Dilemmas and tradeoffs of digital governance models: the European Union, China and United States compared

Klooster, K. van t; Hosli, M.O.; Torres Jarrín, M.

EU Diplomacy in the Digital Age.

Authors:

Kayle van't Klooster and Madeleine Hosli

Chapter Title:

Dilemmas and Tradeoffs of Digital Governance Models: The European Union, China and United States Compared

Abstract:

How a state approaches digital governance can directly and significantly impact economic, social, and political trends domestically. The strength of democracy, especially within the context of the global democratic recession, is often argued to be closely tied to digital governance. This chapter explores how a state's chosen model of digital governance impacts the strength of its democracy over time, by exploring the different approaches to digital governance utilized by the European Union (EU), China, and the United States. The United States has primarily prioritized economic gains in its model to digital governance and while this has produced considerable economic gains, it has been at the expense of the strength of its democracy. China, on the other hand, has prioritized state control and political stability. This has indeed strengthened the Communist Party's authoritarian grip on power, but the crackdown has also stifled China's once-flourishing technology sector. Finally, the EU and its member states have developed a human-centered model, that prioritizes regulation, inclusivity, and democracy. However, the EU has had issues in the past asserting its digital sovereignty and promoting its technology sector. The chapter argues that democracy must be carefully considered when conducting digital policy. While competent digital governance can have a democratizing impact if the government embraces it fully, the opposite is also true. Often, digital governance has proven to be self-reinforcing. Governments utilize digital governance to become more democratic or authoritarian depending on their regime. However, digital governance is complex, and governments face several trade-offs and dilemmas in terms of their policy approaches.

The research question we aim to resolve with this book is: *What is the role of the EU in the digital age?*

Introduction

Policymakers around the world have diverged in how they approach digital governance. This chapter will summarize and analyze the three most prominent and influential approaches, the capitalist American approach, the Chinese authoritarian approach and the European regulatory approach. Each approach has costs and benefits for each respective polity. While the American approach has generated astounding economic gains for the country, it has come at the expense of the strength of its democracy. Similarly, while the Chinese government has used digital technology to strengthen the Communist Party of China's (CPC) domestic position, it has hampered the growth of its digital economy, especially beyond China's internal market. Lastly, Europe adopted a human-centric approach which seeks to uphold democratic values but risks losing out on economic activity and innovation.

This divergence in approaches to digital governance comes at a time when many democracies have weakened. Even the United States of America, once the world's most ardent defender of democracy, has not been immune. There are many causes for the democratic recession, but many academics and policymakers are increasingly blaming challenges in cyberspace as the drivers of this anti-democratic influence. Many experts have expressed concerns that advances in digital technology could weaken core aspects of democracy and democratic representation over the next decade (Rainie & Anderson, 2020). Cyberspace has become increasingly important, and its impacts non-neglectable, for democracy to reverse its decline. Moments of crisis, such as the Covid-19 pandemic or the 2022 Russian invasion of Ukraine, have underscored the importance of effective digital governance, as these crises brought with them difficult digital challenges, notably widespread disinformation.

There is a plethora of digital challenges that threaten the health of democracies globally. 2016 was an obvious watershed for this threat. Two significant votes that year, the Brexit referendum, and the American presidential election, were both colored by subsequent outrage at issues and disruptions in cyberspace (Scott, 2018; Guo, Rohde & Wu, 2020; Frost, 2020). These high-profile votes were catalysts that spurred the increased academic attention made poor digital governance a common factor to cite when seeking to explain the recent erosion of democracy (Manville, 2019; Zuboff, 2020; Walker, 2016; Scott, 2018; Rolfe, 2016; Rainie & Anderson, 2020). Various potential undemocratic influences have been identified, such as online

disinformation, political polarization and social disorder driven by online discourse and foreign influence in the democratic process (Engesser, Fawz & Larsson, 2017; Bastug, Douai & Akca, 2020; Frost, 2020).

While not immune to these threats, the EU is uniquely positioned to positively shape digital governance and the digital future generally in the coming years. As an established regulatory power, it has already had some successes in bringing about a more human-centric digital world which is based on democratic standards and values. However, these successes should not come at the expense of economic, or technological loses. In addition, the EU must continue to work with other democratic nations, especially the United States, to ensure that there is further convergence on digital policies and the integration of democratic standards into digital technology.

Understanding the trade-offs inherent in different models of digital governance could be essential in building a knowledge base that democratic countries can employ to strengthen democracy, while minimizing loses in economic activity and innovation. If there are remedies to what ails democracy, governments in the West cannot ignore them. An analysis of the three leading approaches to digital governance helps to refine concepts and give policymakers a clear understanding of what is at stake in this debate.

The Chinese Approach

China's approach to digital governance has been labeled "digital authoritarianism" (Lilkov, 2020; Schneider, 2020). This approach has conceptualized digital governance as a means of strengthening state control over various aspects of society. From traditional surveillance technology like security cameras, to more dramatic measures like the now infamous social credit system, the CPC seems set on using the full extent of digital technology's more problematic capabilities. This model has successfully barricaded Chinese cyberspace from the international internet and barred its citizens from engaging with unwanted content, enabling a higher degree of state control over citizens. However, this dramatic increase in political power over the population has come at a cost. While China's tech companies like Alibaba and Tencent were once rapidly expanding with little expectation of any slowdowns in the near future, the CPC's heavy handed policy work has slowed significantly.

The basis for China's digital authoritarianism is the surveillance of its vast population by collecting tremendous amounts of data. While the largescale collection of big data is certainly not a phenomenon exclusive to China, there are three major sources which make it more effective in the Chinese market, the internet of things, smart cities and super apps. Each of these are more prevalent in China than in the West (Deng & Chen, 2018; Mozur, 2020; Wood, 2015). Abusing user data is also far from exclusively an issue in China but it is essential for the West to understand how authoritarian regimes use big data and set up protections against these sorts of practices. Unlike in the West, where data is primarily monetized through the use of hyper-targeted advertising, this data is increasingly used for pervasive surveillance. This massive amount of data has enabled Chinese authorities to make sophisticated systems such as facial-recognition systems which can identify citizens even if their faces are partially covered (Baptista, 2022).

A new policy approach, called "one person, one file" has become popular with companies and the state organizations in China. Based on this policy, new systems have been developed to organize the massive volumes of data. These systems collect data and use complex algorithms and machine learning to create customized files for individuals. According to government documents, these files even update themselves automatically as the software sorts the data (Baptista, 2022). However, just as in the West, it is China's tech giants who are collecting this data, and this has made the CPC nervous. As a result, there has been increasing domestic pressure on China's tech companies.

The CPC has engaged in a widespread crackdown on its digital technology industry, which intensified significantly in 2021. The crackdown has several official motivations, including the need to ensure that wealth generated by tech companies is evenly distributed among the population and the need to curb excess debt. However, it is increasingly apparent that the crackdown is inherently politically motivated (Mozur, 2020). Companies that enjoy close relationships with the government, such as Huawei, have been largely left alone while others are not as fortunate. DiDi, a once promising ride-sharing app became the target of Chinese regulators shortly after its initial public offering on the American stock exchange. Chinses regulators removed the app from Chinese app stores, arguing that DiDi was misusing user data. This resulted in Didi going from being considered the most valuable Chinese start-up to running an

operating loss of $6.3 billion for the first nine months of 2021. The crackdown has been described by some experts as “data nationalization” and could transform this crucial economic sector into a mere appendage of the state (Yuan, 2022).

This crackdown has had negative economic consequences for the China’s economy. For many tech companies, even some of the best-known tech giants, this new regulatory era is a time of layoffs, reductions and faltering growth. In the third quarter of 2021, Tencent posted its slowest revenue growth since its public listing and the e-commerce giant Alibaba’s profitability declined 38% from 2020 (Yuan, 2022). For workers, the crackdown has been similarly problematic. The extreme measures taken against the education technology and online tutoring industry, which the CPC saw as a factor driving down the birthrate, has led to millions losing their jobs. Layoffs are common across the sector, dashing the dreams of many ambitious young graduates who had hoped to join the once-prosperous industry and adding to a rising youth unemployment rate (Yuan, 2022).

Companies in China must now follow much stricter data storage rules, in pursuit of “cyber-sovereignty.” Chinese companies must now ensure their data is stored domestically and there are tight restrictions on sending data out of the country. Companies which run afoul of these rules face steep financial penalties. This is part of the reason why DiDi faced such difficult regulatory blowback (Haldane, 2021). In addition, state censorship and propaganda have stifled the growth of creative outlets and platforms. iQiyi for example was once hailed as China’s answer to Netflix, watched as their shared fell 85% over the course of 2021. These restrictions have also slowed innovation. For some fields like AI, where access to large amounts of data, sufficient investment and a supportive environment are crucial, China is losing its international competitiveness (Yuan, 2023).

All this domestic pressure has slowed growth in China’s tech and digital sectors, but it has not killed it. More importantly for the CPC, their iron grip on political power in the world’s most populous country is growing stronger. This showcases how digital governance can work as a kind of policy feedback loop. When an authoritarian country employs an authoritarian style of digital governance the impact will inevitably be a more authoritarian, perhaps totalitarian state. As seen in this example, digital governance allows a state to double down on its ideological leanings. For China and its ruling party, this means an even stronger authoritarian style which

succeeds in the CPC's ultimate goal, securing its domestic position. However, China also sees digital authoritarianism as a valuable asset for exportation. The level of control China's innovation gives the state is very attractive to other authoritarian states (Wang, 2021). Therefore, it is crucial to understand China's model of digital governance so that it can be effectively countered on the global marketplace of ideas. However, when these ideological leanings differ, it is clear how digital governance can be used to achieve very different policy goals.

American Approach

The American model of digital governance has privileged economic considerations above social and political implications. The ideological factor which shapes American digital governance the most is not democratic ideals, but a dedication to capitalism. A clear focus of policymakers is maintaining a laissez-faire, free-market approach, which prefers self-regulation to government regulation (Schneider, 2020). This has of course led to economic success for American businesses. The big five of Silicon Valley, Microsoft, Alphabet, Facebook, Amazon, and Apple make up a large portion of economic growth in the United States and four out of the five are worth more than $1 trillion. However, this economic success has not come without tradeoffs, which have taken the form of negative social and political trends (Pitt, Diaconescu & Ober, 2018 pp.39). Indeed, the United States has become a posterchild for the global democratic decline. Placing the blame for this democratic decline on challenges in cyberspace has become a common narrative in both academic literature and popular media (Manville, 2019; Zuboff, 2020; Walker, 2016; Scott, 2021; Rolfe; Rainie & Anderson, 2020). This narrative has been further strengthened by the shocking storming of the United States Capitol building on January 6th, 2021, caused in part by online radicalization and the emergence of fringe movements like QAnon. These issues have sparked public debate on regulating American social media (Ghosh, 2021; Rubin, Bruggeman, & Steakin, 2021; Sunstein, 2000).

The American approach, characterized by libertarian values, and a free market approach to digital governance, is argued to prevent government influence over online discourse and protect freedom of speech (Schneider, 2020 pp. 3). This orientation has made private companies very wealthy but also hugely influential as companies can now determine what is acceptable content and can shape online political discourse (Zuboff, 2020). Public discourse, especially online, is

increasingly problematic in the United States as a myriad of issues have arisen, such as online disinformation, political polarization, and radicalization (Engesser, Fawz & Larsson, 2017; Benkler, Faris & Roberts, 2018; Bastug, Douai & Akca, 2020; Frost, 2020). Each of these issues have proven difficult for the American model to address adequately, due to its economic structure and overreliance on market solutions. The negative social impacts of social media are caused by the same features which keep costumers coming back to the platforms. These worrisome impacts are not overlooked by the public either, as a growing and clear majority of Americans agree that social media is dividing the country (Murray, 2021).

American citizens have become politically polarized, which creates antagonisms and a sense that political disagreements are increasingly personal (Pew Research Center, 2014). The average Republican and Democrat have moved further right-wing and left-wing, respectively. Even more concerning is that antipathy is surging in both groups and a growing number of both party supporters see the other party as a threat to the United States (Pew Research Center, 2014). This political discontent is partly caused by America's social media and online political discourse as social media platforms like Facebook and Twitter are prone to creating echo chambers. Citizens see specialized content that reinforces their worldviews, even if they are highly problematic or based on false information (Guo, Rohde & Wu, 2020, pp 235). Social media companies are economically incentivized to show users content that is specially selected for their viewing. This process keeps users engaged and ensures that everything users see is based on their expressed ideological views without critical consideration (Freelon & Wells, 2020, pp.147). The only opposing views they see are often extreme and meant to cause outrage, which keeps the users engaged by manipulating their emotions and polarizes them further from other political views (Dawson, 2020, pp.67). Gradually, users become more set in their ways and potentially hostile to those who challenge them.

As Sunstein (2000) argues, citizens who have been collected into homogenous groups gradually adopt increasingly extreme views. Groups that users join on Facebook and other social media sites have this effect. Sunstein (2000) also notes that including dissenting opinions can ward off polarization and extremism, but users will often moderate these groups and exclude anyone who dissents. In addition, citizens have also become more prone to being swayed by populists who capitalize on the polarization and alienation caused by social media (Engesser, Fawz & Larsson,

2017; Rolfe, 2016; Bobba, 2018). Constant re-enforcement of one's ideological perspective can contribute to radicalization. Online radicalization is more influential in the radicalization process than traditional sources of radicalization like friends, family, radical clerics, or political figures (Bastug, Douai & Akca, 2020 pp.631).

There is also a certain degree of variation in how the two major American political parties' approach digital governance, which reflects this political polarization. The Democratic party has become increasingly willing to intervene when it comes to countering disinformation and content moderation. However, there are some exceptions to this. For example, the Republican party remains willing to crack down on foreign-owned companies such as Tik-Tok (Washington, 2024). Indeed, both parties have shown willingness to intervene for foreign policy purposes. For example, anxiety over losing market dominance over key technologies such as 5G has prompted government interventions. These actions have their origins in the trade war which President Trump launched in 2017 (Schmalz, 2024).

Radicalization is also linked closely to exposure to disinformation and false information. The United States government has effectively allowed for its digital communications to become an incubator for disinformation, although disinformation can also originate abroad. The impact of disinformation may play a central role in America's democratic decline (Benkler, Faris & Roberts, 2018; Lange, 2020). However, combating disinformation and other toxic content is not as simple as merely removing problematic content, as this limits public debate and establishes a context in which all content must be approved by the ruling power, stifling debate and limit the space for dissenting opinions (Frost, 2020 pp. 16). Despite its flaws, this is the current system and the ruling powers are the companies which own social media platforms, rather than public officials.

Mark Zuckerberg previously stated that he does not want tech companies to become "the arbiters of truth" (Fernandez, 2020). However, it is currently up to these companies to combat disinformation on their own. This responsibility also makes these companies unjustly influential in the democratic process. This fact is not lost on wealthy elites either and increasingly many see the potential for using this influence for their own benefit. For example, some have speculated that Elon Musk's initial interest in acquiring Twitter is motivated by the political influence it will give him (Leparmentier, 2022). Musk's continued rise in political influence seems to have

confirmed this. Cracks are beginning to show in this status-quo however, as social media companies have begun to be increasingly unwilling to work to remove problematic content. It is unclear whether American officials will act to fill this policy vacuum (Booth, 2025).

Disinformation spreads more easily in the United States due to its basic economic structure. Because disinformation can keep users engaged, digital platforms are incentivized to develop algorithms which build psychological profiles citizens and micro-target with disinformation which will keep them engaged. This function was precisely what allowed Cambridge Analytical to be so successful at influencing the 2016 American election and the Brexit referendum (Cadwalladr, 2018). This microtargeting is the business model of most American technology companies, although it is typically used for corporate advertising, not political manipulation. Zuboff (2020) describes the economic structure of American cyberspace as surveillance capitalism. Surveillance capitalism is an economic system in which massive amounts of personal data are fed into algorithms and machine learning programs to create predictive products, essentially collections of assumptions on our individuals will act in the future. These behavioral predictions are then bought and sold on markets. This system is the business model of most large American tech companies, particularly its social media platforms, and has first built and implemented by Google (Zuboff, 2020 pp.8).

Improved strategies must be implemented to counter the threat of disinformation. In the current state, the political polarization and mass manipulation of citizens through disinformation has “strikingly limited “the American public’s viability as a democratic check (Graham & Svolik, 2020). Building new collaborative tools to counter disinformation, which shares the responsibility between the private companies, government, and civil society groups, would be ideal. Unfortunately, the American prioritization of economic gain and free-market policies has resulted in a system that promotes the spread of disinformation, rather than combats it. Efforts to counter disinformation may also be undercut by the financial incentive for social media companies to continue to allow problematic content. Content that is attention-grabbing and triggers an emotional reaction in the user is precisely the kind of content, social media news feeds are meant to show users, since it maximizes engagement (Dawson, 2020 pp.67). For this and other reasons, social media companies are not trusted by the public to be objective in their efforts against disinformation. Many Americans, especially Republicans, believe that social

media companies are purposely censoring their political views. This loss of confidence nullifies the attempts by social media companies to correct disinformation (Vogels, Perrin, & Anderson, 2020).

Ultimately, the United States must reform the economic structure of cyberspace. Although it has been hugely successful in generating wealth, the current structure is unable to tackle the challenges of political polarization, radicalization and disinformation. There is also a real risk of these systems enabling mass manipulation for either corporate profit or political power (O'Connor & Weatherall, 2019; Zuboff, 2020; Dawson, 2020). The democratic woes do not come from glitches but from the system working as it was designed to.

The European Approach

In contrast to the Chinese and American models, the EU attempts to promote a human-centric approach to digital governance which emphasizes democratic norms and values. Some of the most prominent focuses have been privacy regulations, anti-monopoly policy and curbing the influence of large, non-European tech companies. Although previously national government had taken the lead on making digital policy, the center of gravity has shifted considerably towards the European level. The EU has taken an active role in implementing tighter regulations on user data and attempting to limit the influence of large tech companies (Goodman, 2020). Although national governments have not stopped engaging with digital governance altogether, there does seem to be some agreement that working at the EU level ensure the policies are as impactful as possible (Mărcuţ, 2020 pp.59). Specifically, it is the European Commission that has become the central actor in developing European digital policies (Mărcuţ, 2020 pp.66).

One of the first major policy proposals in the EU was the implementation of the Digital Single Market in 2015. This policy initiative was based on three pillars: access, environment and growth. Access referred to measure meant to enable better access to digital goods and services for citizens and business across the EU. Environment in this case refers to the efforts to bring about the appropriate conditions and a level playing field for digital economic activity. Lastly, the third pillar is maximising the growth potential of the European digital economy (European Commission, 2015) Generally, this policy has been well received within Europe and is found to

have contributed significantly to economic growth (Marcus et al., 2019). However, its most significant effect has been the unification of the EU's significant market power into one bloc. This elimination of national boundaries in the digital economy, coupled with a European Commission which has stepped up as a coordinating actor to implement digital governance policies has enabled the EU to become a global regulatory power due to its utilization of the European market power.

The EU, directed by the European Commission chiefly, has undertaken a number of high profile and influential policy measures to govern digital technology. The most well known and influential of these digital policies is by far the General Data Protection Regulations (GDPR). The GDPR was an ambitious piece of legislation at its inception, as it covered the data of all EU residents, regardless of where that data is processed (Goddard, 2017). Once implemented, it pushed to establish higher standards of transparency concerning how the data was used and accountability which ensured that the data was sued responsibly. Because of the wide jurisdiction the GDPR has, European regulators have often cooperated with third parties to govern big data around the world (Goddard, 2017). This cooperation with third parties means that Europe's regulatory influence in the digital sphere is significant. Many countries reference the GDPR when producing their own data protection regulations and due to the GDPR's wide scope many Chinese or American companies already have to follow the EU's regulation (Goddard, 2017; Li, Yu, & He, 2019). As of 2021, the European Commission has recognized a number of countries that had adequate level of data protection in line with the GDPR, including Japan, South Korea and Argentina (European Comission, 2021).

Another high-profile plank of the EU's regulatory model is its continued struggle to enact anti-trust actions against large, often-times American tech companies. There is an observable tendency of modern high-tech companies to establish monopolies quickly and effectively. This stems from the fact that tech companies often operate based on self-reenforcing network connections, which benefit greatly from rapidly becoming the most popular and remain dominant because they are. In addition, tech companies can scale up very quickly to serve a large user base far faster than a company that relies on traditional infrastructure, especially expenses like retail space or a large workforce (Bartlett, 2018, pp. 132). Tech monopolies present in developed countries today are more challenging to break up than past monopolies because anti-trust laws in

many countries specifically call for action when raising the prices for consumers. Tech companies usually push the prices down for consumers, at least initially. In addition, most of the political debate on monopolies will occur on those platforms, which politicians and civil society are also now dependent on to reach their communities (Bartlett, 2018 pp.132).

The EU has shown increasing willingness to work to curtail monopolies or what it calls "gatekeeper companies," companies which have platforms on which users success other content or products. The Digital Markets Act, passed in March 2022, takes aim at companies which the EU claims use anti-competition tactics to cement their market positions. Among the companies most likely to be impacted are Google, Meta, Apple and Amazon which smaller European companies like Booking have had accommodations written into the law (Stolton, 2022). This is however only the latest in a long string of battles, often playing out in courtrooms in drawn out disputes, which EU competition chief Margrethe Vestager has fought. In 2017, Commissioner Vestager led the charge to levy a €2.42 billion fine on Google for abusing its dominant position in the search engine market by giving advantages to its own shopping service over competitors (European Commission, 2017). Cases like this are increasingly common in the EU and show that while the American model implicitly supports the creation of massive, influential companies which can maximize their profits, the EU would rather create an equal playing field for all.

Unfortunately, this focus on regulation and attempts to limit the influence of private companies comes with a trade off. The EU needs to improve how it stimulates innovation and supports growing technology companies to ensure it has a private sector which can compete with China and the United States. Some commentators argue that the EU's regulatory fixation stands in the way of innovation, just as China has similarly stifled its innovation. The development of so-called "digital champions," large American-style tech giants, has not occurred in the EU with the exception of ASML in the Netherlands. Some have argued that this is a failure of the Digital Single Market, which deprives European tech companies of the large domestic market and sources of user data which American companies benefit from more readily (Gaskell, 2019). Across the European market, many companies struggle to expand beyond their domestic borders. Increasingly many argue that the EU is overregulating its digital economy, a sector which is indeed much less explosive than the American or Chinese counterparts. There is indeed a risk that prioritizing issues like user data protections and localization over economic growth for too

long may mean that the EU will be continually unable to innovate and reliant on foreign technology (Lewis, 2022).

The EU should be aware of the economic trade off which this regulatory approach may have imbedded within it. However, even though the claims that this approach is bad for business are not exaggerated, the EU still has reason to follow this regulatory framework. Many of the democratic challenges which are present in the American model of digital governance are addressed by the European model. The EU is also the only major model of digital governance which explicitly aims to safeguard liberal values and democracy over all other concerns. This is quite significant and will likely motivate the EU to stay the current course. There will likely be more efforts in the coming years to build on the EU's previous work by pushing forward with more alignment with like-minded countries on issues like devising trustworthy artificial intelligence, managing markets to balance innovation and fairness, and data to establish user control over digital identities.

Conclusion

Democracy must be a priority when policy makers are considering how to regulate cyberspace Europe and the United States use many of the same devices, platforms, and infrastructure components, although the majority of these are American. Building on this interoperability with further collaboration in the digital domain, with an emphasis on democracy, would benefit both parties. Each party has proven to be very adept at what the other struggles in. While the United States has generated enormous wealth form its digital sector, the EU has failed to germinate any digital champions. Simultaneously, while the United States has largely shied away from regulation in its approach to digital governance, the EU has implemented ambitious policy programs which have been influential globally. With an eye on the risk emanating from China's digital authoritarianism, The EU and America are critical to safeguarding democracy. There must be further cooperation and convergence between the two, each adopting each other's strengths, in order to find success in the future. In short, a more unified democratic model of digital governance should be developed which is committed to democratic norms and ideals, while encouraging economic growth.

Digital governance is a reinforcing factor that can either improve democracy when done right or works to accelerate a country's democratic decline if neglected. Digital governance is not an island apart from other aspects of governance but an integral part of governing a modern state. Democracies must actively decide how to govern cyberspace or face the consequences of its neglect. This is phenomenon which China understands very well, and it is precisely why the Chinese model of digital governance is designed as it is. Lilkov (2020) and Wang (2021) both show that China strengthens the power of the Chinese Communist Party through digital authoritarianism, further cementing their totalitarian rule. The democracies of the world must counter this strongly, especially as the influence of the authoritarian model creeps across the globe.

Digitalization has sown political polarization, radicalization and disinformation. Many of the major issues which are caused in part by the flaws in the American model can also be seen plainly in the EU and beyond. However, if policymakers do not deftly maneuver past the obstacles and pitfalls of cyberspace, the democratic recession will only continue to worsen. Democracy has indeed lost momentum internationally and is suffering from a kind of crisis of confidence. However, if democracy is prioritized when policymakers engage in digital governance, democracy can recover.

The EU, along with the United States, must double down to its efforts to use digital governance as a means of safeguarding democracy. This should be down by sticking with the strong stance the EU has already taken on regulation in the digital domain and continuing efforts to reach out to third parties to converge on regulations. The EU must also remain steadfast in this approach, despite pressure which may emanate from the United States to ease off regulatory pressure. In addition, more innovative solutions, inspired from the American model, should be employed to help grow the European technology sector. Policymakers must recognize the current tradeoffs inherent in the models of digital governance and work to correct them, so that democracy can continue to thrive in the digital age.

Bibliography

Anderson, M., & Kumar, M. (2019, May 7). *Digital divide persists even as lower-income Americans make gains in tech adoption*. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/

Baptista, E. (2022, April 8). *China uses AI software to improve its surveillance capabilities*. Reuters. https://www.reuters.com/world/china/china-uses-ai-software-improve-its-surveillance-capabilities-2022-04-08/

Bartlett, J. (2018). *The people vs. tech: How the internet is killing democracy (and how we save it)*. Ebury Press.

Bastug, M., Douai, A., & Akca, D. (2020). Exploring the "demand side" of online radicalization: Evidence from the Canadian context. *Studies in Conflict & Terrorism, 43*(7), 616–637. https://doi.org/10.1080/1057610X.2018.1494409

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.

Bobba, G., Cremonesi, C., Mancosu, M., & Seddone, A. (2018). Populism and the gender gap: Comparing digital engagement with populist and non-populist Facebook pages in France, Italy, and Spain. *The International Journal of Press/Politics, 23*(1), 24–44.

Booth, R. (2025, January 8). *Meta to get rid of fact-checkers and recommend more political content*. The Guardian. https://www.theguardian.com/technology/2025/jan/07/meta-facebook-instagram-threads-mark-zuckerberg-remove-fact-checkers-recommend-political-content

Cadwalladr, C. (2018, March 18). 'I made Steve Bannon's psychological warfare tool': Meet the data war whistleblower. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. *Computers in Human Behavior, 97*, 202–215. https://doi.org/10.1016/j.chb.2019.03.032

Dawson, J. (2020). Microtargeting as information warfare. *The Cyber Defense Review, 6*(1). https://doi.org/10.31235/osf.io/5wzuq

Deng, I., & Chen, C. (2018, August 16). *The WeChat story: How Tencent's super-app changed China*. South China Morning Post. https://www.scmp.com/tech/article/2159831/how-wechat-became-chinas-everyday-mobile-app

Engesser, S., Fawzi, N., & Larsson, A. (2017). Populist online communication: Introduction to the special issue. *Information, Communication & Society, 20*(9), 1279–1292. https://doi.org/10.1080/1369118X.2017.1328525

European Commission. (2020). *Shaping Europe's digital future*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

European Commission. (2021, December 17). *Adequacy decisions*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

European Commission. (2015, May 6). *A digital single market for Europe: Commission sets out 16 initiatives to make it happen*. https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4919

European Commission. (2017, June 27). *Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison-shopping service*. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784

Fernandez, M. (2020, May 28). *Mark Zuckerberg: Social networks should not be "the arbiter of truth"*. Axios. https://www.axios.com/mark-zuckerberg-fact-check-twitter-facebook-0e3d9e92-00cd-4467-9ac8-bc50d4f8800e.html

Freelon, D., & Wells, C. (2020). Disinformation as political communication. *Political Communication, 37*(2), 145–156. https://doi.org/10.1080/10584609.2020.1723755

Frost, C. (2020). The power of voice: Bots, democracy, and the problem of political ventriloquism. *Journal of Political Power, 13*(1), 6–21.

Gaskell, A. (2019, September 23). *Is the Single Market preventing digital champions in Europe?* Forbes. https://www.forbes.com/sites/adigaskell/2019/09/20/is-the-single-market-preventing-digital-champions-in-europe/

Ghosh, D. (2021, January 14). *Are we entering a new era of social media regulation?* Harvard Business Review. https://hbr.org/2021/01/are-we-entering-a-new-era-of-social-media-regulation

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), 703–705. https://doi.org/10.2501/ijmr-2017-050

Goodman, M. P. (2020). *Time to align on digital governance*. CSIS. https://www.csis.org/analysis/time-align-digital-governance

Graham, M. H., & Svolik, M. W. (2020). Democracy in America? Partisanship, polarization, and the robustness of support for democracy in the United States. *American Political Science Review, 114*(2), 392–409. https://doi.org/10.1017/s0003055420000052

Guo, L., Rohde, J., & Wu, H. (2020). Who is responsible for Twitter's echo chamber problem? Evidence from 2016 U.S. election networks. *Information, Communication & Society, 23*(2), 234–251. https://doi.org/10.1080/1369118X.2018.1499793

Haldane, M. (2021, September). *What China's new data laws are and their impact on Big Tech*. South China Morning Post. https://www.scmp.com/tech/policy/article/3147040/what-chinas-new-data-laws-are-and-their-impact-big-tech

Kharpal, A. (2022, March 23). *Tencent 'exploring' a financial holding company for WeChat Pay if Chinese regulators require it*. CNBC. https://www.cnbc.com/2022/03/23/chinas-tencent-exploring-a-financial-holding-company-for-wechat-pay.html

Lange, E. (2020, November 23). *How one social media app is beating disinformation*. Foreign Policy.

Lee, J. (2022). *The connection of everything: China and the Internet of Things*. MERICS. https://merics.org/en/report/connection-everything-china-and-internet-things

Leparmentier, A. (2022, April 26). *Elon Musk's very political Twitter buyout sparks debate on freedom of speech*. Le Monde. https://www.lemonde.fr/en/economy/article/2022/04/26/elon-musk-s-very-political-twitter-buyout-sparks-debate-on-freedom-of-speech_5981665_19.html

Lewis, J. A. (2020, March 9). *Has Europe lost both the battle and war over its digital future?* Center for Strategic and International Studies. https://www.csis.org/analysis/has-europe-lost-both-battle-and-war-over-its-digital-future

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management, 22*(1), 1–6. https://doi.org/10.1080/1097198x.2019.1569186

Lilkov, D. (2020). Made in China: Tackling digital authoritarianism. *European View, 19*(1), 110. https://doi.org/10.1177/1781685820920121

Manville, B. (2019, September 8). *Will technology kill democracy—or reinvent it?* Forbes. https://www.forbes.com/sites/brookmanville/2019/09/08/will-technology-kill-democracyor--reinvent-it/?sh=534725d36a1b

Mărcuț, M. (2020). *The governance of digital policies: Towards a new competence in the European Union*. Springer International Publishing AG.

Marcus, J. S., Petropoulos, G., & Yeung, T. (2019, January). *Contribution to growth: The European Digital Single Market*. Bruegel. https://www.bruegel.org/wp-content/uploads/2019/02/IPOL_STU2019631044_EN.pdf

Mozur, P. (2020, September 4). *Forget TikTok. China's powerhouse app is WeChat, and its power is sweeping*. The New York Times. https://www.nytimes.com/2020/09/04/technology/wechat-china-united-states.html

Mozur, P. (2021, October 5). *The end of a 'gilded age': China is bringing business to heel*. The New York Times. https://www.nytimes.com/2021/10/05/business/china-businesses.html

Murray, M. (2021, May 9). *Poll: Nearly two-thirds of Americans say social media platforms are tearing us apart*. NBC News. https://www.nbcnews.com/politics/meet-the-press/poll-nearly-two-thirds-americans-say-social-media-platforms-are-n1266773

O'Connor, C., & Weatherall, J. O. (2019). The social media propaganda problem is worse than you think. *Issues in Science and Technology*, *36*(1). https://www.jstor.org/stable/10.2307/26949075

Pitt, J., Diaconescu, A., & Ober, J. (2018). Knowledge management for democratic governance of socio-technical systems. In *The future of digital democracy: An interdisciplinary approach* (pp. 123–138). Springer. https://doi.org/10.1007/978-3-030-05333-8

Pew Research Center. (2014, June 12). *Political polarization in the American public*. https://www.pewresearch.org/politics/2014/06/12/political-polarization-in-the-american-public/

Rainie, L., & Anderson, J. (2020, February 21). *Concerns about democracy in the digital age*. Pew Research Center. https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/

Rolfe, M. (2016). *The reinvention of populist rhetoric in the digital age: Insiders & outsiders in democratic politics*. Springer Singapore.

Rubin, O., Bruggeman, L., & Steakin, W. (2021, January 20). *QAnon emerges as recurring theme of criminal cases tied to US Capitol siege*. ABC News. https://abcnews.go.com/US/qanon-emerges-recurring-theme-criminal-cases-tied-us/story?id=75347445

Schmalz, S. (2024). Varieties of digital capitalism and the US–China rivalry: The rise of competing technological spheres. *Critical Sociology*. https://doi.org/10.1177/08969205241291645

Schneider, I. (2020). Democratic governance of digital platforms and artificial intelligence? *JeDEM - EJournal of eDemocracy and Open Government, 12*(1), 1–24. https://doi.org/10.29379/jedem.v12i1.604

Scola, N. (2020, July 3). *Inside the ad boycott that has Facebook on the defensive*. Politico. https://www.politico.com/news/magazine/2020/07/03/activists-advertising-boycott-facebook-348528

Scott, M. (2018, March 27). *Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower*. Politico. https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/

Scott, M. (2021, February 25). *Facebook's 'Supreme Court' to receive new powers*. Politico. https://www.politico.eu/article/facebook-supreme-court-thomas-hughes/

Stolton, S. (2022, March 25). *EU negotiators agree new rules to rein in tech giants*. Politico. https://www.politico.eu/article/eus-digital-markets-act-adopted/

Sunstein, C. R. (2000). Deliberative trouble? Why groups go to extremes. *The Yale Law Journal, 110*(1), 71–119. https://doi.org/10.2307/797587

Sunstein, C. R. (2021, January 17). *How government should regulate social media lies*. Bloomberg. https://www.bloomberg.com/opinion/articles/2021-01-17/first-amendment-can-t-stop-u-s-from-regulating-social-media-lies

Vogels, E., Perrin, A., & Anderson, M. (2020, August 19). *Most Americans think social media sites censor political viewpoints*. Pew Research Center. https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/

Walker, C. (2016). The authoritarian threat: The hijacking of "soft power." *Journal of Democracy, 27*(1), 49–63.

Wang, M. (2021, April 8). *China's techno-authoritarianism has gone global*. Foreign Affairs. https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global

Washington, J. (2025, January 9). *The TikTok ban is also about hiding pro-Palestinian content. Republicans said so themselves*. The Intercept. https://theintercept.com/2025/01/09/tiktok-ban-israel-palestine-republicans/

Wischmeyer, T. (2019). Making social media an instrument of democracy. *European Law Journal, 25*(2), 169–181. https://doi.org/10.1111/eulj.12312

Wood, A. (2015, March). *The internet of things is revolutionising our lives, but standards are a must*. The Guardian.

Yuan, L. (2021, July 19). *What China expects from businesses: Total surrender*. The New York Times. https://www.nytimes.com/2021/07/19/technology/what-china-expects-from-businesses-total-surrender.html

Yuan, L. (2023, February 17). *Why China didn't invent ChatGPT*. The New York Times. https://www.nytimes.com/2023/02/17/business/china-chatgpt-microsoft-openai.html

Yuan, L. (2022, January 5). *As Beijing takes control, Chinese tech companies lose jobs and hope*. The New York Times. https://www.nytimes.com/2022/01/05/technology/china-tech-internet-crackdown-layoffs.html

Zuboff, S. (2020). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.