INNOVATION ▼▲ FREEDOM ▼▲ PROSPERITY

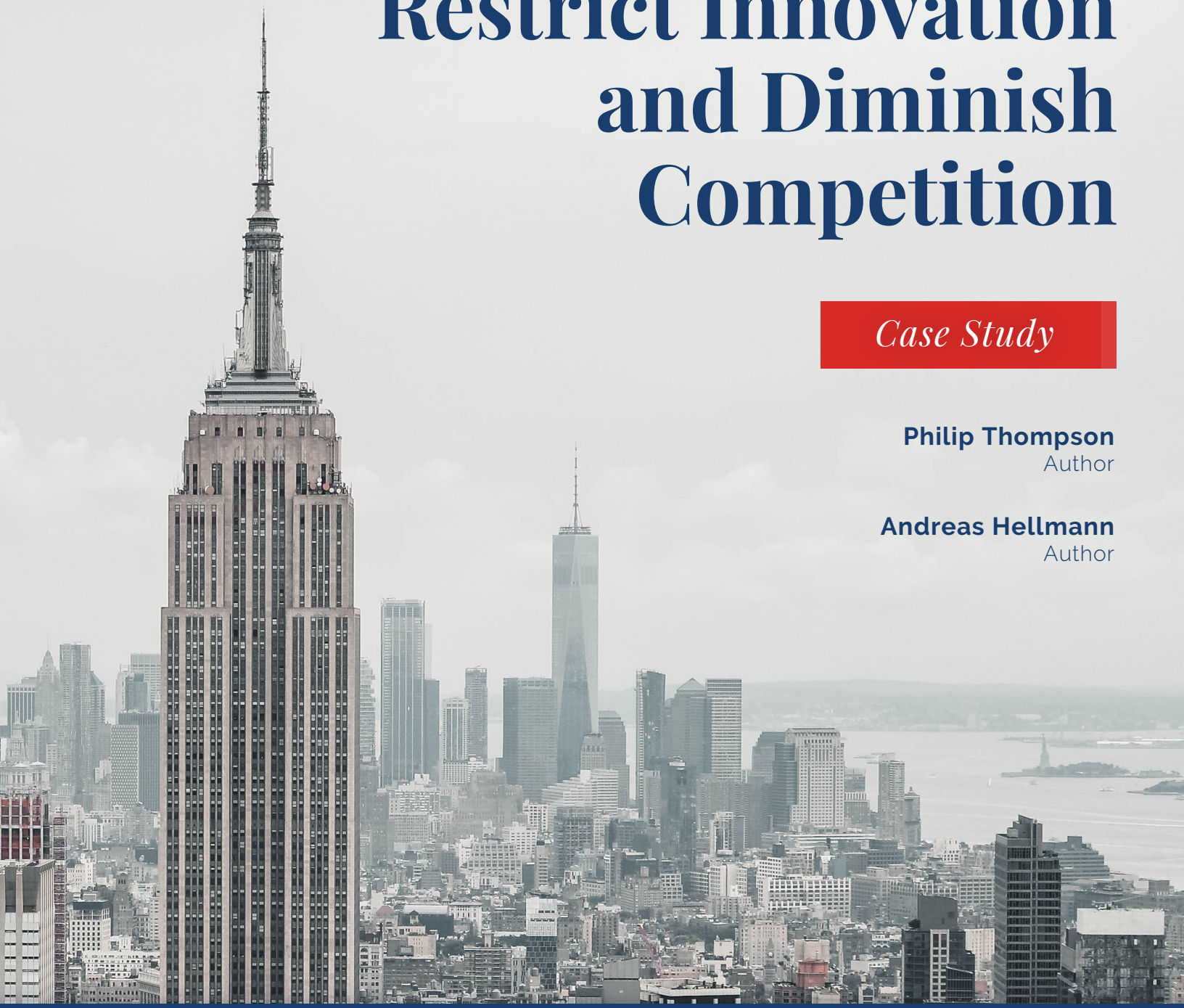
International Trade Barrier Index 2023

EU Protectionist Digital Trade Barriers Restrict Innovation and Diminish Competition

Case Study

Philip Thompson
Author

Andreas Hellmann
Author



THOLOS
FOUNDATION

In the past decade, the European Union (EU) has pioneered restrictive regulations on the flow of data across borders as well as the larger digital economy in an attempt to tame a new industry considered to be unregulated and escaping from oversight. In doing so, the EU has passed what has become model legislation for data protection and digital taxes while jeopardizing data flows with its largest trade partner and inviting a potential tariff war for its discrimination. The latest EU digital regulations such as the Digital Markets Act and cloud certification schemes go further by restricting free expression and prohibiting foreign competition. These new rules governing digital competition will increase the regulatory burden imposed on the targeted companies and pose great danger to innovation, competition and the digital economy as we know it.

As French President, Emmanuel Macron, returns from a recent trip to China, his comments that Europe should be a "third pole," or another unaligned country between the United States (U.S.) and China, caught many leaders in European capitals and Washington, D.C. off guard. Yet, in the tech space this position should be of no surprise. In her first speech as incoming European Commission President, Ursula von der Leyen called for EU "technological sovereignty." Then, in a later op-ed, she identified "quantum computing, 5G, cybersecurity or artificial intelligence" as areas ripe for "strategic investment" from the private and public sector in order to provide "the same opportunities as their counterparts in Silicon Valley."

The statement nearly mirrors the state-driven industrial strategy pursued by the Chinese Communist Party (CCP) which announced its Made in China 2025 that identifies 10 areas of high-end manufacturing it seeks to develop in order to remain a "leading manufacturing power by the year 2049." The China plan includes similar goals of high-end chip production, computing, artificial intelligence, and electric vehicles.

As Europe's technological sovereignty agenda unfolds, it is clear the process is different from China's; it is more democratically driven and focused on preserving privacy rights, yet the outcome is remarkable similar. Both highly restrict market access and limit the competition models followed by American tech firms. The data found under the digital trade restrictions component of the 2023 Trade Barrier Index confirms as much.

China's great firewall is well known all over the world; the Golden Shield Project moderates online content critical of the government as well as "false ideals and thoughts." Nearly every American search engine and social media platform is blocked in China: Google, Facebook, WhatsApp, Twitter, Discord, Reddit, and Wikipedia to name a few. Also banned are nearly every mainstream media news site: The New York Times, The Wall Street Journal, The Economist, The Washington Post, the BBC, etc…

While this type of extreme restriction of speech, free-expression and information might seem absolutely incompatible with values expounded by leaders in Europe and America. Nevertheless, the laws in China that set the legal framework for the Great Wall are not too different from those under consideration in the EU and the United States today. The first regulation, issued in 1997, forbid internet use from inciting unrest, inciting overthrow of the government, making falsehoods or distorting the truth, inciting terrorism, and messages injuring state organs and reputations to name a few restrictions.

In 2023 the United States, for instance, saw more than 100 laws in the federal and state governments with the aim of some form of content moderation for "fake news," not that different from the acts China forbids. The bills can be categorized in several ways. Some targeted politicians and forbid social media platforms from censoring their content, others focused on the privacy rights of children, and others join a growing trend in Europe that would restrict platforms from hosting content that was harmful but not illegal. The category of "harmful" can include anything from incitement content to disparagement of political institutions. Many of these bills proposed expanding the scope of existing telecom regulations to include internet platforms such as SB 2161 in Tennessee. That law would have social media platforms register with the public utilities commission which would have the power to investigate and fine a company for violating the content moderation rules.

Fortunately, only two such laws passed at the state level: Florida and Texas. And none passed at the federal level. Speech online in the United States is heavily protected by the first amendment, the right to free speech, and Section 230 of the Communication Decency Act which limits the liability of internet platforms when users post content that may be illegal or harmful. The laws that passed in Florida and Texas are currently being challenged at the Supreme Court for violating Section 230.

By expanding the scope of existing telecom regulation, the Tennessee law joined Australia, the European Union, India, and South Korea which have followed, or have proposals to follow, the same strategy. These states seek to leverage the authority of an agency already tasked with basic consumer protections such as data, privacy, and price transparency. However, the business models of traditional telecom operators, namely cellular networks and broadcast networks, is remarkably different from online platforms and cloud services. Treating these networks in the same way does not equate to a level playing field and may create more unintended consequences.

It is also similar to other regulations from China, such as State Council Order No. 292, the Cyber Security Law, the Cyberspace Administration of China, and the Data Security Law which force entities handling specified forms of data to be licensed or registered with a state agency. The agency then obligates the entity to maintain their registration by following guidelines that overtime have contributed to several layers of the Chinese firewall. Today, due to these regulations, only licensed websites can broadcast news and approved firms with "critical infrastructure" can store, process, and transfer certain information overseas. As a result, the Chinese Communist Party is in complete control of speech online, how online businesses operate, and the CCP determines which agencies can store, process, and transfer data.

This brings us to Europe, which has historically been an advocate for open trade and the free flow of data across borders. Two famous hiccups in this cross-Atlantic relationship have been the passing of the General Data Protection Legislation (GDPR) and the Max Schrems cases at the European Union Court of Justice, which invalidated the Safe Harbor mechanism and, later, the EU-US Privacy Shield, which were the primary data transfer mechanisms for the safe and free flow of data between the EU and U.S. In short, the GDPR mandated that data associated with EU citizens can flow freely only to countries with similar adequate safeguards as the EU or via Standard Contractual Clauses. These decisions jeopardized nearly $7 trillion in trade between the close trade partners. With the implementation of the 2022 European Union U.S. Data Privacy Framework, the U.S. should earn a new adequacy decision in early 2023. Despite the focus on the privacy rights of EU citizens propelling the litigation against the mechanisms allowing data flows between the EU and U.S., the EU has not scrutinized the mechanisms permitting EU data flows with other countries, such as China.

Rather than a re-start with a clean slate provided by the new privacy framework, the EU is introducing a next chapter of regulations defining "digital sovereignty" targeting U.S. tech firms and cross border data flows to them. The Trade Barrier Index identifies the Digital Markets Act, the Digital Services Act, The AI Act, the Digital Operators Resilience Act, the Foreign Subsidies Regulation, the Data Act, schemes such as Sending Party Network Pays taxes to fund ISPs, digital services taxes (DST), and a very troubling Cybersecurity Certification Scheme for Cloud Services. Late breaking, after data was compiled for the data restrictions component of the TBI, a leaked plan was released to regulate prices for Standard Essential Patents and limit enforcement.

This list of discriminatory digital restrictions by no means is a complete record of the cross-Atlantic tech tensions. For instance, the EU is pursuing several antitrust cases against American tech firms and the U.S. passed Inflation Reduction Act are on separate paths of conflict.

Many of these regulations break with established competition law and other norms. For instance, the Foreign Subsidies Regulation (FSR) grants the Commission exclusive competence to initiate investigations into any company for any reason if they suspect the entity benefits from unfair subsidies directly or indirectly in the EU or outside the EU. The investigation can take into account proprietary technology, specialized staff, know-how, and patents. Finally, acting as judge, jury, and executioner if the Commission determines a subsidy may indeed be negatively affecting the market, there isn't a limit to how it can redress the situation. The FSR suggests a few measures: a fine based on global revenue, repaying the subsidy, providing access to infrastructure, granting licenses, divestment of assets, and reducing market presence.

The Digital Markets Act (DMA) and Digital Services Act (DSA) also break with competition law norms. They create a new class of businesses called Very Large Online Platforms (VLOPs) in the DSA and "gatekeepers" in the DMA; virtually all are American. The measures subject these service providers to transparency reporting, including audits, and disclosing their recommendation algorithm. The DSA increases liability and adopts a similarly broad censorship standard found in Chinese-style content moderation rules. It requires VLOPs to restrict harmful but not illegal content. The DSA is so restrictive, one of its first uses could be removing Twitter from the EU market.14 If so, it would join an exclusive club whose members include China, Russia, Iran, Turkmenistan, Uzbekistan, North Korea, and at times India and Nigeria.

The Digital Markets Act will be enforced through a European supervisory architecture, under which the European Commission will be the sole enforcer of those rules, in close cooperation with authorities in European Union Member States. The European Commission will be able to impose penalties and fines of up to 10% of a company's worldwide turnover, and up to 20% in case of repeated infringements. In the case of systematic infringements, the European Commission will also be able to impose behavioral or structural remedies necessary to ensure the effectiveness of the obligations, including a ban on further acquisitions.

Another regulation quickly advancing in Europe is the EU's Cybersecurity Certification Scheme for Cloud Services (EUCS). The draft proposal includes data localization provisions and, for the certification of "high assurance level," it includes content localization and employee nationalization requirements. This would include an obligation for customer service employees and cloud services providers to be operated by companies and people based in the EU, and who do not have a controlling stake by foreign firms. This would be a huge break from established norms, including those set by the EU with GDPR. This requirement would very likely run afoul of World Trade Organization (WTO) national treatment obligations. In the past the EU had joined the U.S. in advocating that due to the technological advancements of cloud services, the physical place of data storage and processing was negligible; the standards, certifications, encryption measures, and the due process of law used by cloud services were enough to ensure data handling were in compliance with domestic regulations.

With these regulations in mind, the blueprint is in place. Europe may not be banning American online platforms or greatly restricting their ability to process and transfer data today. However, these set the legal framework to fine, restrict, and ban platforms tomorrow in the name of digital sovereignty. This agenda even comes with similar subsidies, restrictions of online speech, and industrial goals as China's industrial strategy. Far from preserving human rights, propelling innovation, or keeping critical infrastructure safe, these policies send the opposite message. Rather than encourage tech start-ups to enter the market with a dream and entrepreneurial mind set, they must first consider compliance with the goals of the administrative state.

THOLOS

FOUNDATION

TRADEBARRIERINDEX.ORG