The Splinternet's Shadow: Intellectual Property and Innovation in an Era of Ascendant Digital Sovereignty

Cybel N. Ekpa
Washington University of Science and Technology, Virginia, United States of America

***Abstract*—The intersection of digital sovereignty and intellectual property rights presents a formidable challenge to the global technology landscape. As nations assert sovereign control over data, digital infrastructure, and online ecosystems, established intellectual property frameworks face significant strain. This paper examines the tension between national digital sovereignty initiatives and the inherently global nature of innovation. Through a comparative analysis of legal and policy frameworks in the European Union, the United States, China, and India, it identifies key areas of conflict, including data localization mandates, technology transfer requirements, the fragmentation of patent regimes, and jurisdictional disputes. While digital sovereignty measures are often enacted to protect national security and citizen privacy, they risk creating barriers to innovation, increasing compliance costs, and fragmenting global technology markets. This paper proposes a framework for balanced governance that respects national sovereignty while preserving the collaborative ecosystem essential for technological advancement. This framework emphasizes harmonized standards, reciprocal international agreements, and flexible regulatory mechanisms capable of adapting to rapid technological change. The future of global technology markets may depend on developing new models of governance that reconcile legitimate national interests with the transnational cooperation required for sustained innovation and economic development.**

I. INTRODUCTION

The digitalization of the global economy has fundamentally altered the application of sovereignty in the 21st century. Traditional notions of territorial sovereignty, predicated on physical borders and tangible assets, are ill-suited to address the borderless nature of digital technologies, data flows, and intellectual property.[4] In response, the concept of digital sovereignty, the principle that a state possesses the authority to govern the digital infrastructure, data, and technological systems within its jurisdiction, has emerged as a central policy framework worldwide.[5] Concurrently, intellectual property (IP) rights remain a primary legal mechanism for incentivizing innovation by protecting creators and inventors while facilitating the dissemination of knowledge.[6]

The convergence of these two paradigms creates significant challenges for global technology markets. States increasingly implement digital sovereignty measures to protect national security, ensure citizen privacy, and maintain economic competitiveness.[7] However, the cumulative and collaborative nature of modern innovation depends on the cross-border flow of ideas, data, and protected intellectual property.[8] This tension is manifest in several policy domains: data localization laws mandating the domestic storage of citizen data, technology transfer requirements that condition market access on the disclosure of proprietary information, divergent patent regimes that fragment global innovation systems, and regulatory barriers that increase compliance costs and impede technological deployment.[9]

The economic and geopolitical stakes are substantial. The increasing fragmentation of digital markets through sovereignty-driven regulations threatens to balkanize the internet, create incompatible technology ecosystems, and slow the pace of global innovation. This paper provides a comprehensive legal and policy analysis of the interplay between digital sovereignty and intellectual property. It examines how different jurisdictions balance these competing interests, analyzes the economic and innovation impacts of various regulatory approaches, and proposes frameworks for achieving equilibrium between legitimate sovereignty concerns and the global collaboration necessary for continued technological progress.

II. DIGITAL SOVEREIGNTY: CONCEPT AND EVOLUTION

Defining Digital Sovereignty

Digital sovereignty extends the traditional legal concept of state sovereignty into the digital realm, asserting a nation's right to govern digital activities, data flows, technology infrastructure, and cybersecurity within its territory.[10] The application of this concept, however, varies significantly across jurisdictions, reflecting divergent political systems, economic priorities, and legal traditions.

In the European Union, digital sovereignty is primarily framed through the lens of fundamental rights, data protection, and ethical technology governance, as embodied in the General Data Protection Regulation (GDPR).[11] The European approach seeks to establish a regulatory model that prioritizes citizen rights while maintaining an open market. The GDPR's extraterritorial scope demonstrates the EU's objective of setting global standards for digital governance, a phenomenon often described as the "Brussels Effect."[12]

The United States has traditionally favored market-driven policies and the principle of free data flow, viewing digital openness as critical to the global competitiveness of its technology sector.[13] However, increasing concerns over national security, particularly regarding foreign surveillance and technological competition, have led to targeted restrictions on technology transfers and data access involving foreign adversaries.[14]

China's interpretation of digital sovereignty emphasizes cybersecurity, technological self-sufficiency, and state control over its domestic digital ecosystem. Foundational laws such as the Cybersecurity Law of 2017 provide a comprehensive framework for government oversight of digital activities, mandating data localization and granting state authorities broad access to information.[15] This strategy explicitly links technological independence with national security and political stability.

In India, digital governance policy combines elements of different approaches. Initiatives to promote digital infrastructure development are paired with data protection and localization requirements aimed at building domestic technological capabilities, as codified in the Digital Personal Data Protection Act of 2023.[16] India's approach reflects its ambition to become a leading technology power while safeguarding the digital rights of its large population.

Historical Development

The concept of digital sovereignty evolved as the internet's transformative impact on traditional state functions became apparent. Early internet governance models, such as the multi-stakeholder framework embodied by the Internet Corporation for Assigned Names and Numbers (ICANN), emphasized technical coordination over direct governmental control, reflecting an ideal of a borderless cyberspace.[17] This consensus began to erode as nations recognized the strategic importance of digital technologies. The 2013 disclosures of widespread state surveillance programs catalyzed a global reassessment of digital governance, prompting many countries to implement measures to assert greater digital autonomy.[18]

The subsequent decade witnessed a proliferation of digital sovereignty initiatives. The GDPR, implemented in 2018, established a new global benchmark for data protection. Other nations followed with similar legislative frameworks, including Brazil's *Lei Geral de Proteção de Dados* (LGPD).[19] During this period, China solidified its state-centric model of digital governance and accelerated efforts toward technological self-reliance, while other nations enacted data localization and cybersecurity laws. The COVID-19 pandemic further accelerated these trends, as increased reliance on digital services and supply chain disruptions highlighted the strategic importance of domestic digital infrastructure and technological capacity.

III. INTELLECTUAL PROPERTY IN THE DIGITAL AGE

IP Frameworks and Global Innovation

Intellectual property rights are designed to incentivize innovation by granting creators limited exclusive rights over their inventions and creative works. The global IP system, administered primarily through the World Intellectual Property Organization (WIPO) and governed by multilateral treaties such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), aims to harmonize minimum standards of protection while permitting national variations.[20]

The primary forms of IP include patents, which protect novel inventions; copyrights, which protect original works of authorship; trademarks, which protect brand identity; and trade secrets, which safeguard confidential business information.[21] This system, developed over centuries, has adapted to successive technological revolutions. However, digital technologies present unique challenges to these traditional IP frameworks. Software, for example, possesses both functional and expressive characteristics, creating ambiguity between patent and copyright protection.[22] Artificial intelligence (AI) systems can now generate creative works and inventions, raising complex questions of authorship and ownership under existing law.[23] Furthermore, the ability to replicate digital goods at virtually no cost undermines traditional economic models based on scarcity.

The global and collaborative nature of digital innovation adds further complexity. A single digital product may incorporate code from developers across multiple jurisdictions and rely on open-source components, challenging territorial IP systems designed for tangible goods.[24]

IP and Competitive Advantage

In a knowledge-based global economy, intellectual property is a central element of competitive advantage. The market value of leading technology corporations is largely derived from intangible assets, including extensive patent and trademark portfolios. IP licensing generates significant revenue streams and is crucial for establishing technical standards and ensuring interoperability.

Consequently, nations increasingly view the promotion and protection of IP as a strategic economic objective. The United States has long advocated for strong global IP enforcement through its trade policy, identifying nations with perceived deficiencies in its annual Special 301 Report.[25] This position reflects the view that robust IP protection is essential for maintaining technological leadership and preventing unfair competition.

China's evolution from a manufacturing-based economy to an innovation-driven one illustrates the shifting dynamics of global IP. Once criticized for weak enforcement, China is now the world's leading source of patent applications and has become more assertive in protecting the IP of its domestic firms abroad.[26] This transition reflects a strategic shift toward indigenous innovation. At the same time, the rise of "patent thickets", dense and overlapping webs of IP rights, in sectors like telecommunications can create barriers to entry and stifle innovation, raising concerns about the potential for abuse of the IP system.[27]

IV. TENSIONS BETWEEN DIGITAL SOVEREIGNTY AND IP

Data Localization and Innovation

Data localization requirements, which mandate that data be stored or processed within a nation's borders, represent a direct conflict between digital sovereignty and innovation. Proponents argue that such measures enhance national security, protect citizen privacy, and facilitate law enforcement access. However, data localization imposes significant costs on innovation. Modern AI systems, for example, require access to vast and diverse datasets for training; geographic restrictions on data flows can fragment these datasets, reducing the quality of AI models and slowing algorithmic development.[28]

Cloud computing, a foundational technology for the digital economy, derives its efficiency from the ability to distribute data globally to optimize performance and cost. Localization undermines this model by forcing companies to build redundant and costly infrastructure in each market where they operate.[29] This burden falls disproportionately on small and medium-sized enterprises (SMEs) and startups, which often lack the resources to navigate complex and varied regulatory regimes, thereby creating barriers to entry and limiting competition. Furthermore, scientific research that relies on international collaboration, such as in medicine and climate science, is impeded when cross-border data flows are restricted.[30]

Technology Transfer Requirements

Some nations condition market access on technology transfer, requiring foreign companies to share intellectual property with domestic partners. China's policies in this area have been a significant source of international trade friction, with the United States and the European Union alleging that their companies face pressure to transfer trade secrets and proprietary

technology in exchange for access to the Chinese market.[31]

Such mandates can reduce the incentive to invest in research and development, as companies may be unable to capture the full economic returns of their innovations. This risk is particularly acute in industries with long development cycles and high capital costs, such as semiconductors and pharmaceuticals. Forced technology transfer also creates significant risks for IP protection, as disclosed proprietary information becomes vulnerable to misappropriation, particularly where legal enforcement mechanisms are weak. These practices have been a central issue in trade disputes, including the U.S.-China conflict, leading to provisions in trade agreements aimed at prohibiting forced technology transfer.[32]

Patent System Fragmentation

Despite harmonization efforts under treaties like the Patent Cooperation Treaty, patent systems remain fundamentally territorial.[33] An inventor must typically file separate patent applications in each jurisdiction where protection is sought, navigating different procedural rules and examination standards. This fragmentation creates legal uncertainty and increases costs for innovators, particularly in the context of digital technologies that operate globally.

Substantive standards for patentability also vary. The patent eligibility of software, for instance, is treated differently in the United States, Europe, and other jurisdictions, creating challenges for securing consistent global protection.[34] The rapid pace of technological change in fields like AI and quantum computing further strains the capacity of patent offices, which struggle to develop examination expertise and manage growing application backlogs, leading to delays and uncertainty for innovators.

V. COMPARATIVE REGULATORY APPROACHES

European Union: A Rights-Based Framework

The European Union has established a comprehensive, rights-based framework for digital governance. The GDPR imposes strict requirements for the processing of personal data and grants individuals extensive rights, including data portability and the right to erasure.[35] The Digital Markets Act (DMA) and Digital Services Act (DSA) extend this approach to platform governance, imposing obligations on large technology companies designated as "gatekeepers" to ensure fair competition and protect user rights.[36] Europe's approach reflects a commitment to prioritizing individual rights and ethical technology use, though it has drawn criticism for potentially creating significant regulatory burdens that may stifle innovation.[37] The EU also pursues technological sovereignty through industrial policy, such as the European Chips Act, which aims to build domestic semiconductor production capacity.[38]

United States: A Market-Driven and National Security-Focused Approach

The United States has historically favored a market-driven approach to digital regulation, characterized by strong IP protection and reliance on sectoral laws rather than a comprehensive data privacy framework.[39] This environment has fostered a powerful innovation ecosystem dominated by American technology firms. However, this model is evolving. Privacy concerns have led to state-level legislation, most notably the California Consumer Privacy Act (CCPA), which established rights similar to those in the GDPR.[40] Antitrust scrutiny of large technology companies has intensified, and national security concerns regarding Chinese technology have resulted in significant export controls and restrictions on specific companies.[41] Recent industrial policy, such as the CHIPS and Science Act, signals a more active government role in securing the domestic technology base through substantial subsidies for semiconductor manufacturing.[42]

China: A State-Directed Model

China's approach to digital sovereignty is characterized by extensive state control over digital activities, implemented through content censorship, cybersecurity regulations, and data localization requirements.[43] Its IP system has expanded rapidly, with a surge in patent filings and strengthened enforcement mechanisms, yet concerns about local protectionism in IP disputes persist.[44] Industrial policies like "Made in China 2025" explicitly target technological self-sufficiency in strategic sectors, utilizing a combination of government funding, market access restrictions, and technology acquisition

to build domestic capabilities. Through its Digital Silk Road initiative, China also exports its digital governance model and infrastructure, potentially establishing technical standards that challenge Western influence in global digital governance.[45]

India and Emerging Economies

As a major emerging economy, India is balancing multiple objectives in its digital governance strategy. The Digital India initiative aims to expand digital infrastructure and services, while the Digital Personal Data Protection Act of 2023 establishes a data protection framework that includes provisions for data transfers and localization.[46] India's IP policies reflect its developmental priorities, utilizing flexibilities within the TRIPS Agreement, such as for compulsory licensing of pharmaceuticals, to ensure access to essential medicines.[47] Many other emerging economies face similar challenges, seeking to attract investment and foster innovation while avoiding "digital colonialism," where foreign technology firms extract data and value with limited local economic benefit.

VI. ECONOMIC AND INNOVATION IMPACTS

Costs of Fragmentation

Digital sovereignty measures that lead to market fragmentation impose substantial economic costs. Companies must navigate multiple, often conflicting, regulatory regimes, build redundant infrastructure, and adapt products for different markets. Studies have estimated that restrictive data localization policies can reduce a country's GDP by inhibiting trade in data-enabled services.[48] These compliance costs disproportionately affect SMEs, which may lack the resources to expand internationally, thereby reducing competition and innovation. Furthermore, restrictions on data flows and technology sharing impede the international collaboration that is essential for modern scientific and technological advancement. This fragmentation can also weaken the network effects that are fundamental to many digital platforms, leading to incompatible ecosystems and reduced consumer choice.[49]

Perceived Security and Privacy Benefits

Proponents of digital sovereignty argue that these measures provide security and privacy benefits that justify the economic costs. Data localization may be perceived as reducing foreign surveillance risks by keeping sensitive data within a country's legal jurisdiction. Cybersecurity mandates can enhance the resilience of critical infrastructure. Restrictions on technology transfers may prevent potential adversaries from acquiring strategic capabilities. Regulations like the GDPR have prompted global improvements in corporate data protection practices, extending benefits beyond the EU by giving individuals greater control over their personal information. While national security concerns related to critical infrastructure are legitimate, the challenge lies in calibrating regulations to achieve these objectives while minimizing negative impacts on innovation and economic growth. Targeted, risk-based measures are often more effective than blanket restrictions.[50]

VII. FRAMEWORK FOR BALANCED GOVERNANCE

Harmonization Through International Agreements

Harmonization through international agreements offers a promising approach to balancing digital sovereignty and innovation. Modern trade agreements increasingly include chapters on digital trade that establish rules for cross-border data flows, prohibit data localization requirements, and protect source code. The United States-Mexico-Canada Agreement (USMCA) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) both contain such provisions.[51] Sectoral agreements on specific technologies, such as AI, could establish common ethical principles and safety standards. Mutual recognition agreements, where countries accept one another's standards as equivalent, can also reduce compliance burdens, although past attempts like the EU-U.S. Privacy Shield have faced legal challenges over surveillance concerns.[52]

Flexible Regulatory Mechanisms

Given the rapid pace of technological change, regulatory frameworks require flexibility. "Regulatory sandboxes," which allow companies to test innovative products in a controlled environment with relaxed

rules, can foster experimentation while managing risks.[53] Principle-based regulation, which establishes broad objectives rather than prescriptive technical rules, allows for greater adaptability as technology evolves. Governance models that involve multiple stakeholders, including governments, industry, civil society, and technical experts, can also improve regulatory quality and legitimacy, as demonstrated by internet standard-setting bodies like the Internet Engineering Task Force (IETF).

Reciprocity and Conditionality

Reciprocal agreements, where countries grant market access and regulatory recognition on the condition that their partners meet equivalent standards, can incentivize the adoption of high-standard rules for IP protection, data privacy, and competition. Conditionality can also be applied to technology and data sharing, enabling beneficial collaboration while managing risks. For example, data sharing agreements can include specific contractual protections for privacy and security. The formation of "digital trade coalitions" among like-minded countries can establish high-standard frameworks that other nations can join, creating a "race to the top" rather than a compromise based on the lowest common denominator.

VIII. CASE STUDIES

The Global Impact of GDPR

The GDPR serves as a prominent example of how one jurisdiction's assertion of digital sovereignty can have global effects. Due to its extraterritorial scope, the GDPR has become a de facto global standard for data protection, compelling companies worldwide to adapt their data handling practices. This "Brussels Effect" demonstrates the power of a large market with high regulatory standards to shape global corporate behavior.[54] However, the GDPR has also imposed significant compliance costs, particularly on SMEs, and its complexity has led to legal uncertainty and litigation. While the GDPR has inspired similar legislation globally, variations between these frameworks continue to create compliance challenges.

U.S.-China Technological Competition

The technological competition between the United States and China represents a significant driver of digital fragmentation. Both nations view technological leadership as essential to national security and economic prosperity. U.S. export controls targeting China's access to advanced semiconductors and related equipment are designed to slow its military and technological advancement.[55] China has responded with measures to promote indigenous innovation and reduce its dependence on foreign technology. This rivalry risks bifurcating global technology markets into separate, incompatible ecosystems, a "splinternet", which would impose significant costs through lost economies of scale, duplicative standards, and reduced innovation.

Pharmaceutical IP and the COVID-19 Pandemic Response

The COVID-19 pandemic highlighted the tension between IP protection and public health. A proposal was introduced at the World Trade Organization (WTO) by India and South Africa to temporarily waive IP rights on COVID-19 vaccines and treatments to expand global manufacturing and access.[56] Proponents of the waiver argued that humanitarian imperatives justified the suspension of IP monopolies, particularly given the substantial public funding that supported vaccine research. Opponents, including pharmaceutical companies and several developed nations, contended that strong IP protection was the primary incentive for the rapid development of the vaccines and that weakening it would discourage future innovation. The debate culminated in a limited and complex WTO agreement, demonstrating the profound difficulty of adapting global IP frameworks to address public health crises.[57]

IX. FUTURE DIRECTIONS AND RECOMMENDATIONS

Toward Digital Multilateralism

A new framework for digital multilateralism is needed to counter the trend toward fragmentation. This framework should be based on core principles that can command broad consensus, such as privacy, cybersecurity, fair competition, and transparency, while allowing for different national implementations. Institutional reforms could support this effort, such as strengthening WIPO's role in harmonizing IP standards or expanding the WTO's mandate to more

effectively govern digital trade. Regional agreements may also serve as building blocks for broader international cooperation.

Adaptive Governance for Emerging Technologies

Emerging technologies like AI and quantum computing require new, adaptive governance approaches. "Anticipatory regulation," which considers potential impacts before widespread deployment, can help mitigate risks while enabling innovation. Tiered, risk-based approaches can apply more stringent rules to high-risk applications (e.g., autonomous weapons) while permitting greater flexibility for low-risk uses. Given the inherently global nature of these technologies, international collaboration on safety standards and ethical principles is essential.

Strengthening and Adapting IP Systems

Intellectual property systems must be updated for the digital era. Greater international harmonization of patent examination standards, particularly for software and AI-related inventions, would reduce fragmentation and legal uncertainty. Improving patent quality through robust examination and post-grant review processes can prevent the issuance of overly broad or non-novel patents that stifle legitimate innovation. It is also important to continue exploring alternative innovation incentives, such as prize funds and advance market commitments, which can complement the IP system. Finally, ensuring that flexibilities within international agreements, such as compulsory licensing and research exceptions, remain available is critical for balancing innovation with equitable access.

X. CONCLUSIONS

The principles of digital sovereignty and intellectual property are in a state of growing tension, shaping the future of the 21st-century global economy and international relations. As nations assert greater control over their digital territories, the collaborative and borderless ecosystem that has fueled innovation faces significant challenges. Data localization, technology transfer mandates, and divergent regulatory frameworks threaten to fragment global technology markets, imposing substantial economic costs and slowing technological progress.

However, a zero-sum choice between sovereignty and innovation is not inevitable. Both concepts represent legitimate state interests: nations have a responsibility to protect their citizens and national security, while innovation thrives on international collaboration and robust IP protection. The central challenge is to develop governance frameworks that reconcile these interests. This paper has examined the diverse approaches taken by major global actors, revealing that the path forward will likely require hybrid models that are adaptable to different technologies and national contexts.

Progress will depend on a commitment to several guiding principles. International harmonization through trade and sectoral agreements can reduce fragmentation. Flexible, principle-based regulatory mechanisms are needed to keep pace with technological change. Reciprocity and multi-stakeholder governance can foster cooperation and improve regulatory outcomes. The economic stakes are immense, but more importantly, technological innovation is critical to addressing humanity's most pressing challenges. The current trajectory toward digital nationalism is detrimental to these shared goals. A renewed commitment to digital multilateralism, based on shared principles and institutional cooperation, offers a more constructive path. The decisions made in the coming years regarding the governance of technology, data, and intellectual property will have lasting consequences for global prosperity, security, and human progress.

REFRENCE

[1] Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World (2006).
[2] Anne-Marie Slaughter, A New World Order (2004).
[3] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015).
[4] Anne-Marie Slaughter, A New World Order (2004).
[5] *See* Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World (2006).
[6] *See generally* Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the

World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS Agreement].
[7] *See* Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong.., Nov. 7, 2016, effective June 1, 2017) (P.R.C.).
[8] *See generally* World Intellectual Prop. Org., World Intellectual Property Report 2022: The Direction of Innovation (2022).
[9] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015).
[10] *See generally* Milton L. Mueller, Networks and States: The Global Politics of Internet Governance (2010).
[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].
[12] Anu Bradford, The Brussels Effect: How the European Union Rules the World (2020).
[13] *See generally* U.S. Dep't of Com., Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (2010).
[14] *See, e.g.*, Addition of Certain Entities to the Entity List, 84 Fed. Reg. 22,961 (May 21, 2019) (codified at 15 C.F.R. pt. 744).
[15] Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong.., Nov. 7, 2016, effective June 1, 2017) (P.R.C.).
[16] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).
[17] *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Electronic Frontier Found. (Feb. 8, 1996), www.eff.org.
[18] *See* Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (2014).
[19] Lei Geral de Proteção de Dados Pessoais (LGPD), Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.).
[20] TRIPS Agreement, *supra* note 6.
[21] *See generally* Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, *as revised at Paris*, July 24, 1971, 25 U.S.T. 1341, 1161 U.N.T.S. 3; Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, *as revised at Stockholm*, July 14, 1967, 21 U.S.T. 1583, 828 U.N.T.S. 305.
[22] *See Alice Corp. Pty. Ltd. v. CLS Bank Int 'l*, 573 U.S. 208 (2014) (addressing the patent eligibility of computer-implemented inventions).
[23] Ryan Abbott, *I Think, Therefore I Invent: Creative Computers and the Future of Patent Law*, 57 B.C. L. Rev. 1079 (2016).
[24] Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. Rev. 925 (2001).
[25] *See generally* Office of the U.S. Trade Representative, 2024 Special 301 Report (2024).
[26] World Intellectual Property. Org., World Intellectual Property Indicators 2023 (2023).
[27] Carl Shapiro, *Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard Setting*, *in* 1 Innovation Policy and the Economy 119 (Adam B. Jaffe et al. eds., 2001).
[28] *See* Info. Tech. & Innovation Found., How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them (2017).
[29] *Id.*
[30] Paul Sawers, *How Data Localization Is Threatening the Promises of Medical Research*, VentureBeat (Mar. 18, 2019), venturebeat.com.
[31] *See* Office of the U.S. Trade Representative, Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974 (2018).
[32] *See* Economic and Trade Agreement Between the Government of the United States of America and the Government of the People's Republic of China, Jan. 15, 2020.
[33] Patent Cooperation Treaty, June 19, 1970, 28 U.S.T. 7645, 1160 U.N.T.S. 231.
[34] *See, e.g.*, Convention on the Grant of European Patents art. 52, Oct. 5, 1973, 1065 U.N.T.S. 199 (excluding "programs for computers" as such from patentability).
[35] GDPR, *supra* note 11.
[36] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the

Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1; Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

[37] *See* Matthias Bauer et al., *Harming EU Competitiveness and Restricting Digital Trade: The Impact of the EU's Proposed Digital Markets Act*, ECIPE Policy Brief No. 2/2021 (2021).

[38] Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 Establishing a Framework of Measures for Strengthening Europe's Semiconductor Ecosystem and Amending Regulation (EU) 2021/694 (Chips Act), 2023 O.J. (L 229) 1.

[39] *See generally* Adam Thierer, *The Perils of Precautionary Regulation: A Critical Analysis of the Proposed EU AI Act*, Mercatus Ctr. (2021).

[40] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 *et seq*. (West 2020).

[41] *See, e.g.*, Export Administration Regulations; Entity List Additions, 84 Fed. Reg. 43,493 (Aug. 21, 2019) (adding Huawei and its affiliates to the Entity List).

[42] CHIPS and Science Act of 2022, Pub. L. No. 117-167, 136 Stat. 1366 (2022).

[43] *See* Samm Sacks, *China's Cybersecurity Law Takes Effect*, Ctr. for Strategic & Int'l Stud. (June 1, 2017).

[44] *See* U.S. Chamber of Commerce, International IP Index (11th ed. 2023).

[45] Eyck Freymann & Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future*, Ctr. for Strategic & Int 'l Stud. (2021).

[46] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).

[47] TRIPS Agreement, *supra* note 6, art. 31.

[48] Matthias Bauer et al., *The Costs of Data Localization: A Friendly Fire on Economic Recovery*, ECIPE Policy Brief No. 1/2021 (2021).

[49] *See* Joseph Farrell & Paul Klemperer, *Coordination and Lock-In: Competition with Switching Costs and Network Effects*, *in* 3 Handbook of Industrial Organization 1967 (Mark Armstrong & Robert Porter eds., 2007).

[50] Eleanor M. Fox, *National Champions, Globalization, and the Rule of Law*, 43 Wake Forest L. Rev. 831 (2008).

[51] Agreement Between the United States of America, the United Mexican States, and Canada, ch. 19, July 1, 2020, ustr.gov; Comprehensive and Progressive Agreement for Trans-Pacific Partnership, ch. 14, Dec. 30, 2018, www.mfat.govt.nz.

[52] *Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (Schrems II)*, ECLI:EU: C:2020:559 (July 16, 2020).

[53] Hilary J. Allen, *Regulatory Sandboxes*, 87 Geo. Wash. L. Rev. 579 (2019).

[54] Bradford, *supra* note 12.

[55] Addition of Certain Entities to the Entity List and Revisions to the Export Administration Regulations, 88 Fed. Reg. 73,424 (Oct. 25, 2023) (codified at 15 C.F.R. pts. 734, 744).

[56] World Trade Organization, Council for Trade-Related Aspects of Intellectual Property Rights, *Waiver from Certain Provisions of the TRIPS Agreement for the Prevention, Containment and Treatment of COVID-19*, IP/C/W/669 (Oct. 2, 2020).

[57] World Trade Organization, Ministerial Conference, Twelfth Session, *Ministerial Decision on the TRIPS Agreement*, WT/MIN(22)/30 (June 17, 2022).