Convergence
A Journal for Young Researchers

ORIGINAL REVIEW

Received: 8-26-25; Accepted: 11-25-25;
Managing Editor: Jonas Katona;
Action Editors: Beniamin Goldstein, Jonas Katona

Big Tech and the Rise of Digital Infrastructure in Border Control

Anna Giulia Golden

Escola Comunitária de Campinas, Campinas, Brazil

Abstract

The use of digital technology in migration control is growing into a worldwide phenomenon. As borders harden and global mobility declines due to restrictive immigration laws and surveillance technologies, governments are leaning on technologies developed by the world's largest and most influential technology companies, also known as "Big Tech," to reshape how movement is managed. This paper investigates how states are increasingly digitizing sovereignty and the exercise of border and migration control, and how they contract Big Tech companies such as Amazon, Tencent, and Palantir to do so. I argue that these companies mediate digital border regimes, not just supporting state apparatuses but shaping mobility through data collection, biometric systems, and algorithmic control. This study builds on existing scholarship, which increasingly frames tech firms as geopolitical actors. I argue that Big Tech's role in border control is not merely technical, but deeply political. I show that structurally distinct regimes such as the United States, historically considered democratic, and China, historically seen as authoritarian, are increasingly relying on similar digital architectures to accomplish essentially the same objective: border and population control. Moreover, tech companies are taking on quasi-sovereign roles, often without accountability, thus raising urgent concerns about digital authoritarianism and the normalization of surveillance. Through comparative case studies based on secondary source analysis of academic articles and media reports, this paper reveals the expanding power of Big Tech companies in shaping twenty-first-century borders.

Keywords: big tech, digital border regimes, global mobility, surveillance technologies, digital authoritarianism, platform governance, algorithmic control

1. Policing Borders in the Algorithmic Age

In June 2025, Los Angeles became the epicenter of a clash between federal enforcement and local protests. Immigration and Customs Enforcement (ICE) raids on Home Depot stores and garment factories in the Fashion District resulted in dozens of

arrests and triggered mass demonstrations. Tensions escalated when federal agents deployed tear gas and detained protesters outside the Roybal Federal Building. In response, the Trump administration dispatched 2,000 National Guard troops to the city without the governor's consent, prompting legal challenges from California state officials. What was initially framed as an immigration enforcement operation had quickly escalated into a militarized confrontation. Yet behind the headlines and street-level conflict was an invisible but powerful infrastructure: the digital systems that enabled the targeting, tracking, and coordination of the raids. From facial recognition scans to algorithmic risk profiling, these operations were powered by cloud platforms and public-private partnerships that now underpin modern immigration control.

Almost 7,000 miles away, a parallel logic of digital enforcement is visible in western China. In the Xinjiang Uyghur Autonomous Region, since late 2016, Chinese authorities have operated the Integrated Joint Operations Platform, a centralized surveillance and policing system that aggregates biometric records, travel histories, communication data, electricity consumption, and personal networks into a single interface. Human Rights Watch reverse-engineered the police app associated with this system and found that it "flags individuals for investigation" based on algorithmic assessments of commonplace behavior, such as using encrypted messaging apps or traveling overseas, and that many of those flagged were subsequently detained or sent to reeducation facilities ("China's Algorithms of Repression," 2019). The United Nations has similarly written on how the Chinese government uses data collection and digital monitoring as part of a larger plan to control the Uyghur population and constrain their freedom of movement (OHCHR, 2022).

In today's increasingly digitized society, border control is not solely controlled by agents who are posted along physical walls made of concrete and fencing, but also by search engines, social media platforms, and predictive algorithms. In other words, states have turned to digital technologies as a means to manage and monitor movement. It is somewhat paradoxical that the internet is being used to increase the global flow of information while at the same time being so effectively deployed to reduce the global mobility of humans. Exiting an international flight or crossing borders by land or sea requires submitting to facial recognition technology knowingly or unknowingly in various countries, including the United States, Australia, and Dubai, to name just a few. The twenty-first century consists of constant use of code, cloud servers, and biometric checkpoints as governments' tactics to control global mobility.

These impressive infrastructures are difficult to manage and are hardly operated by governments alone. The "masterminds" behind the technology used in today's border control are powerful tech corporations, which design, own, and operate with minimal transparency. These companies are often referred to as "Big Tech," a term commonly used to describe the world's most influential companies, such as Apple, Amazon, Google, Meta, Microsoft, Alibaba, Palantir, and Tencent. Big Tech is often equated with corporate surveillance, monopoly, and market power, commanding our political economies and societies (Birch & Bronson, 2022).

These Big Tech companies deploy their border control and mobility-regulating technologies in support of governments commonly considered ideological opposites. The United States is historically considered the beacon of liberal democracy, and China the epitome of authoritarian control. Regardless of perceived ideological differences between the US and Chinese regimes, stark similarities between the two become evident: both countries utilize increasingly powerful technology developed by Big Tech companies to monitor populations, consolidate data, and control movement under the guise of security and sovereignty.

This paper proceeds in five sections: it first offers an overview of the rise of digital border regimes and how governments are

using technology to control their borders. Then, it offers a review of the literature on digital borders, platform power, and surveillance technologies. It identifies foundational contributions to the field and highlights scholarly debates. It continues with a discussion of the ethical and political consequences of this phenomenon, then explores the cases of the United States' use of corporate infrastructure in digital sovereignty and of China's Great Firewall. Finally, it provides a comparative analysis of the similarities and differences of the US and Chinese digital border regimes and their implications and consequences for civil rights and freedoms.

In terms of data sources, the case studies draw on secondary research, including peer-reviewed academic literature, media reports, news investigations, and government documents. This research design enables triangulation among academic discussions, political analysis, and actual migration procedures. The research focuses on observable structures of digital border enforcement instead of speculative tactics by analyzing publicly available material instead of classified operational systems. The study develops a comparative perspective of digitally mediated sovereignty by methodically synthesizing sources on China and the United States, even though it does not use fieldwork or interviews. This method makes it possible to examine how various political systems use comparable biometric monitoring, data extraction, and algorithmic control infrastructures to govern movement. When taken as a whole, these resources shed light on the developing logic of digital border regimes as well as the consequences of contracting out sovereign activities to state-engineered information systems and private platforms.

2. The Rise of Digital Border Regimes

Governments are increasingly using technology to govern. An example of this is that the governance of movement is no longer restricted to existing territory, but now permeates the multiple layers of digital space and everyday life (Narváez, 2025). Surveillance exists beyond ports of entry; through mobile phones, social media activity, and digital databases, those being monitored have little to no clue that they are being watched.

Digital border regimes refer to systems of control embedded in platforms and infrastructures that govern migration long before an individual reaches a physical border. To understand the importance and complexity of these regimes, an understanding of the term "digital infrastructure," a term coined by Santiago Narváez (2025), is necessary. As Narváez argues, "We use the term digital infrastructure to describe the establishment of a foundation that will be fundamental to how world powers will practice migration control... While it may look like technological experimentation... the growth of digital border infrastructure is by design." This quote shows that digital border regimes are not haphazard or temporary. They are part of a long-term strategy by powerful states to expand their control through non-territorial means. These infrastructures operate beneath public scrutiny, which makes them harder to regulate or resist. Digital border regimes extend border governance into daily life and embed it into technical systems that feel neutral, inevitable, or even invisible.

As governments are expanding their use of technology to extend their control well beyond borders or ports of entry, certain states have increasingly outsourced their digital infrastructure and control of digital borders to private companies, such as Amazon, Palantir, and Meta, which are not bound by the same accountability as public institutions. This implies a deeper transformation in sovereignty itself. This shift in the way governance is carried out is indicated by the shift from physical borders to digital infrastructures. According to Vivek Krishnamurthy (2025), digital control works through "anchored infrastructure," or systems that have power through design rather than through legal authority. Media scholar José van Dijck (2018, p.18) also emphasizes how platforms now handle infrastructure tasks like identity verification, mobility management,

and public communication that were previously the purview of governments. Tech platforms are not just working for the government when they make decisions about who is allowed access and who is not. They are exercising sovereign forms of authority.

The experience of mobility in the digital age is shaped by the same platforms that both aid and endanger refugees. Refugees today rely on WhatsApp, Google Maps, and Facebook to coordinate their journeys, locate resources, and stay in contact with family members. But these tools are also used to track, monitor, and occasionally criminalize their movements (Narváez, 2025). The needs of displaced people were never taken into consideration when designing these platforms. Rather, they serve security and commercial interests, leaving refugees vulnerable to monitoring and exploitation. When control is incorporated into the very architecture of the digital systems that refugees must use, rather than just being imposed through state policy, this paradox becomes even more perilous.

Digital border regimes are more than just instruments to help governments control migration. These are control systems that are integrated right into the infrastructures and platforms that influence daily life. In the background, these technologies silently decide who is free to move and who is not. These days, biometric scans, data tracking, and platform surveillance allow migrants and refugees to engage with borders long before they physically cross. Although the businesses that create and run these systems frequently operate without public oversight, they have an impact on choices that were previously solely the domain of the state. The line between political power and technical service is blurring as private companies increasingly influence how mobility is governed. Understanding how digital technologies are changing borders and redefining what it means to be a citizen and belong in the twenty-first century requires an awareness of this change.

3. Literature Review and Argument

As the role of government evolves with technology and governments are giving Big Tech increasingly prominent roles in border control and digital sovereignty, scholarly research on these two related shifts has been on the rise. Narváez (2025) and other scholars describe this shift in border control as "the everywhere border," a phrase that captures how movement is increasingly regulated far beyond the physical frontier. Mark Latonero and Paula Kift (2018) use the term "digital passages" to describe how migrants navigate systems shaped by both state and corporate actors. The most prominent example of this model would be the Great Firewall of China, a digital barrier established by the state that controls information flows, monitors internet activity, and prohibits many foreign websites and services. As one scholar notes, it is "the most sophisticated censorship apparatus in the world, built not just to block content but to control a population" (Baron, 2019). Latonero and Kift (2018) comment on how platforms like Facebook and WhatsApp serve as both an essential tool for refugees and the very systems that expose them to surveillance and data extraction.

Similarly, E. Tendayi Achiume (2020) documents that facial recognition technologies and algorithmic scoring systems are often disguised as neutral, but their true nature is often one of racial bias, endangering vulnerable populations. A 2024 study by Saura García (2024) calls this phenomenon "bordering by design," arguing that commercial platforms embed control logic directly into their architecture. García (2024) also states that companies such as Palantir and Amazon have become vital to Western immigration enforcement systems while operating outside of the public eye. Meanwhile, the Chinese state has built a legal and technological framework that turns digital infrastructure into a tool of sovereignty. Scholars define this as "anchored infrastructure," where control is practiced through technical systems rather than traditional policy (Krishnamurthy, 2025). Hoang et al. (2021) further show how censorship and control infrastructures are expressions of

political ideology as much as engineering design.

José van Dijck's (2018, p. 2) work in The Platform Society clearly mentions how tech firms have taken over infrastructural functions traditionally managed by the state. Krishnamurthy (2025), a writer for the Chicago Journal, extends this logic, emphasizing that infrastructure has become a mode of governance, deciding who is recognized by the state and who remains invisible. Based on investigations made by scholars, these digital enforcement systems disproportionately harm Black, Indigenous, and migrant communities, often resulting in discriminatory profiling or even deadly outcomes (Achiume et al., 2020). Once these digital infrastructures are normalized, it becomes difficult to question their legality or ethics (García, 2024). As one Eritrean asylum seeker in Brussels stated, "We are Black and border guards hate us. Their computers hate us too" (Achiume et al., 2020).

While existing scholarship often examines Chinese censorship and U.S. surveillance systems separately, this paper brings the two into conversation to show how structurally distinct regimes rely on similar digital architectures. Drawing on scholarship in platform governance, surveillance studies, and digital sovereignty, the paper investigates how companies such as Amazon, Palantir, Meta, and Alibaba act as infrastructural gatekeepers, often performing quasi-sovereign functions to determine who is permitted to move, who is watched, and who is excluded. Drawing on José van Dijck's concept of the platform society and Vivek Krishnamurthy's idea of "anchored infrastructure," I argue that Big Tech companies are increasingly performing state-like functions in regulating movement. These firms design and operate systems that determine access, visibility, and identity—roles traditionally reserved for sovereign governments. By embedding control into technical design rather than legal mandate, digital infrastructures function as instruments of governance. This is problematic in that governance is thereby shifted from public or institutional oversight and accountability to opaque and less transparent control with different incentives than traditional governance. This framework helps advance the scholarship by studying how structurally distinct regimes, from historically democratic to historically authoritarian ones, arrive at similar practices of digital border enforcement.

4. Ethical and Political Consequences of Digital Border Regimes

A border is a marker of where a state's territory begins and where it ends. Those inside the state's territory must abide by its laws. While the idea of borders is not new, the current map of the world and its nation-states is relatively new, due to European colonization and decolonization, two world wars, and the fall of the Soviet Union. Traditionally, the role of states in border security is seen as protecting national sovereignty through controlling the movement of people and resources across borders. In fact, the right of the government to protect its territorial sovereignty is so fundamentally and universally accepted that it is enshrined in Articles 2(4) and 2(7) of the UN Charter, which state that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State…" and that "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state…"

There is no doubt that without borders, the governance of a state becomes unclear. The goods and services a state would provide would be difficult to deliver, resulting in a lack of clarity about who receives such benefits, including public health, social welfare, law and order, and economic regulation. In short, the existence of borders is fundamentally important and necessary. Although this is true, the purpose of a border can quickly become blurred with one of excessive control and restriction. The question arises: how far should the commonly accepted role of the state in securing its borders go before it

impedes basic human rights?

Embedding border control into digital infrastructure has profound ethical and political implications. First, it normalizes surveillance. Migrants and refugees now enter a continuous security architecture long before crossing any physical border. Every app login or location ping can put them on a watchlist. As Latonero observes, "every text message, money transfer, social media login… generates data on refugees as well as smugglers," data that companies collect for profit (Kara, 2017). In other words, the act of fleeing becomes entangled with being monitored. Fleeing one's homeland is already dehumanizing; being monitored against one's will only adds to the humiliation. Biometric screenings at airports, facial-recognition cameras in cities, automated "risk scores" in databases—these were once extraordinary measures but are becoming routine. Over time, this ubiquity of monitoring reshapes social norms: it becomes accepted that people's mobility and private information are tracked in the name of migration control. These "anchored infrastructures" exert control through design rather than legislation, which makes surveillance seem unavoidable (Krishnamurthy, 2025). Democratic checks are undermined by this slow change because there will be less opposition to and scrutiny of the use of these systems if society starts to accept ongoing digital surveillance as the norm.

Second, digital border regimes have the potential to make inequality and discrimination worse. According to UN Special Rapporteur Tendayi Achiume's (2021) analysis, "it is the core… function of borders to discriminate" along racial, national, and class lines even before the advent of digital technology. Digital tools can make this worse. Algorithmic profiling, for instance, tends to reinforce preexisting biases. For instance, if certain nationalities are arbitrarily identified as "risk," automated systems will routinely apply harsher enforcement to those groups. According to scholars writing for BBC News, the UK's Home Office utilized an algorithm that resulted in discrimination in visa approvals based on racial and national biases (BBC News, 2020). Achiume (2021) draws attention to the idea of "digital racial borders," in which data-driven criteria and purportedly neutral algorithms reinforce racist or xenophobic results. In reality, migrants of color frequently come under more scrutiny. For example, even if their travel documents are in order, digital processing probably catches them more frequently because facial recognition systems have higher error rates for non-white faces. "Even top-performing algorithms will erroneously recognize images labeled 'Black women' 20 times more frequently than images labeled 'white men'" (Israel, 2020). Furthermore, vulnerable populations may be exploited by the data economy of migration. Refugees express concern that their digital footprint, including photographs, posts on social media, and GPS data, will be exploited against them. According to Achiume, this has a chilling effect because migrants may choose not to use services or the internet to avoid being watched. As people look for covert routes or communications to avoid detection, Latonero cautions that excessive tracking can drive refugees "off the grid" (Kara, 2017). The human cost is obvious: individuals lose their autonomy and sense of dignity, and some might even choose not to share data in favor of receiving aid or legal counsel.

Finally, human rights and governance are threatened by digital border regimes. Without the same accountability, private tech companies have taken over functions that were previously performed by governments or aid organizations. As demonstrated by Amazon and Palantir, these corporations have sovereign-like control over decisions pertaining to mobility, but they are exempt from judicial review, democratic oversight, and transparency laws. This can result in glaring injustices. For example, a mistaken flag in a database might detain an innocent asylum seeker without recourse, and there is no clear process to challenge an opaque algorithmic output. Normal government transparency mechanisms (public records, court hearings) do not extend into corporate code. Latonero and colleagues (2018) argue that when platform architecture "decides… who is allowed access, and who is not," these decisions are effectively "exercising sovereign forms of authority." Ethically, this displacement of authority violates basic rights: it undermines due process, privacy, and equality before the law. It transfers

political power into unaccountable channels. According to one critique, states use their tools to implement laws that might otherwise incite public outrage, while tech companies "have hidden behind [the ideal of] information wants to be free… to dodge regulations and build monopolies" (Great Firewall, 2025).

A significant change is represented by the emergence of digital border regimes. These systems, which frequently disproportionately affect already marginalized groups, have normalized previously unheard-of levels of monitoring and control. We are seeing the convergence of digital enclosures and racialized borders, as Achiume (2021) highlights, creating a "digital racial border" that deprives individuals of their rights in algorithmic ways. The ethical stakes are high: technologies created without taking into account the interests of individuals jeopardize freedom of movement and human dignity. Scholars and advocates contend that stringent oversight, transparency requirements, and legal protections are necessary to protect rights and democracy. The fate of refugees and migrants will be shaped by the covert logic of private code and state security prerogatives if digital border infrastructures are not governed (Achiume, 2021).

5. Case Study Analysis: Comparing the US and Chinese Approaches to Digitizing Border Regimes

5.1. The US Case: Corporate Platforms as Infrastructures of Migration Enforcement

The infrastructure of contemporary migration control in the United States is now supported by large technology companies. Enforcement agencies use tools and data systems developed by companies like Palantir, Amazon Web Services (AWS), and Meta (via Facebook and WhatsApp) to track, manage, and detain migrants.

It is important to outline the difference in accountability between public versus private institutions. Whereas public institutions are held directly accountable to the people and have constitutional and democratic obligations, private institutions that are hired by government agencies are only accountable to the agency that hired them, not directly accountable to the people. For example, public agencies are subject to various oversight mechanisms, such as the Freedom of Information Act (FOIA), Congressional oversight, the Administrative Procedures Act, and so forth. With the exception of Congress's ability to investigate their dealings with the government, private companies are not subject to these means of oversight. To imagine this in practice, the U.S. Immigration and Customs Enforcement Agency (ICE) is legally subject to FOIA requests, whereas Palantir would not be directly subject to FOIA requests. It's worth noting that under the current Trump administration, the function of congressional oversight, even over public institutions such as ICE, is subject to failure under extreme political partisanship.

Alongside having little public or institutional oversight, these private platforms are motivated by incentives for innovation and profit. For instance, Palantir was recently awarded a $30 million contract by the U.S. Immigration and Customs Enforcement (ICE) agency to develop "ImmigrationOS," a system that will provide ICE with "near real-time visibility" into potential deportees (Haskins, 2025). As evidence of how the company's financial success is linked to fortifying the border, internal documents reveal that Palantir's technology has been extensively incorporated into ICE operations for over ten years; the corporation has acknowledged working with the Department of Homeland Security since 2012 (Bhuiyan, 2025). Similarly, Amazon's cloud arm (AWS) powers much of the U.S. border regime: DHS agencies rely heavily on AWS to store and analyze massive datasets on migrants. Amazon Web Services hosts ICE's Investigative Management System and other Department of Homeland Security immigration databases, including biometric records for over 230 million people, and Palantir pays Amazon

around $600,000 a month to use its servers (Hao, 2020). Corporate economic motives are linked to the growth of digital immigration enforcement systems, as evidenced by Amazon's position as the federal government's primary cloud provider and its strong institutional ties to DHS (Hao, 2020).

These corporate systems profit from migrant data while remaining opaque due to the lack of transparency and oversight that is required from public agencies. Refugees themselves point out that digital platforms were not designed for their needs. As previously mentioned, Latonero and Kift (2018) observe migrants depend on tools like WhatsApp and Google Maps to survive, yet those same platforms "serve security and commercial interests," leaving refugees "vulnerable to monitoring and exploitation." The data trails that migrants leave (every text message, social-media login, money transfer) are harvested by companies (e.g., Facebook, Vodafone, Western Union) for profit (Kara, 2017). Even well-meaning features, like Facebook's "community help" for refugees, sit beside aggressive data collection. WhatsApp, for instance, offers encrypted chats, but it also generates metadata (timestamps, contact lists) that can be, and has been, accessed by authorities worldwide. In short, Big Tech firms market themselves as neutral platforms or even humanitarian enablers, yet behind the scenes, their services are integral to border enforcement. According to recent reports, Silicon Valley's technologies have become essential to immigration enforcement, with Palantir being referred to as ICE's "corporate backbone" and its technology being integrated into daily deportation and surveillance activities (Bhuiyan, 2025).

For refugees and migrants, the repercussions are severe. Because private tech firms are not subject to democratic oversight or governmental accountability systems, choices that impact people's lives and freedoms may be incorporated into proprietary code. For example, these privately owned platforms can knowingly or unknowingly write biases into their algorithms with no recourse for correction as would be available with public oversight in, for example, traditional democratic systems. Without any public discussion, data-driven targeting may lead to the separation of families or the detention of individuals. In practice, this means that traditional questions of who decides who belongs have shifted from courts and legislatures into corporate boardrooms and engineering teams. As Latonero notes, when "control is incorporated into the very architecture of the digital systems" used by refugees, "the paradox becomes even more perilous" (Kara, 2017).

In summary, US migration enforcement today is powered by corporate infrastructure. Companies like Palantir, Amazon, and Meta make tens of millions of dollars in contracts in the United States alone by using digital tools to enforce borders, but their operations are kept secret from the public (Haskins, 2025). Transparency, bias, and the rights of individuals entangled in these digital webs are pressing issues brought up by this dynamic, particularly when AI models are used. Much of the inner workings of these platforms—the algorithms, data sources, and risk assessments—are proprietary and confidential, meaning the public and affected individuals have little insight into how decisions are made or how errors are addressed.

6. The Great Firewall of China: Censorship, Control, and Digital Sovereignty

In contrast to the US approach to digital border control, in which state agencies partner with private corporations, China operates "the Great Firewall," a system built from a combination of legal, technical, and political measures used to control internet access and content. It includes nationwide filtering of foreign websites, data localization laws, state-mandated content moderation, and collaboration with domestic platforms like Tencent and Alibaba. Through these layers of control, the Chinese government asserts digital sovereignty over its cyberspace, turning the internet into a managed border. As journalist James Griffiths describes, what once was "little more than a glorified porn filter" has been built into "the most sophisticated system of online censorship in the world" (Great Firewall, 2025). Underpinning the GFW is China's doctrine of

"cyber-sovereignty": the idea that the Chinese government has supreme authority over all network traffic within its borders. The state's ability to oversee international corporations and manage information flows is demonstrated by successive laws, like the 2017 Cybersecurity Law and the 2021 Data Security Law, which mandate that businesses store data inside China and provide authorities access to digital systems (Wee, 2017). This legal framework not only shields the domestic tech sector (fostering giants like Alibaba and Tencent) by giving them favored status (Alsabah, 2017) but also forces global firms to comply or be shut out. For example, Chinese data laws compelled foreign companies to conform. In order to comply with government regulations, Apple transferred Chinese users' iCloud data and encryption keys to servers run by a state-affiliated company in 2018 (BBC News, 2018). These measures enshrine digital sovereignty by design, making China's internet a fenced-off world where content is tightly controlled.

Censorship within the GFW is executed by both public and private actors. On the state side, the Cyberspace Administration of China (CAC) writes regulations and coordinates enforcement. On the technical side, filtering equipment (often supplied by domestic firms) is deployed at national gateways and ISP networks. Griffiths and others document how even encrypted or VPN traffic is now subject to automated filtering and active probing (Great Firewall, 2025). To bypass the firewall, citizens have begun to use VPNs, tools that encrypt internet traffic and hide users' locations, as a way to access information and websites otherwise blocked by the Chinese government. In 2017, Mehmut Memtimin, a Uyghur computer science student at Xinjiang University, was sentenced to thirteen years in prison for using a VPN to bypass state internet controls and access information deemed "illegal" (Uyghur, 2025). The university student's arrest exemplifies the intentions of the Chinese government: authority and total control over its citizens. The sophistication of these tools means that typical privacy measures are often ineffective; in effect, the Chinese state has built surveillance into the internet's architecture. Meanwhile, Chinese tech companies operate under explicit censorship mandates. Domestic platforms (WeChat, Weibo, etc.) must pre-screen content for political sensitivity, and employees face criminal penalties for failing to censor forbidden speech. Even global internet standards are being reshaped: Chinese proposals at international bodies press for "cyber-sovereignty" norms that would legitimize each state isolating its segment of the net.

In sum, China's digital border is a state-crafted "splinternet," a term coined by Clyde Wayne Crews in 2001 to describe parts of the internet that are divided or separated from the universally accessible internet. By combining hard infrastructure (firewalls, filters, and data centers) with strict legal controls, the Chinese government has rendered the internet an extension of territorial sovereignty. Griffiths notes that this model not only clamps down on domestic dissent but also exports influence: other authoritarian states are now adopting similar tactics (sometimes even buying Chinese tech) to police information. Furthermore, China is a prime example of digital sovereignty in action. Building "cyberspatial ramparts" to regulate online flows shows how states can redraw informational borders similarly to physical ones, influencing who can access or distribute information and igniting a larger global "splinternet" movement (The Economist, 2025).

7. Analysis of Similarities and Differences in the US and China Digital Border Regimes

The United States and China represent two of the most influential models of digital border governance in the world. Each illustrates how states are adapting to the challenges of migration, mobility, and information control by embedding power into technical infrastructures. The two systems appear distinct in both political logic and institutional design. In the United States, digital border control grows from collaboration between state agencies and private corporations that design and manage the tools of enforcement. In China, this originates from the government's direct claim of control over networks, data, and platforms under the notion of cyber-sovereignty. Yet, despite their structural and ideological differences, both models

reveal a convergence in practice: the use of digital systems to regulate movement, filter access to information, and consolidate authority through technology.

The interests and activities of Big Tech companies have become undeniably linked to the architecture of border control in the United States. Businesses like Palantir, Amazon, and Meta are crucial allies of organizations like DHS and ICE. These businesses create and manage data infrastructures that provide the government with unprecedented accuracy in tracking, analyzing, and detaining migrants. The outsourcing of sovereign responsibilities to private parties sets this approach apart. The public cannot access or study proprietary systems that make decisions about collecting, handling, and use of information in enforcement. This approach undermines accountability since corporate motivations for efficiency and profit control the technological infrastructure that enables policy enforcement, even while state authorities are responsible for enforcing it. As a result, the border functions through networks owned and run by private companies, frequently without the democratic control that typically limits state power. This is a type of privatized sovereignty.

China's digital border regime, which is based on centralization of authority rather than its dispersion, has a different course. Comprehensive state control over cyberspace is made possible by the Great Firewall, the 2017 Cybersecurity Law, and the 2021 Data Security Law. The Chinese government depicts this system as a declaration of national sovereignty, asserting that it has the authority to control all online activity and content inside its borders. As extensions of the government, businesses like Tencent and Alibaba are required to monitor, filter, and report user activities in accordance with official borders. The border, in this context, is not limited to the physical frontier but extends into every node of digital communication. It defines what information can circulate, who may access global networks, and under what conditions. In practice, this system transforms cyberspace into a managed territory, where surveillance and censorship are tools of both governance and social order.

Although the two regimes differ in structure, they converge in their outcomes. Both rely on massive infrastructures of surveillance and data management that blur the distinction between state power and corporate power in governance. In each instance, digital systems that were initially portrayed as impartial instruments of efficiency have evolved into tools of control. While Chinese residents live in an internet environment where access and expression are strictly regulated by law, migrants and refugees in the United States negotiate a landscape where every digital trace can be examined by private or governmental actors. In both situations, the border serves as a dynamic network of checkpoints dispersed throughout data centers, devices, and algorithms rather than a fixed geographic boundary. The parallels imply that shared technological imperatives, rather than political ideology, dictate digital border regimes. Both authoritarian and democratic nations use the same infrastructures to control migration, classify populations, and secure information.

Taken together, these cases reveal the emergence of a global pattern in which borders are increasingly defined by code rather than just by territory. The technologies used to monitor, categorize, and control populations travel across political systems, even as they serve different national purposes. The United States privatizes its border through the market, while China digitizes its border through centralized state control of cyberspace. However, both support a more comprehensive shift in sovereignty, where digital infrastructure rather than human judgment is used to determine who is identified, who moves, and who belongs. Their mutual reliance on data systems, biometric identification, and algorithmic analysis to control mobility in a world where the digital and the physical are inextricably linked is what connects them rather than their ideology.

8. Digital Borders, New Global Order

This study has demonstrated that the expansion of digital infrastructure is transforming borders from fixed lines on a map into distributed systems embedded in data collection, biometric surveillance, and networked platforms. Consequently, software systems, remote databases, and algorithmic tools increasingly determine who has the right to move, who is flagged for scrutiny, and who receives legal protection long before reaching a physical checkpoint. The geography of population control is changing as enforcement now takes place inside refugee camps, airports, telecom networks, and social media ecosystems. By integrating refugees into a global data infrastructure that links camps across continents and links assistance access to digital enrollment, the UNHCR's biometric identification systems serve as an example of this change. What was once a humanitarian register has evolved into an infrastructure that both empowers and disciplines, demonstrating the technological integration of security procedures and humanitarian systems. Foley describes China's Great Firewall as an attempt to "stop unwanted information at its borders" (Foley, 2023). It is an example of a state-driven model of cyber-sovereignty in which power is exercised by filtering, inspecting, and controlling information flows to protect national authority and restrict unwanted content. These cases show that digital borders are no longer hypothetical. They are functioning infrastructures that shape mobility and belonging in real time.

The consequences for sovereignty are noteworthy because, although states used to have exclusive authority over mobility regulation, private companies that create and run digital systems essential to border security now partially share that authority. Biometric databases and automated screening technologies that are created by private businesses under government contracts serve as extensions of sovereign authority while staying outside of conventional public or institutional accountability processes. In the meantime, governments are establishing their own digital authority through extensive information control regimes, national identity stacks, and sovereign cloud initiatives. Examples of these include China's internet governance apparatus and Europe's endeavor to develop autonomous digital infrastructure (Foley, 2023). These advancements demonstrate that in the twenty-first century, control over data standards, cloud storage, identification protocols, and cross-border information flows is just as important to exercising sovereignty as territorial control. This hybrid paradigm blurs accountability and makes it challenging to identify who ultimately controls mobility by combining public and private authority. Increasingly, sovereignty is found in infrastructure and code rather than only in outwardly visible organizations.

Individual rights and civil freedoms are significantly impacted by these structural changes. Digital border technologies frequently exacerbate inequality and limit access to fundamental rights like nondiscrimination, privacy, and asylum, according to a warning from Amnesty International (Amnesty International, 2024). Once-unusual practices, such as demanding access to personal devices or communication records, are now commonplace components of border screening. Data becomes a condition of mobility within and between states, requiring persons who are already at risk to divulge personal information to systems that they are unable to scrutinize or challenge. Because of this, digital boundaries run the potential of establishing a tiered mobility system where certain people can travel freely within and freely outside, while others are subject to increased surveillance and exclusion. Additionally, when algorithmic models classify people as dangerous based on ambiguous and sometimes faulty criteria, these technologies reinforce and replicate biases. In this situation, technology is not neutral; rather, it actively influences how migration and citizenship are experienced.

Legal innovation, transparency measures, and human rights-based ethical obligations are necessary to address these issues. Even ambitious frameworks find it difficult to keep up with the rapid advancements in technology, and current policy efforts

are still inconsistent. Vulnerable people are subject to opaque and error-prone systems due to the European Union's Artificial Intelligence Act's inadequate regulation of high-risk migratory technology (Weizenbaum Institut, 2024). As evidenced by the ongoing discussions surrounding EuroStack, policymakers are actively debating how to integrate displaced individuals into emerging European digital identification systems without reproducing exclusionary practices (Pai, 2025). These discussions highlight the political, not just technical, nature of digital infrastructure governance. Digital boundaries run the potential of becoming irreversible systems of surveillance and exclusion in the absence of significant oversight. However, by requiring openness, minimizing data, making appeals procedures accessible, and involving the public in the design process, these systems can also be shaped in a way that is rights-centered. The decisions taken today about the governance of technology, who is involved in those decisions, and whether or not mobility and dignity are given precedence above efficiency and control will decide the future of borders.

This study also opens several avenues for future research. Comparative analysis could be expanded to other emerging digital border regimes, such as the European Union's digital identity system or biometric corridors in East Africa. Ethnographic methods could explore how migrants themselves navigate and resist these infrastructures. Finally, further legal scholarship is needed to assess how international frameworks, such as the right to seek asylum, should adapt to digital governance practices shaped by both states and private firms.

9. References

Achiume, E. T. (2021). Digital racial borders. *AJIL Unbound*, 115, 333–338. https://doi.org/10.1017/aju.2021.52

Achiume, E. T., Chander, S., & Molnar, P. (2020, November 23). Technology is the new border enforcer, and it discriminates. *Al Jazeera*. https://www.aljazeera.com/opinions/2020/11/23/technology-is-the-new-border-enforcer-and-it-discriminates

Alsabah, N. (2017, March 22). China's cyber regulations: A headache for foreign companies. *Merics*. https://merics.org/en/comment/chinas-cyber-regulations-headache-foreign-companies

Amnesty International. (2024, May 22). *Global: New technology and AI used at borders increases inequalities and undermines human rights of migrants*. https://www.amnesty.org/en/latest/news/2024/05/global-new-technology-and-ai-used-at-borders-increases-inequalities-and-undermines-human-rights-of-migrants/

Baron, J. (2019, April 8). Cyber-sovereignty and China's Great Firewall: An interview with James Griffiths. *Forbes*. https://www.forbes.com/sites/jessicabaron/2019/04/08/cyber-sovereignty-and-chinas-great-firewall-an-interview-with-james-griffiths/

BBC News. (2018, July 18). *Apple iCloud: State firm hosts user data in China*. https://www.bbc.com/news/technology-44870508

BBC News. (2020, August 4). *Home Office drops "racist" algorithm from visa decisions*. https://www.bbc.com/news/technology-53650758

Bhuiyan, J. (2025, September 22). Documents offer rare insight on Ice's close relationship with Palantir. *The Guardian*.

https://www.theguardian.com/us-news/ng-interactive/2025/sep/22/ice-palantir-data

Birch, K., & Bronson, K. (2022). Big tech. *Science as Culture*, 31(1), 1–14. https://doi.org/10.1080/09505431.2022.2036118

Cheney, K., & Gerstein, J. (2025, June 10). California asks judge to 'immediately' block military from joining ICE raids. *POLITICO*. https://www.politico.com/news/2025/06/10/california-restraining-order-national-guard-00397401

Foley, J. J. (2023, November 15). China's authoritarian grip: How China reinforces social control, cultivates a climate of fear, and minimizes dissent. *Journal of Indo-Pacific Affairs*. https://www.airuniversity.af.edu/JIPA/Display/Article/3587653/chinas-authoritarian-grip-how-china-reinforces-social-control-cultivates-a-clim/

García, C. S. (2024). Datafeudalism: The domination of modern societies by big tech companies. *Philosophy & Technology*, 37(3), Article 54. https://doi.org/10.1007/s13347-024-00777-1

Griffiths, J. (2025, April 11). *The Great Firewall of China: How to build and control an alternative version of the internet*. https://jamestgriffiths.com/great-firewall/

Hao, K. (2018, October 22). Amazon is the invisible backbone behind ICE's immigration crackdown. *MIT Technology Review*. https://www.technologyreview.com/2018/10/22/139639/amazon-is-the-invisible-backbone-behind-ices-immigration-crackdown/

Haskins, C. (2025, April 18). ICE is paying Palantir $30 million to build 'ImmigrationOS' surveillance platform. *WIRED*. https://www.wired.com/story/ice-palantir-immigrationos/

Henessy-Fiske, M., Thebault, R., & Berman, M. (2025, June 9). L.A. protesters clash with officers as National Guard presence draws pushback. *The Washington Post*. https://www.washingtonpost.com/nation/2025/06/09/la-protests-ice-national-guard/

Hoang, N. P., Niaki, A. A., Dalek, J., Knockel, J., Lin, P., Marczak, B., Crete-Nishihata, M., Gill, P., & Polychronakis, M. (2021, June 3). *How Great is the Great Firewall? Measuring China's DNS Censorship* (Version 1). arXiv. https://arxiv.org/abs/2106.02167

Human Rights Watch. (2019). *China's algorithms of repression: Reverse engineering a Xinjiang police mass surveillance app*. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance-app

Israel, T. (2020, September 30). *Facial recognition at a crossroads: Transformation at our borders and beyond*. Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic. https://ssrn.com/abstract=3714297

Kara. (2016, February 8). For refugees, a digital passage to Europe. *Responsible Data*. https://responsibledata.io/2016/02/08/for-refugees-a-digital-passage-to-europe

Krishnamurthy, V. (2025). Anchoring digital sovereignty. *Chicago Journal of International Law*. https://cjil.uchicago.edu/print-archive/anchoring-digital-sovereignty

Latonero, M., & Kift, P. (2018). On digital passages and borders: Refugees and the new infrastructure for movement and control. *Social Media + Society*, 4(1), Article 205630511876443. https://doi.org/10.1177/2056305118764432

Narváez, M. Á. B. (2025, July 10). The everywhere border. *Transnational Institute*. https://www.tni.org/en/article/the-everywhere-border

Office of the United Nations High Commissioner for Human Rights. (2022, August 31). *OHCHR assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China*. https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf

Pai, R. (2025, May 6). EuroStack's digital sovereignty push risks excluding people on the move. *Tech Policy Press*. https://www.techpolicy.press/eurostacks-digital-sovereignty-push-risks-excluding-people-on-the-move/

The Economist. (2025, September 4). What the splinternet means for big tech. *The Economist*. https://www.economist.com/business/2025/09/04/what-the-splinternet-means-for-big-tech

Uyghur, B. R. (2023, June 8). Uyghur university student serving 13-year sentence for using VPN. *Radio Free Asia*. https://www.rfa.org/english/news/uyghur/student-sentenced-06082023154805.html

Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.

Wee, S.-L. (2017, May 31). China's new cybersecurity law leaves foreign firms guessing. *The New York Times*. https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html

Weizenbaum Institut. (2024, October 9). AI and surveillance at the border – "The technology doesn't actually work at all". https://www.weizenbaum-institut.de/news/detail/ai-and-surveillance-at-the-border-the-technology-doesnt-actually-work-at-all/

Acknowledgements

I would like to express my sincere gratitude to Dr. Ida Danewid, Associate Professor in Gender & Global Political Economy (International Relations) at the School of Global Studies, University of Sussex, and to Ms. Tanja Weis, PhD Research Student in the Department of International Relations at the University of Sussex, for their invaluable mentorship and guidance through Indigo Research. Their insights, encouragement, and critical feedback were instrumental in shaping the direction and depth of this research.

Author Biography

Anna Giulia Golden is a Brazilian-American student currently completing high school in Brazil after studying in the United States until her sophomore year. Her multicultural upbringing has shaped her interest in global politics and inspired her to pursue International Relations at the university level. Beyond her academic work, she is dedicated to expanding literacy globally through Bee Readers, a student-led initiative that collects and donates books to underserved communities in the US, Brazil, and Kenya. Through her research and community efforts, she hopes to contribute to a more informed and

inclusive global society.

Mentor Contribution Statements

Dr. Ida Danewid, an Associate Professor in Gender and Global Political Economy at the University of Sussex's School of Global Studies, acted as the principal mentor for this project. She was instrumental in helping to shape the manuscript. She helped refine the main question, bolster the theoretical framework, and organize the argument at the early stages of the research's conceptualization. Her comments helped shape the early drafts, particularly in terms of defining important terms, enhancing links to previous research, and improving the paper's general structure. Additionally, Dr. Danewid suggested foundational material that influenced the project's analytical course. The manuscript's clarity, rigor, and scholarly depth were greatly enhanced by her intellectual direction.

Ms. Tanja Weis, a PhD research student in the University of Sussex's Department of International Relations, acted as a co-mentor early on in the study. She offered thorough criticism on the first drafts, which helped to improve the manuscript's analytical flow, structural coherence, and scope. Ms. Weis made a contribution by pointing out places that needed clarification, offering suggestions for improving the argument's precision, and suggesting extra literature to bolster and broaden the analysis. She provided mentorship and critical comments that helped build a solid basis for the work.

Dr. Gwendolyn Whidden, who received a PhD in International Relations at the University of Oxford, provided mentorship during the revision stage of the manuscript, after it had already entered the application process for the Convergence Journal. Her efforts were concentrated on implementing the feedback and recommendations of the peer reviewers. She pointed out instances where the argument could be more succinct or better supported, offered suggestions for improving transitions within and between paragraphs and sections, and advised structural changes to improve the flow and coherence of the arguments. Gwendolyn provided editorial advice that improved the final manuscript's quality and cohesion.