

Article

After TikTok: International Business and the Splinternet

Maximilian Stallkamp¹  ^a

¹ Virginia Tech, USA

Keywords: global strategy, digitalization, internationalization, digital firms, internet

<https://doi.org/10.46697/001c.21943>

AIB Insights

Vol. 21, Issue 2, 2021

The internet is evolving from a globally connected and lightly regulated network to a ‘splinternet’ governed by diverging national policies. Governments are effectively re-creating national borders in digital space by asserting their authority over areas such as data protection, taxation, censorship, and national security. This increasing fragmentation of the internet creates new challenges for companies that use the internet to offer digital products and services (such as apps) internationally. Rather than addressing global markets more or less by default, these digital firms must make strategic choices with respect to foreign market selection, entry modes, local adaptation, and stakeholder management.

“The era of a global Internet may be passing. Governments across the world are putting up barriers to the free flow of information across borders” (Chander & Lê, 2014)

INTRODUCTION

TikTok, a mobile app for sharing short videos, appeared to be a global success story for its Beijing-based parent company ByteDance, and a prime example of internet-based internationalization. In little over two years, the app picked up hundreds of millions of users worldwide, with nearly 100 million in the United States alone (Sherman, 2020). However, in July 2020, the US government announced plans to ban the app from the American market, citing national security concerns due to potential Chinese government influence over ByteDance. TikTok, previously the poster child for the seemingly boundless global business opportunities of the digital economy, suddenly became a cautionary tale illustrating the re-emergence of national borders in the digital economy. Over the past decade, governments around the world have increasingly asserted their sovereignty over the digital domain, imposing local laws and regulations on digital transactions. This accelerating trend is replacing the open, lightly regulated, and globally connected internet with a fragmented digital reality – often referred to as the splinternet (Lemley, 2020). In this article, I review the main forces driving this fragmentation and discuss the major consequences for the international strategies of digital firms, i.e., firms selling purely digital products. As the importance of the digital economy continues to grow, it is crucial for practitioners and scholars of international business to understand the changing nature of the internet and its implications for business.

THE EARLY INTERNET AND INTERNATIONAL BUSINESS

The early internet, as a decentralized and globally connected network, seemed to be inherently location-agnostic and borderless. Many internet pioneers subscribed to Barlow’s (1996) famous Declaration of the Independence of Cyberspace, which argued that governments did not have the right – nor the technical ability – to enforce their national laws on the internet, proclaiming that “cyberspace does not lie within your borders”. In hindsight, Barlow’s views might charitably be described as idealistic. And yet, with the exception of China and a handful of authoritarian countries, the early internet and the emerging digital economy were mostly characterized by a *laissez-faire* attitude among regulators (Hill, 2014). As late as 2013, former Google CEO Eric Schmidt called the internet “the world’s largest ungoverned space” and “an online world that is not truly bound by terrestrial laws” (Schmidt & Cohen, 2013: p.1).

Digital firms benefitted greatly from this open, global internet. Digital products and services – such as apps, games, and social media platforms – could be distributed remotely over the internet, giving companies instant access to potential users around the world (with the exception of China and a few other countries). By serving foreign markets virtually from a distance, digital firms could avoid or postpone costly foreign direct investments, which allowed even small startups to internationalize rapidly (Monaghan, Tippmann, & Coviello, 2020). As many regulators and tax authorities were unprepared to handle intangible digital services and unfamiliar digital business models, digital firms were often able to extend their user base in foreign markets with little regard to local rules.

^a Contact: mstallkamp@vt.edu

This is not to say that internationalization became trivial or inevitable. For many digital firms, issues such as cultural differences, customer preferences, and different languages remained formidable market entry barriers (Shaheer, 2020). However, the open nature of the internet at least allowed digital firms to make their products globally available at minimal costs, which represented a major departure from traditional international business.

SPLINTERNET: THE FRAGMENTATION OF THE INTERNET

Over the past decade, there has been a sharp increase in regulation of the internet, especially with respect to cross-border digital transactions (US International Trade Commission, 2017). By insisting that digital firms follow local rules and respect national policies, governments are effectively restoring the role of national borders in the digital economy. While there are many different motivations for such restrictive measures, four broad concerns account for a large proportion of digital fragmentation: Privacy/data protection, taxation, censorship, and national security.

PRIVACY AND DATA PROTECTION

Most digital firms collect vast amounts of data on their users. In response, privacy concerns are growing around the world, especially after revelations of rampant state and private espionage, such as the Snowden and Cambridge Analytica scandals (Hill, 2014). Over 120 jurisdictions have now passed legislation governing data protection and the digital privacy rights of their citizens (Congressional Research Congressional Research Service, 2019). The most influential example is the European Union's 2018 General Data Protection Regulation (GDPR), which grants extensive privacy rights and imposes stringent obligations on companies to safeguard data (Kaelin, 2019). There has also been a surge in data localization laws, which restrict cross-border data flows and require certain data be stored on domestic servers (Chander & Lê, 2014). Data protection and localization regulations are not necessarily discriminatory against foreign companies, as they apply to domestic and foreign companies alike. However, much like regulatory non-tariff barriers in conventional trade, they create entry barriers and increase costs for foreign companies, which now face a complex array of different host-country regulations (US International Trade Commission, 2017).

TAXATION

The growth of the digital economy has fueled concerns about the ability of governments to effectively tax digital transactions, as their intangible nature facilitates tax avoidance (Ting & Gray, 2019). However, facing budget shortfalls and public pressure, governments are intensifying efforts to tax digital transactions. While multilateral proposals under the auspices of the OECD, the EU, and the G20 made little headway, 38 countries had implemented or announced their own national digital taxes by early 2021 (KPMG, 2021). For example, Britain imposed a tax on revenues generated from digital services attributable to British users. It is levied on

revenues, rather than profits, to reduce tax avoidance. Like data protection rules, taxation of digital services is not inherently discriminatory against foreign companies, but the development of a nation-based patchwork of digital taxes introduces substantial uncertainty and compliance costs for digital firms seeking to offer their services internationally.

CENSORSHIP

One of the defining features of the early internet was the free flow of information. Any content posted to the web could be accessed by internet users anywhere. This is no longer the case, as governments increasingly restrict which content is accessible and which digital apps are available from within their national territory. The most well-known censorship scheme is the Chinese Great Firewall, which not only blocks many foreign-owned digital services but leverages advanced surveillance technologies to remove sensitive content. Although determined individuals may find ways to circumvent digital censorship, the Chinese approach is generally effective and has prompted similar initiatives in other countries. While content filtering and restrictions on foreign apps were initially mostly used by authoritarian governments (Hill, 2014), many democratic countries now debate to what extent objectionable or harmful content (e.g., extremism, misinformation) should be suppressed. As more countries wall off 'their' internet and impose restrictions on content, users located in different parts of the world increasingly see different versions of the internet. For companies producing digital content, products, and services, this creates new barriers to serving foreign markets.

NATIONAL SECURITY AND GEOPOLITICS

As the TikTok example shows, some government interventions are motivated by national security. Given the extensive data collected by many software applications and the far-reaching influence of social media, governments are justifiably concerned about foreign espionage and the ability of foreign powers to exert political influence. Responses range from targeted measures designed to protect domestic data to wholesale bans of foreign apps and services. Moreover, governments may block foreign apps as a tactical maneuver in broader geopolitical disputes, as was reportedly the case with India's ban in September 2020 of over 100 Chinese apps (Kastrenakis, 2020). As governments are beginning to view the digital economy through the lens of national security and geopolitics, digital firms are increasingly exposed to political risks.

OTHER POLICY OBJECTIVES

Many other social and economic considerations can motivate policies contributing to digital fragmentation. For example, governments routinely impose sector-specific regulations on industries such as gambling, finance, or healthcare. Moreover, the official policy objective may serve as a disguise for protectionist measures designed to shield domestic companies from foreign competition.

WHAT DOES ALL THIS MEAN FOR DIGITAL FIRMS?

The internet is undergoing an important shift from largely ‘ungoverned space’ to a patchwork of regulations that reflect the diverse policy priorities of different countries and regions. This digital fragmentation or ‘splinternet’ poses new challenges for digital firms operating internationally. Below, I discuss four major business implications, summarized in [Figure 1](#).

1. MORE LOCAL ADAPTATION

A central concept in international business is the tension between global standardization and local adaptation. Global standardization, i.e., offering the same product in all markets, minimizes complexity and reduces costs. This strategy is especially attractive for digital firms because digital products generally exhibit economies of scale (once developed, they can serve any number of users at minimal marginal cost). However, the fragmentation of the internet forces firms to adapt their products for different countries, limiting their ability to reap the benefits of standardization. To meet legal obligations and social expectations in foreign markets, digital firms often need revise not just consumer-facing aspects of their products (e.g., content, user interfaces) but also back-end processes and business models, for example with respect to data collection, storage, and monetization. The cost of complying with foreign regulations such as GDPR can amount to millions of dollars per company (PWC, 2018). In addition to one-off adaptation costs, the need for ongoing monitoring of evolving legal frameworks in multiple countries adds to the cost (monetary and in terms of management attention) of operating internationally, which can impose a substantial burden on smaller startups.

2. SELECTIVE ENTRY

With the renewed salience of national borders and improved technologies for pinpointing the locations of users, it can no longer be assumed that digital products are globally available by default. On one hand, governments can block access to digital services, as threatened in the case of TikTok. On the other hand, companies themselves can choose not to make their digital products available in certain geographies for strategic reasons. If the compliance costs of operating in a country are deemed too onerous, companies may prefer to avoid (or postpone) market entry. For example, when the GDPR came into effect in 2018, Europeans found that many non-European news websites were suddenly no longer accessible – rather than comply with GDPR, several large news organizations instead blocked their content in the EU. The move towards smartphones and tightly controlled app stores (Hestres, 2013) has given digital firms the tools to actively manage the geographic distribution of digital products. As a result, digital firms can and should make deliberate strategic choices about which markets to enter, and which ones to avoid.

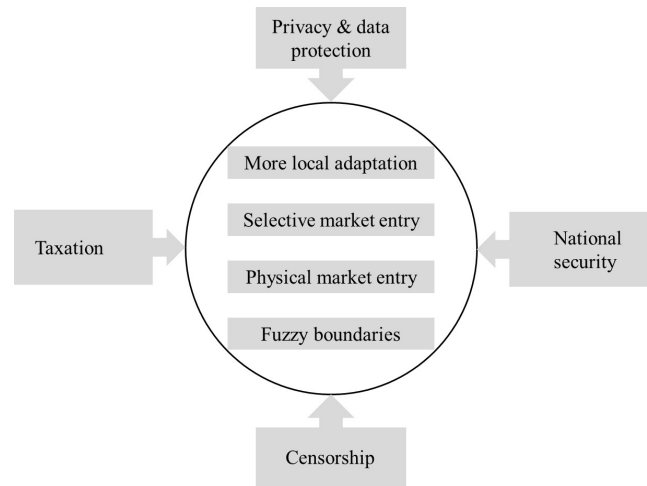


Figure 1: Forces Driving Digital Fragmentation and International Business Implications for Digital Firms

3. PHYSICAL ENTRY INTO FOREIGN MARKETS

One of the unique attributes of digital firms is their ability – at least in principle – to serve foreign markets virtually from a distance, simply by making their digital products available over the internet. However, digital firms face growing pressure to establish a physical presence in at least some of their markets. Local data centers may be required to comply with localization laws, while stakeholder relations teams need to be on the ground to effectively manage regulatory and political risks. Social media companies like Facebook and TikTok employ large numbers of local content moderators to filter out offensive or censored content. Moreover, alliances and joint ventures between foreign and local companies are becoming increasingly important, as digital firms seek local partners to help them navigate complex foreign markets. In sum, the splinternet is forcing many digital firms to think beyond purely virtual market entry modes.

4. MANAGING FUZZY BOUNDARIES

Despite increasing digital fragmentation, it would be a mistake to treat countries as if they were completely independent. Information eventually spreads around the world through digital and other channels. This creates additional challenges for digital firms as they must navigate diverging regulations and social expectations in multiple countries, without alienating stakeholders elsewhere. For example, the communication platform Zoom became the target of international criticism for complying with Chinese censorship requests, both inside and *outside* of China (Mozur, 2020). Conflicting laws with respect to free speech, privacy rights and the banning of objectionable content will inevitably lead to disputes. This is further complicated by disagreements over the territorial reach of many internet-related regulations: Can a French regulator force Google to remove a search result from the non-French versions of its search engine? Can authoritarian governments enforce censorship

outside of their national borders? Digital firms operating internationally will face intense scrutiny and will need to manage these tensions carefully.

CONCLUSIONS: LIVING WITH THE SPLINTERNET

The trend towards digital fragmentation is unlikely to be reversed anytime soon. As societies, economies, and businesses increasingly depend on digital technologies, it is unsurprising – and necessary – that governments take a more active role in regulating the digital domain and enforcing national policies. The diversity of political systems, policy priorities, and cultural values across countries means that rules will differ from place to place. As with any international business transaction, this tends to generate friction in the cross-border flow of digital products and services. Multilateral agreements, such as OECD efforts to harmonize taxation, could help limit such frictions, but are notoriously difficult to negotiate. Regional solutions, such as the digital provisions of the new North American USMCA trade agreement, may prove easier to implement but still contribute to region-based fragmentation and the emergence of digital trade blocs. It is possible that national or regional rules (such as GDPR) could become de-facto global standards, which would facilitate the international operations of digital firms.

In the meantime, however, digital fragmentation will continue to increase the cost, complexity, and risk of entering and operating in foreign countries. This adds to various competitive challenges related to user adoption and monetization faced by digital firms in foreign markets (Shaheer, 2020; Verbeke & Hutzschenreuter, 2020). Consequently, there is an urgent need for practitioners and scholars of international business to think more strategically about the international expansion of digital firms. In the early stages of digitalization, there was a tendency to view digital firms

as operating in a borderless ‘digital space’ and competing globally by default. Many international business challenges and practices from the brick-and-mortar era began to appear antiquated. Today, it is becoming increasingly apparent that many of these traditional international business issues – market selection, entry modes, local adaptation, trade barriers, bargaining with host-country governments, to name a few – remain highly pertinent for digital firms. Fortunately, a wealth of international business theories, strategies, and analytical tools has been developed to address these issues. The challenge for international business practitioners – and scholars – is to apply these tools to the digital context and, where necessary, adapt or reinvent them.

ACKNOWLEDGMENTS

I thank Dr. Newburry and the anonymous reviewers for their constructive comments. I also thank Sali Li for his feedback on an early draft of this manuscript.

ABOUT THE AUTHOR

Max Stallkamp is an Assistant Professor of Management at Virginia Tech. He received his PhD from the Ivey Business School at Western University, Canada. His research examines the internationalization of firms, with an emphasis on digital and technology ventures, and has been published in the *Journal of International Business Studies*, *Global Strategy Journal*, and the *Journal of Management Studies*.

Submitted: September 20, 2020 EDT, Accepted: March 24, 2021 EDT



This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CCBY-4.0). View this license's legal deed at <http://creativecommons.org/licenses/by/4.0> and legal code at <http://creativecommons.org/licenses/by/4.0/legalcode> for more information.

REFERENCES

- Barlow, J. P. 1996. *Declaration of the independence of cyberspace*. Electronic Frontier Foundation. <https://www.eff.org/cyberspace-independence>.
- Chander, A., & Lê, U. P. 2014. Data nationalism. *Emory Law Journal*, 64: 677–739.
- Congressional Research Service. 2019. *Digital Trade and U.S. Trade Policy. Report #44565*. <https://crsreports.congress.gov/product/pdf/R/R44565>.
- Hestres, L. E. 2013. App neutrality: Apple's app store and freedom of expression online. *International Journal of Communication*, 7: 1265–1280.
- Hill, J. F. 2014. *The growth of data localization post-Snowden: Analysis and recommendations for US policymakers and business leaders*. The Hague Institute for Global Justice, Conference on the Future of Cyber Governance. <https://doi.org/10.2139/ssrn.2430275>.
- Kaelin, M. 2019. GDPR: A cheat sheet. *Tech Republic*. <https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/>.
- Kastrenakis, J. 2020, September 2. India bans PUBG Mobile, Alipay, Baidu, and more Chinese apps. *The Verge*. <https://www.theverge.com/2020/9/2/21418120/pubg-mobile-india-ban-118-apps-china-alipay-baidu>.
- KPMG. 2021. *Taxation of the digital economy: Developments summary*. <https://tax.kpmg.us/content/dam/tax/en/pdfs/2020/digitalized-economy-taxation-developments-summary.pdf>.
- Lemley, M. A. 2020. The Splinternet. *Stanford Law and Economics Olin Working Paper #555*. <https://doi.org/10.2139/ssrn.3664027>.
- Monaghan, S., Tippmann, E., & Coviello, N. 2020. Born digitals: Thoughts on their internationalization and a research agenda. *Journal of International Business Studies*, 51(1): 11–22.
- Mozur, P. 2020, June 11. Zoom blocks activist in U.S. after China objects to Tiananmen vigil. *New York Times*. <https://www.nytimes.com/2020/06/11/technology/zoom-china-tiananmen-square.html>.
- PWC. 2018. *Pulse Survey: US Companies ramping up General Data Protection Regulation (GDPR) budgets*.
- Schmidt, E., & Cohen, J. 2013. *The new digital age: Transforming nations, businesses, and our lives*. Knopf Doubleday Publishing Group.
- Shaheer, N. A. 2020. Reappraising International Business in a Digital Arena: Barriers, Strategies, and Context for Digital Internationalization. *AIB Insights*, 20(4). <https://doi.org/10.46697/001c.17849>.
- Sherman, A. 2020, August 24. TikTok reveals detailed user numbers for the first time. *CNBC*. <https://www.cnn.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html>.
- Ting, A., & Gray, S. J. 2019. The rise of the digital economy: Rethinking the taxation of multinational enterprises. *Journal of International Business Studies*, 50(9): 1656–1667.
- US International Trade Commission. 2017. *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions. Publication Number: 4716*. https://www.usitc.gov/publications/industry_economic_analysis_332/2017/global_digital_trade_1_market_opportunities_and.htm.
- Verbeke, A., & Hutzschenreuter, T. 2020. The Dark Side of Digital Globalization. *Academy of Management Perspectives*. <https://doi.org/10.5465/amp.2020.0015>.