealed microphones hidden in the desks and walls of the building.[88] While it is often difficult to prove that Chinese companies transfer data gained through their overseas operations to the Chinese government, the suspicion of this potential for espionage is already shaping business opportunities for companies such as Huawei.[89] The US is now leading the quest to rein in Huawei's—and, according to the US, the Chinese government's—global influence by banning Huawei from US networks and urging other nations to do the same.[90] This battle involving the US government and China's Huawei illustrates how the reach of one digital empire into the territory of another can morph into a conflict with global implications.

If the US and Chinese models reach across the global marketplace, so does the European rights-driven model. The externalities associated with the EU model relate to the global reach of European regulations. The most interventionist laws constraining the power of today's tech companies can often be traced to European civil servants writing them in Brussels and European judges interpreting them in Luxembourg. These laws call for more data privacy, greater competition, and less harmful content, often shaping tech companies' global business practices and thus affecting digital citizens around the world.[91] As a result, foreign internet users today have more privacy and are exposed to less hate speech online because of the EU. While many of them welcome the global reach of the European laws, others criticize the EU for engaging in digital protectionism and regulatory imperialism while tampering with innovation and free speech—not just in Europe, but around the world.[92]

Whatever one's normative views on the merits of the EU regulations, few can dispute that its impact is felt far outside of the EU. Consider the highly consequential decision in June 2020 in which the European Court of Justice invalidated the US–EU Privacy Shield agreement that had previously provided a legal basis for transatlantic data transfers, citing

inadequate data privacy protections in the US.[93] That decision threw much transatlantic commerce into disarray, as unhindered data flows are critical in sustaining the $7 trillion transatlantic economic relationship. In its 2022 annual report to the US Securities and Exchange Commission, Meta even warned that, absent a government-negotiated solution to the transatlantic data transfers, the company may need to pull out its key services—such as Facebook and Instagram—from the EU.[94] Should this happen, internet users across Africa, Asia, Australia, and North and South America would be disconnected from their friends and family in Europe. This is but one example of what the critics describe as "regulatory imperialism," accusing the EU of externalizing its data privacy norms around the world without seeking the consent of foreign regulators, companies, or internet users.[95]

These examples illustrate how the US, China, and the EU each export their models abroad, expanding their respective spheres of influence as expansionist empires, each with their own global ambitions and distinct methods of influence. The US's global influence today manifests through the dominance of its tech companies that exercise *private power* across the global digital sphere.[96] China's global influence can be traced to its *infrastructure power*, where Chinese firms—all with close ties to the Chinese state—are building critical digital network infrastructures in countries near and far.[97] The EU exercises global influence primarily through *regulatory power* that entrenches European digital norms across the global marketplace.[98] Like traditional empires, these digital empires' growth and expansion is constrained by the efforts of the other digital empires to extend their own influence using their preferred mechanisms. As a result, unaligned foreign markets often turn into critical battlefields, with local governments navigating the effects of American companies, Chinese infrastructure, and European law on their markets. These governments need to decide issues such as whether to allow China's Huawei to build their digital infrastructure, generously financed by the Chinese government while actively opposed by the US government. They must also decide whether to allow the outsized presence of US companies in their markets to shape their economies and societies or to instead join the EU's efforts to restrain them.

This imperial projection has ingrained American private power, Chinese infrastructure power, and European regulatory power deep into the economic, physical, and legal foundations of foreign societies. While there is legitimate criticism of these digital empires' efforts to extend their influence abroad, foreign stakeholders often view the US, China, and the EU operating as "empires by invitation."[99] For example, many foreign consumers welcome the presence of American tech companies in their markets, embracing their

products and services increasingly depending upon them. Many foreign citizens also relish the global reach of EU digital regulations that protect their privacy or help ensure a safer online environment, the same way several foreign governments often willingly emulate EU regulations which they believe benefit their societies. The Chinese Digital Silk Road is also not merely a manifestation of Chinese government's deliberate expansionist strategy; instead, many foreign governments—in particular those across the developing world—welcome Chinese infrastructure (and capital) as a pathway for digital development. Thus, today's digital empires can be both admired and reviled across the territories that fall under their influence.

What Is at Stake: The Battle for the Soul of the Digital Economy

A key question for the coming years is how these battles will evolve and which regulatory model—if any—will dominate in the future. In the public conversation and news commentary, there is a commonly repeated narrative that suggests that the main contest over the future of the digital economy takes place between the US and China. These two powerful digital regimes not only compete for technological supremacy but also engage in a fundamental battle of values as they advance two competing visions for the global digital order: the American vision of economic and political freedom and the Chinese vision of technological progress fused with state control. But this narrative, which leaves the EU and other countries to choose between these two variants of digital worlds, is flawed in drawing the main battleline between the American and Chinese models. Instead, as this book explains, the American market-driven regulatory model is fading as countries around the world are rejecting the free market and free speech as cornerstones of their digital economies.[100] Even the US itself is now questioning the virtues of an unregulated digital marketplace, with the American public supporting stronger tech regulations and Congress debating the need for legislative reform. In deserting the US's regulatory approach, countries around the world are left with choices that lead them to either coalesce behind a version of the Chinese state-driven model or adopt the core tenets of the European rights-driven regulatory models; in that scenario, it is likely that the US will be forced to choose between joining forces with the EU and the rest of the democratic world, or acceding to China's growing influence over the global digital economy.

The prospect of the Chinese state-driven regulatory model prevailing is as real as it is disconcerting for the US and its allies. A growing number of countries in Africa, Asia, and South America in particular are now embracing

Chinese technology for both financial and geopolitical reasons, importing China's state-driven regulatory norms in the process. The US and other democratic countries remain concerned about the way the Chinese government engages in censorship, suppresses individual rights, and deploys the internet as a tool for surveillance. But these very features of the Chinese model are welcomed by many authoritarian leaders seeking to maintain their own political control, suppress dissent, and hold onto power. The number of such authoritarian leaders is also rising in today's world where democracy is on the decline in a growing number of countries.[101]

In contrast, in the democratic world, the European rights-driven regulatory model is emerging as the most desirable alternative to the waning American market-driven regulatory model.[102] The European model is associated with a set of values—fundamental rights, fairness, and democracy—that are often undermined by today's tech giants. The EU's regulatory approach has also been validated by numerous high-profile data privacy and disinformation scandals that have further eroded citizens' trust in tech companies, elevating the EU's standing in the debate and facilitating the global emulation of its regulatory model. Increasingly disillusioned with free markets, toxic online speech, repeated privacy violations, and other harms associated with unregulated tech companies, many American citizens would also welcome the US shifting toward the European rights-driven regulatory model.

At the same time, others remain cautious about emulating the EU model, fearing a loss of technological and economic progress if the government steps in and replaces companies' freedom to innovate with the state's authority to regulate. However, as this book will argue, more digital regulation does not necessarily mean less innovation. Instead, the EU's inability to produce its own tech giants to date can be attributed not to digital regulation, but to various other policies that have thwarted European technological progress. This observation should alleviate the concerns of American policymakers and other stakeholders about the consequences of endorsing EU-style digital regulations, paving the way for their adoption in the US. An additional reason for the US to more closely align itself with the EU arises from the perceived urgency to consolidate a democratic front to restrain China's growing influence. The US is already calling for closer cooperation of the world's "techno-democracies" to counter the growing influence of China and other "techno-autocracies,"[103] suggesting that this contest—where battlelines are drawn according to fundamental political and ideological convictions—is now increasingly central in defining the evolution of the digital economy.

The stakes in the unfolding horizontal and vertical battles cannot be overstated. These regulatory conflicts are taking place in an era of mounting

geopolitical tensions, entangling questions of technology, trade, and innovation with questions of national security and global power politics. The resolution of these battles has a direct bearing on economic prosperity, political stability, and the individual freedom of every person that uses the internet. But the most consequential battle is the one being fought over the very future of liberal democracy itself. As this book shows, there are two likely pathways for liberal democracy to potentially deteriorate through these battles. First, democratic institutions in any jurisdiction will be undermined if the US, the EU, and their democratic allies lose their horizontal battle to China, and governments around the world shift toward a state-driven model. China's victory in this battle would usher in a world where technology is harnessed to empower the state, not its people, subjugating individual rights and freedoms to state control. However, democratic institutions can also be weakened if the US and the EU are to ultimately lose their vertical battle to tech companies—a realistic possibility given the power of these companies and the many challenges the EU has faced to date in implementing its ambitious digital regulations in practice. Victory for the tech giants would leave internet users and societies at the mercy of these companies' business models, even when those business models compromise individual rights or undermine democratic elections. In the end, it is this existential battle over the fate of liberal democracy as a form of government that will provide the US and the EU with the greatest impetus to join forces in both their horizontal and vertical battles—knowing that, if that fight is lost, the battle for the soul of the digital economy is also lost.

The Structure of the Book

Understanding how the global digital economy has evolved to date, and how it is likely to evolve going forward, requires integrating numerous scholarly and policy conversations that span across different jurisdictions and policy domains. This book is an effort to provide such an integrated approach, identifying and analyzing the key forces that determine the legal and political foundations of today's and tomorrow's digital societies. It is divided into three parts, with each part contributing key elements toward the book's larger argument regarding the present and future state of the global digital economy. The chapters in the first part introduce the three *digital empires*—the US, China, and the EU—and describe their regulatory models that provide competing visions for the digital economy; the chapters in the second part focus on *imperial rivalries*, outlining the key battle lines being contested as the regulatory models collide in the global marketplace; and the chapters in the third part address the strategies employed by each for the *expansion of their empires*,

explaining how the US, China, and the EU are battling for global influence, exporting their regulatory models and shaping the digital destinies of the societies and individuals around the world.

Part I (Chapters 1–3) discusses the three digital empires' competing visions of how the digital economy ought to be regulated. In governing the tech industry, the US draws on its market-driven instincts whereas China elevates the role of the state to the heart of its regulatory model. The EU differs from both the American market-driven model and the Chinese state-driven model in its focus on the individual and collective rights of its citizens in the digital economy. Despite many differences across the three jurisdictions' regulatory philosophies, the book shows how all three models also have some overlapping commitments that coexist alongside those differences. All models also evolve over time, which both amplifies their similarities and makes starker some of their differences.

Chapter 1 discusses the American market-driven regulatory model, which centers on protecting free speech, the free internet, and incentives to innovate. This regulatory approach rests on a policy view that places notable faith in markets and embraces a limited role for the government. According to this view, the government needs to step aside to maximize the private sector's unfettered innovative zeal—except when it comes to protecting national security, including cybersecurity, where the government can and must work alongside private companies. The chapter traces the ideological origins of the US model and shows how the values and principles underlying that model have been deeply engrained in existing legal frameworks and actual government policy. However, the political winds are turning in the US as well. The public and political leaders are starting to question the virtues of the free internet and the growing role of the largest tech companies in ordering our societies. At the same time, many voices remain skeptical of change and maintain that market-driven values are deeply entrenched in Americans' institutions and mindsets, making it difficult to reverse the regulatory model that, despite all its limitations and false promises, continues to be associated with tremendous wealth and technological progress.

Chapter 2 examines the Chinese state-driven regulatory model. It shows how the Chinese government leverages technology to fuel the country's economic growth and development. In the name of social stability, the government also uses technology as a tool for political control, surveillance, and propaganda, entrenching digital authoritarianism deeply into the Chinese society. These two factors—economic development and social stability—are central to the survival of the Chinese Communist Party (CCP). The chapter engages with criticism of the Chinese regulatory approach, detailing how

the state-driven model infringes individual rights and deprives Chinese citizens of key civil liberties. At the same time, it acknowledges that technological breakthroughs can also emerge under a state-driven regulatory model, suggesting that freedom may not be necessary for a dynamic culture of innovation. However, the future of the Chinese tech industry is uncertain. As with the US, the Chinese regulatory model is undergoing a drastic shift as the Chinese government is abandoning its traditionally lax approach toward tech regulation, and forcefully leveraging its powers to crack down on the tech industry in the name of "common prosperity" while facing little resistance from the industry. This unfolding change further reinforces the core tenet of the state-driven regulatory model by ensuring that the Chinese government, not tech companies, reigns supreme over the digital economy in China.

Chapter 3 brings into view the third major model of digital regulation—the European rights-driven model. The chapter illustrates how the EU asserts its regulatory power in the name of upholding individual and collective rights, protecting democratic values, and ushering in a fair and human-centric digital society. To further these goals, the EU model distributes power away from large tech companies to smaller firms, internet users, and platform workers. The EU often refers to the "digital society of rights and values," which, it claims, cannot be realized under the market-based model that permits the exploitation of personal data by tech companies, nor under the state-centric model that permits censorship and surveillance by governments. The EU further engrains those rights and values in binding regulatory instruments, reflecting its belief that digital transformation needs to be firmly anchored in the rule of law and democratic institutions. Despite the many benefits associated with the EU's regulatory model, the chapter also addresses its shortcomings, including the common criticism that extensive regulation impedes innovation, thereby explaining the EU's inability to date to produce tech companies akin to those that have emerged and thrived under American and Chinese regulatory models.

Part II (Chapters 4–6) turns to analyze conflicts that ensue when the three regulatory models collide in the international domain. Those conflicts manifest both as vertical battles, involving governments and tech companies, and as horizontal battles, involving the governments themselves. It starts by examining the difficult choices faced by tech companies caught between conflicting demands of different regulatory models, before moving to examine the US–China tech war and the evolving regulatory conflicts between the US and the EU.

Chapter 4 specifically examines how American and Chinese tech companies straddle between the market-driven and state-driven regulatory models as they

fight vertical battles against the US and Chinese governments, facing increasingly irresolvable regulatory dilemmas. At worst, tech companies are forced to choose which of the models they comply with—while knowing that their compliance with one regulatory model is deemed to violate another. For example, a Chinese tech company listed in the US stock exchange cannot at the same time obey the US government's request to disclose certain data and the Chinese government's request not to disclose that same data. Similarly, US tech companies operating in China must acquiesce to the Chinese government's demands to censor online content, which puts them directly at odds with the American regulatory model emphasizing free speech, and exposes them to criticism among US lawmakers, their US-based customers, and their own employees. These conflicts have grave implications for the companies involved but also for the broader digital economy, as they risk partially decoupling the leading tech ecosystems.

Chapter 5 shows how the individual vertical battles discussed in Chapter 4 are now evolving into a broader horizontal conflict between the US and China as the two digital powers are fighting for technological supremacy. Over the past few years, the US has taken a number of measures to restrict China's access to strategic technologies, citing national security concerns. China is responding in kind, imposing extensive export and investment restrictions on US companies. This ongoing rivalry has also fueled a subsidy race as the US and China both seek to shore up their capabilities in critical technologies such as semiconductors. Other countries, including those in the EU, are also turning to industrial policy in the midst of the growing US–China tensions and unraveling global supply chains. As a result, the tech war risks entrenching techno-nationalism as a global norm. This can be seen as a victory for the Chinese state-driven model as governments are abandoning the US's vision of an open, free, and global digital economy. The chapter predicts that the US–China conflict is likely to continue, even intensify. But it also shows how deeply intertwined supply chains and commercial pressures in both the US and China are likely to prevent a full decoupling of US and Chinese technological assets. As a result, the horizontal conflict will remain costly, yet will also feature elements of restraint, ultimately denying both satisfactory resolution and averting a complete balkanization of the digital economy.

Chapter 6 closes out Part II by discussing transatlantic regulatory battles, revealing how the US tech companies and the US government are in a much more tenuous position than widely understood. They have over the past years been fighting a two-front battle, not just with China, but also with Europe. One of the most notable areas of transatlantic disagreement relates to data protection, where the EU's focus on fundamental rights clashes with the US's

focus on national security. This disagreement has become a major obstacle for data flows between the EU and the US. Other dominant conflicts revolve around antitrust policy and digital taxation, both realms where the US government has perceived the EU's attempts to impose obligations on American tech giants as acts of digital protectionism. However, on many of these issues, the transatlantic gap seems to be gradually closing. The US is conceding that more regulation of the tech industry is needed and thus moving toward the European regulatory approach, paving the way for transatlantic rapprochement and cooperation. What gives an even greater impetus for bridging the remaining transatlantic differences is the EU and US's shared concern about China's rise and the impact of that rise on the future of liberal democracy. Both parties acknowledge that their policy differences seem manageable compared to China's AI-powered mass surveillance, internet censorship, and government propaganda, all of which are antithetical to the values of democracy and freedom that the EU and the US have long embraced at home and championed abroad.

Part III (Chapters 7–9) extends the discussion from various bilateral battles between digital empires to a global battle that reaches across all continents. In addition to engaging in mutual rivalries, the US, China, and the EU each seek to expand their respective spheres of influence, looking to gain relative influence by shifting the global digital marketplace toward their competing norms and values. In reaching across jurisdictions, each is relying on different forms of influence, with the US leveraging its private power, China its infrastructure power, and the EU its regulatory power.

Chapter 7 examines how the US has exported its market-driven ideals primarily through the penetrating influence of its leading tech companies, which have shaped digital economies around the world through their business practices. Private tech companies have thus been key in not just defending the American market-driven ideals at home, but also in universalizing them through the often-unmitigated influence they exercise over the digital lives of internet users abroad. The US government has further paved the way for its companies' global influence by actively promoting its "internet freedom agenda" as a key element of its foreign policy, urging governments around the world to commit to the economic and political freedoms that underlie the US regulatory model. However, the US model is now becoming a victim of its early success. The outsized influence of the US tech companies and their harmful practices are creating a backlash across jurisdictions. This growing resentment is further contributing to the decline of the US regulatory model and, with that, the dwindling of the influence of the values associated with the most powerful digital empire.

Chapter 8 turns to examine how China is gaining global influence by building digital infrastructures around the world. Country by country, Chinese tech companies—all with varying ties to the CCP—have built the physical components of digital infrastructures, provided critical telecommunications and electronic commerce (e-commerce) services, and supplied surveillance technologies along the Digital Silk Road. This chapter shows how Chinese tech companies have made inroads into numerous markets across Asia, Africa, and Latin America and even parts of Europe. China has also gradually assumed control of key positions in relevant international organizations involved in standard setting across technologies, further allowing the Chinese government to entrench its regulatory standards and surveillance practices—and, with that, its values—around the world. Many receiving countries have welcomed Chinese technologies and accompanying regulatory standards as a path toward digital sovereignty and development. For authoritarian governments, an additional motivation has been to gain access to surveillance technologies that they eagerly use toward illiberal ends. The chapter discusses the unease the US and its allies have regarding the growing sphere of China's influence yet also acknowledges the difficulties they face in countering that influence.

Chapter 9 moves to examine how the EU has also wielded significant international influence through its digital regulations that have spread around the world. By adopting laws such as the GDPR, the EU often shapes the global business practices of leading tech companies, which often extend these EU regulations across their global business operations in an effort to standardize their products and services worldwide—a phenomenon known as the "Brussels Effect." While the GDPR may be the posterchild of the EU's global regulatory influence, this chapter shows how antitrust law, regulation of online content, and rules for emerging technologies such as artificial intelligence can be similarly exported through the Brussels Effect. European digital regulations have not only been incorporated into tech companies' global business practices, but often ingrained in legislation by foreign governments. As democratic governments are turning away from the American market-driven model, they are increasingly embracing the European rights-driven model as an alternative way to govern their digital economies. At the same time, while many foreign stakeholders welcome the EU's global regulatory power, others criticize the EU for engaging in regulatory imperialism and thus undermining the authority of governments to regulate their digital economies in accordance with their national interests and democratic preferences.

The conclusion asks whether the American, the Chinese, or the European regulatory model will prevail in their horizontal battles and quest for global

influence, while simultaneously examining whether the tech companies or governments will ultimately triumph in their various vertical battles. It predicts that the European rights-driven regulatory model is likely to prevail over the American market-driven model within the democratic world. At the same time, the continuing appeal of the Chinese regulatory model limits the EU's ability to entrench its norms and values outside of the democratic world. In addition, the EU model is haunted by the difficulties of enforcing its regulations against powerful tech companies, threatening to render its victory in the battle of values a hollow one. In this state of the world, the US needs to decide whether to align itself more closely with the European regulatory model—in part in response to a shift in domestic policy preferences and in part to contain China's growing influence over the digital economy. If the US can be convinced that embracing the European rights-driven model will not impede innovation and compromise its technological progress, this choice to emulate the EU model will be easier to embrace. Ultimately, the most compelling argument for closer transatlantic alignment comes from a shared perception that the US and the EU both need to focus on the battle that matters the most: the battle that will be fought over the fate of liberal democracy. That battle will ultimately determine the soul of the digital economy, defining what kind of society we will live in for years and decades to come—a battle that neither the US nor the EU can afford to lose.