Big Tech and the Rise of Digital Infrastructure on Border Control

[redacted]

Abstract

ICE agents storm poultry facilities and produce packhouses in targeted raids. Hundreds of migrant workers are rounded up and removed in these highly coordinated initiatives. ICE could not coordinate these raids without help from Big Tech. Palantir Technologies designs and builds data integration and analytics platforms to facilitate ICE in the identification of migrant workers and the coordination of raids. This is not just an American phenomenon; the use of Big Tech in migration control is growing into a worldwide phenomenon. As borders harden and global mobility declines due to restrictive immigration laws and surveillance technologies, Big Tech has become critical in reshaping how movement is managed. This paper investigates how companies such as Meta, Google, Amazon, Microsoft, and Palantir act as digital border regimes, not just supporting state apparatuses but shaping mobility through data collection, biometric systems, and algorithmic control. While scholars increasingly frame tech firms as geopolitical actors, this study builds on work in platform and infrastructure studies to argue that Big Tech's role is not merely technical, but deeply political. This study hopes to add to the existing literature by comparing how 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. These platforms are taking on quasi-sovereign roles, often without accountability, thus raising urgent concerns about digital authoritarianism and the normalization of surveillance. This research emphasizes the expanding power of Big Tech in shaping twenty-first-century borders.

Key Words: Big Tech, Digital border regimes, Global mobility, Surveillance technologies, Digital authoritarianism

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.

Introduction: Policing Borders in the Algorithmic Age

In June 2025, Los Angeles became the epicenter of a clash between federal enforcement and local protest. 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 protestors 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.

In today's increasingly digitized society, border control is not solely controlled by agents that are posted along physical walls made out of concrete and fencing, but by search engines, social media platforms, and predictive algorithms. 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 involves submitting to facial recognition technology knowingly or unknowingly in countries around the world, including the United States, Australia, and Dubai, to name just a few. The twenty-first century consists of a constant use of code, cloud servers, and biometric checkpoints as a government's tactic to control global mobility. Global mobility is in decline due to tightening immigration laws, authoritarian governments, and refugee crises. States have turned to digital technologies as a means to manage and monitor movement. 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 the powerful tech corporations, which design, own, and operate with minimal transparency. Narváez and other scholars describe this shift as "the everywhere

border," a phrase that captures how movement is increasingly regulated far beyond the physical frontier (Narváez, 2025). Mark Latonero and Paula Kift use the term "digital passages" to describe how migrants navigate systems shaped by both state and corporate actors (Latonero & Kift, 2018). The most prominent example of this model would be the Great Firewall of China. 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).

As Big Tech has started to take a more prominent role in border control and geopolitical disputes, scholarly research on this topic has been on the rise. Latonero and Kift 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 (Latonero & Kift, 2018). Similarly, E Tendayi Achiume 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 (Achiume et al., 2020). A 2024 study by Saura García calls this phenomenon "bordering by design," arguing that commercial platforms embed control logic directly into their architecture (García, 2024). Garcia also states that companies such as Palantir and Amazon have become vital to Western immigration enforcement systems while operating outside of the public eye (García, 2024). Meanwhile, the Chinese state has built a legal and technological frame 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 and his team further show how censorship and control infrastructures are expressions of political ideology as much as engineering design (Hoang et al., 2021).

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. This paper is built on ideas such as platform governance, digital sovereignty, and the decline of global mobility. José van Dijck's work in *The Platform Society* clearly mentions how tech firms have taken over infrastructural functions traditionally managed by the state (Van Dijck, 2018, p. 2). Krishnamurthy, 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 (Krishnamurthy, 2025). 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). Latonero and Kift note that refugees, while dependent on corporate platforms to move and communicate, are often unaware that these same systems are tracking, sorting, and sometimes criminalizing their movements (Latonero & Kift, 2018). 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).

This paper contributes to the literature by demonstrating that despite differences in political ideology, both the United States and China rely on comparable digital infrastructures to govern mobility. It argues that, although the United States has been historically seen as a democratic society and China has historically been considered an authoritarian regime, the two societies are now converging on platform-based sovereignty through infrastructures where commercial technologies mediate state control. It argues that historically democratic and historically authoritarian regimes are converging on platform-based sovereignty through infrastructures where commercial technologies mediate state control. The paper proceeds in five sections: it first defines the concept of digital border regimes and situates it in relation to platform power. It then outlines the theoretical framework that defines the analysis and explores U.S. corporate infrastructure. It then studies China’s Great Firewall and finally discusses the ethical and political consequences of this transformation.

Section 1: Digital Border Regimes

To understand how digital infrastructure is reshaping the governance of mobility, this section offers a critical review of the literature on digital borders, platform power, and surveillance technologies. It identifies foundational contributions to the field, highlights scholarly debates, and foregrounds the conceptual gap that this paper addresses: the need to compare how digital infrastructures function similarly across divergent political systems. This section explains the idea of "digital border regimes" and explains how borders now function through digital infrastructures, reshaping conventional ideas of space, control, and sovereignty. It contends that Big Tech platforms are not merely

instruments of border control but are the environments in which borders are enacted.

A new kind of border control has been on the rise in the twenty-first century, one that has permanently redefined borders and how they are perceived. The governance of movement is no longer constricted to existing territory, but now permeates within the multiple layers of digital space and everyday life (Narváez, 2025). Surveillance exists beyond ports of entry but through mobile phones, social media activity, and digital databases. Those being monitored have little to no clue that they are being watched. Certain states have increasingly outsourced these tasks to private companies, such as Amazon, Palantir, and Meta, since they are not bound by the same accountability as public institutions. The notion of a border must be redefined, since borders now go beyond a geographic line. This redefinition would mean the inclusion of the digital space, hence the name "Digital Border Regimes" was created (Narváez, 2025). Digital Border Regimes implicate a deeper transformation in sovereignty itself, since platforms are increasingly beginning to take on state-like functions. This section will further dissect how key theoretical terms brought to us by scholars can help us understand the rise of digital border regimes and how these systems embed power and exclusion into the architecture of digital life. These terms will also help us understand the blurred line between corporate infrastructure and state authority.

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 Narváez and other scholars, is necessary (Narváez, 2025). 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 practise migration control… While it may look like technological experimentation … the growth of digital border infrastructure is *by design*" (Narváez, 2025). 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.

A shift in the way governance is carried out is indicated by the shift from

physical borders to digital infrastructures. Private sector-developed and operated technical systems are being used more and more to handle tasks that were previously handled by state agents. According to Vivek Krishnamurthy, digital control works through "anchored infrastructure," or systems that have power through design rather than through legal authority (Krishnamurthy, 2025). Media scholar José van Dijck also emphasizes how platforms now handle infrastructure tasks like identity verification, mobility management, and public communication that were previously the purview of governments (Van Dijck, 2018, p. 16). Tech platforms are not just working for the government when they make decisions about who is visible, 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). This is referred to by Latonero and Kift as the paradox of "digital passages," a concept that describes how refugees must negotiate sociotechnical systems that both permit and restrict movement (Latonero & Kift, 2018). 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.

A fundamental shift in the way power is used in the modern world is reflected in the transition of border control from physical checkpoints to digital systems. 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 visible, 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.

Section 2: Theoretical Framework: Platform Sovereignty and Digital Infrastructure

Building on the literature reviewed above, this section outlines the theoretical framework that informs the analysis. 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 framework helps explain how structurally distinct regimes arrive at similar practices of digital border enforcement. This is problematic in that governance is thereby shifted from public oversight and accountability to opaque 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.

Section 3: Corporate Platforms as Infrastructures of Migration Enforcement

The infrastructure of contemporary migration control 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. Despite having little public 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, Palantir has long benefited from such contracts (it has been collaborating with ICE since 2011) and boasts of its "deep institutional knowledge" of immigration enforcement(Immigrant Defense Project, 2022). 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. An advocacy report notes that “Amazon’s cloud service allows ICE and DHS to collect, store, and organize a massive repository of information on immigrants, their friends and family,” ranging from biometric scans to social media data(Immigrant Defense Project, 2022). In other words, Amazon “makes billions” from contracts that feed ICE’s surveillance machine(Immigrant Defense Project, 2022).

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 Latonero and Kift 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” (Latonero & Kift, 2018). 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 one report, Silicon Valley's role in "surveillance, data accumulation, arrest, imprisonment, and deportation of immigrants" has been solidified as tech companies have established a "revolving door" with U.S. border agencies”(Immigrant Defense Project, 2022).

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, 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.

Section 4: The Great Firewall of China: Censorship, Control, and Digital Sovereignty

The Great Firewall refers to the combination of legal, technical, and political measures that China uses 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. Successive laws (notably the 2017 Cybersecurity Law and 2021 Data Security Law) require that companies, domestic and foreign, store data locally and submit to government inspections (Staff, 2024). This legal framework not only shields the domestic tech sector (fostering giants like Alibaba and Tencent by giving them favored status (Wikipedia contributors, 2025a) but also forces global firms to comply or be shut out. For example, Apple was compelled to remove apps and encrypt data for Chinese users, while companies like Microsoft and Amazon must allow state access to data centers in China (Staff, 2024). 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. A contributor to Wikipedia states, "In 2017, a Uyghur university student at Xinjiang University, Mehmut Memtimin, was sentenced to 13 years in prison for using a VPN" (Wikipedia contributors, 2025b). 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. 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 ("speech is controlled, dissent quashed" (*Great Firewall*, 2025) but also exports influence: other authoritarian states are now adopting similar tactics (sometimes even buying Chinese tech) to police information. A clear illustration of how borders now operate in cyberspace is the closed ecosystem that results from the integration of private-sector technology under public policy. In the end, China's Firewall demonstrates that digital sovereignty can be literally implemented: the state redraws the boundaries of information using its laws and technology, limiting who can see or say what, much like a nation state regulates the movement of people at its physical border(Staff, 2024).

Section 5: Ethical and Political Consequences of Digital Border Regimes

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 analysis, "it is the core… function of borders to discriminate" along racial, national, and class lines even before the advent of digital technology (Achiume, 2021). This can be made worse by digital tools. Algorithmic profiling, for instance, has a tendency 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 draws attention to the idea of "digital racial borders," in which data-driven criteria and purportedly neutral algorithms reinforce racist or xenophobic results (Achiume, 2021). 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. 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 in order 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 argue that when platform architecture “decides who is visible, 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 highlights, creating a "digital racial border" that deprives individuals of their rights in algorithmic ways (Achiume, 2021). The ethical stakes are high: technologies created without taking into account the interests of migrants 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).

Conclusion: Digital Borders, New Global Order

The digital infrastructure created by (and for) Big Tech is redrawing borders into new, ubiquitous regimes of control, according to this study. We observe software stacks, data flows, and networked devices enforcing migration policy in place of strictly physical gates. The central thesis is that as governments embrace digital sovereignty and digital infrastructure, they outsource and intensify border control in partnership with technology companies, fundamentally altering the meaning of sovereignty and human mobility. Two case studies have illustrated this dynamic. First, refugee movements now depend on and are policed by networks that blend state and corporate actors (e.g., UNHCR's biometric ID platform). These systems instantiate a new kind of infrastructure that is anchored in territory yet extends beyond it (connecting camps in one country to databases in another). Second, China's Great Firewall is a prime example of a top-down digital border. It exercises cyber-sovereignty by strategically placing state-controlled networks at the country's edge and "stopping unwanted information at its borders" (Foley, 2023). Sovereign powers can project authority into cyberspace in both situations thanks to Big Tech and digital infrastructure.

These observations have broader implications. For sovereignty, the line between state and market control is blurring: when a social media platform or AI system serves as a de facto border guard, who really holds the power? Traditional beliefs that only governments can police borders are challenged by the outsourcing of migration management to private companies. Concurrently, the emergence of national digital architectures (such as China's "internet sovereignty" laws or Europe's drive for an independent cloud and identity stack) demonstrates that governments view commanding digital space as essential to their sovereignty (Foley, 2023). The trend is concerning from a rights and liberties perspective. Digital border tools frequently worsen inequality and restrict the most vulnerable's access to basic freedoms (privacy, the right to asylum, and nondiscrimination), according to Amnesty International research (Amnesty International, 2024). The expectation of privacy within one's mobile phone or online profile is severely undermined when crossing a border requires turning over data and submitting to automated scrutiny, thereby normalizing surveillance. In effect, what was once an anomaly, demanding that migrants open their devices or bodies to inspection, is becoming routine.

These developments bring up pressing governance issues for the future. When an algorithmic border checkpoint renders an unfair decision, who bears

responsibility? How can a system developed by private companies under a government contract guarantee transparency? Public policy must grapple with the fact that digital borders are neither fully public nor private; they are hybrid zones. Democratic oversight of border technology is currently weak: for example, new regulations like the EU's AI Act have been criticized for failing to address high-risk migration applications (*AI And Surveillance at the Border – "The Technology Doesn't Actually Work at All*," 2024). There is a critical need to rethink accountability and ethics: should international norms like the right to seek asylum apply to coded decision rules as well as to guards? How do we design technology that respects mobility rather than presumes irregularity? These are not abstract questions. For example, European policymakers are already discussing how to prevent exclusion while incorporating refugees into the proposed EU Digital Identity framework (EuroStack) (Pai, 2025). Their decisions will influence not only capital and trade flows but also the actual cross-border movement of people and information.

In conclusion, software is likely to have an equal role in the future of mobility as steel. Whether a society is coming from an historically democratic tradition or an historically authoritarian tradition, the borders themselves are being rethought; they are no longer merely lines on a map but rather exist in code that is enforced by data centers and apps. There are two sides to this digitization of borders. If it were created with rights in mind, such as interoperable IDs or humane screening algorithms, it might theoretically allow for more seamless transit. However, the present course points to increased monitoring and exclusion. Therefore, the crucial realization is that our decisions regarding technology governance will determine our freedom of movement in the 21st century. Unchecked proliferation of digital walls runs the risk of establishing an all-encompassing border that impedes the very mobility it purports to regulate. On the other hand, these tools could be democratized rather than weaponized if citizens demand accountability and incorporate human rights into the foundations of digital infrastructure. The future of borders will be written in code, and it is our responsibility to make sure that code protects, not restricts, people's freedom of movement.

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

499 international frameworks, such as the right to seek asylum, should adapt to digital
500 governance practices shaped by both states and private firms.

Reference List:

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-a nd-it-discriminates?

AI and Surveillance at the Border – "The technology doesn't actually work at all." (n.d.). Weizenbaum Institut. https://www.weizenbaum-institut.de/en/news/detail/ai-and-surveillance-at-the-border-the technology-doesnt-actually-work-at-all/

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/

Anchoring Digital Sovereignty | Chicago Journal of International Law. (n.d.). https://cjil.uchicago.edu/print-archive/anchoring-digital-sovereignty

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-grea t-firewall-an-interview-with-james-griffiths/

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

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-00 397401

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*. U.S. Air University. 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). https://doi.org/10.1007/s13347-024-00777-1

Great firewall. (2025, April 11). James Griffiths. https://jamestgriffiths.com/great-firewall/

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. arXiv.org.* https://arxiv.org/abs/2106.02167

Immigrant Defense Project. (n.d.). *Amazon: Stop powering ICE's deportation machine*. https://www.immigrantdefenseproject.org/wp-content/uploads/How-Amazon-Powers-IC Es-Deportation-Machine.pdf

Kara. (2017, December 5). *For Refugees, a digital passage to Europe. Responsible Data.* https://responsibledata.io/2016/02/08/for-refugees-a-digital-passage-to-europe

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

Narváez, M. a. B. (2025, July 10). The Everywhere Border | Transnational Institute.

Transnational Institute. https://www.tni.org/en/article/the-everywhere-border

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/

Staff, I. (2024, August 20). China's digital data sovereignty laws and regulations. InCountry. https://incountry.com/blog/chinas-digital-data-sovereignty-laws-and-regulations/

Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world* [Google Books]. Oxford University Press. https://www.google.com.br/books/edition/_/H3BoDwAAQBAJ?hl=en&gbpv=1&pg=PA 1&printsec=frontcover

Wikipedia contributors. (2025a, August 7). *Great firewall*. Wikipedia. https://en.wikipedia.org/wiki/Great_Firewall

Wikipedia contributors. (2025b, August 20). Internet censorship in China. Wikipedia. https://en.wikipedia.org/wiki/Internet_censorship_in_China

Convergence Journal Review of

"Big Tech and the Rise of Digital Infrastructure on Border Control"

An interesting paper. Very creative and thoughtful. Nice work!

There are some occasional minor citation issues – you parenthetically cite Latonero and Kift but there is no information on this citation in your Reference List. This also is the case with Krishnamurthy. On Line 243 you should leave a space between the Haskins citation parentheses and the word.

In the literature review portion, the information is intriguing – it would improve the paper to engage more with the academic, peer-reviewed work out there rather than commercial news articles and Wikipedia pages. This paper does this, but enhanced use of that would improve it. For example, the concepts of "the everywhere border" and "digital passages" that your reference on Lines 70, 71 and 73 come from commercial articles – these articles might be useful – please don't think that Wikipedia sources or commercial articles can't ever be used – but for an academic piece the primary engagement should be with peer-reviewed written work, especially in the literature review portion. If these scholars did coin these terms, then it would be better to source this information from their written, peer-reviewed work. You do this well with Achiume's work. When you work with Wikipedia, you should follow their sources, not use the article itself (for example as you seem to do on Lines 329 to 330. Not a huge deal, just something to consider.

Lines 96 through 98 and 119 through 121 do an excellent job of situating your piece in the literature – this is a skill often lacking in high school research. You have identified relevant work (note my recommendations above) and have shown how you can contribute to the field. Excellent, excellent job!

Lines 121 – 128 are redundant, you can just state the contribution in one sentence once.

This is a stylistic and structural suggestion – for a paper of this size, you don't have to signpost what a section is going to do – just mention it in the introduction and then do it. For example, in Lines 134 through 144 and Line 158 you write in the future tense about what Section 1 is going to do. It's a good idea to be clear in what a paper is doing and you clearly are going for this, but with a paper that is less than 20 pages, this isn't necessary to the degree you are doing it and it can be distracting. Just a suggestion – you should ultimately write in the voice and style you think works for you.

You often do a nice job incorporating the work of others in an appropriate manner – not overusing them to the point of plagiarism or lengthiness, but also using the material in a way that contributes to your piece. One example of many is in Lines 180 through 182. You identify this concept of "anchored infrastructure", say what it is and where it comes from, and move on. This appropriate, constructive, concise use of other's work in a way that contributes to your ideas is a virtue in academic writing. Great job.

Occasionally you describe the same concepts more than once in a way that is redundant. For example, you bring up the use of refugees' unwitting subjection to digital monitoring in Lines 112 through 115. You then use almost the same wording again in Lines

190 through 193. If an idea has already been explained, consider either deleting the redundant explanation, especially when you very recently already explained it.

You occasionally bring up the idea that digital border control technologies decide who is "visible", such as on Line 207. Could you elaborate on what you mean by that?

It's a great idea to consider using subheadings the way you do. As previously mentioned, you are clearly trying to do a good job of organizing the paper in a coherent manner. However, the asymmetry of length in the sections, such as one paragraph for Section 2, does the opposite. I would recommend condensing Sections 1 and 2 into one section and removing the redundancy previously mentioned in Section 2. The theoretical framework and

There is a lot of writing on theories of accountability and responsiveness in government. In the US, you identify a particular lack of accountability that contracted companies might have because they aren't "public" in a sense. It might enhance your theory to further explain what you mean by this. What is the difference between an Amazon contract to provide data services versus Microsoft or Blackberry providing computers for other government agencies? Why does a company contracted and oversought by a federal agency have less accountability than a federal agency itself in the US example. Accountability and responsiveness generally deal with the ability of a principal to directly control the agent and to get information on performance from the agent. Since no federal bureaucrats are directly elected, they are subject to levels of removal from accountability and responsiveness. You could improve your theoretical discussion by outlining the ways you think these levels of lack of responsiveness and accountability are distinct between Palantir and ICE or a Congressional committee (or Congressional leadership). You indicate this type of thinking in Lines 273 through 279, for example. What might a "traditional democratic system", to use the term you use on Lines 278 – 279, look like? When identifying stories about cause and effect or the mechanisms thereof (which is what a theory is), it can help to go into detail where appropriate in order to provide a clearer picture for the reader to assess the theory.

Similarly, in Section 4, it might help your article to go into more detail on how Chinese bureaucracies and companies are distinct from one another. This article makes the very intriguing claim that the conventional notion that there is a major difference between technology-driven surveillance regimes in the US and China are not particularly different. And I think your article does a nice job of that, so there is a possible opportunity to provide just a bit more detail. What arm of the Chinese state or the party that controls it is subject to the same lack of oversight that US contracts are not subject to? What is the nature of this lack of oversight? Answering these questions might enhance your argument.

In Section 5, a reader might raise the obvious questions – what, if anything, is the role of the state in securing a state's borders? If there is no role, what is the role of a border? If there is no role of a border, how might advocates of alternative policy recommendations be assuaged in their concerns about security? There are many possible answers to these questions, but this piece does not address the debate in detail. This paper intelligently brings up the concepts of normalization of surveillance and the rights of refugees, but it might address some of the counterpoints in debates regarding borders and border security. Not every argument can be addressed in every paper, and not every

argument needs to be addressed, but it's worth considering whether to address some of these arguments.

Lines 385-388 make claims about rates of border phenotype error rates for facial recognition and digital processing. It would enhance the paper to cite empirical work on these claims.

The first paragraph of the conclusion beginning on Line 428 includes the claim that two case studies were examined – The China case was examined briefly, but the UNHCR biometric ID platform didn't have very detailed discussion – it would be better to talk about these as perhaps examples instead of case studies, which implies more in-depth analysis.

It might help to elaborate what you mean on Line 478 of "mobility as steel".

This paper does a nice job in the conclusion of pointing to future work that might advance the ideas presented in this paper, such as comparative studies in Europe.

Overall, this paper's idea is creative and interesting – it challenges the idea that there is a significant difference between Chinese and American digital surveillance policy regarding digital border architecture. In doing so, it brings up the ethics of human rights and ideas about democratic accountability.

I recommend an **accept with minor revisions** – address some of the citation incongruity (there are some sources in the body whose citations are not included in the Reference List section), and the minor typographical error on Line 243. You can consider revisions in substance that I have outlined here, but they aren't critical for publication in my view. The concept is creative, original, contributes and engages with the field (although I would recommend improving this), is clear enough and structured logically, writes in a way that reviews pertinent literature and theories, and is free of major grammatical, writing or typographical errors.

As a final note, I just want to reiterate that it would enhance the paper to address counterarguments to the premises and claims of this paper – in human rights ethics, there is inherently a clash with democracy because the two are not compatible in their complete forms (pure democracy says that 50.0001% of the population can vote to literally organ harvest and cannibalize the other 49.99999%, liberal-influence human rights circumscribes limits to democracy). Refugee rights are considered with views on state sovereignty, national sovereignty and citizenship. This paper doesn't address these counterpoints – perhaps it doesn't want to, but a paper that doesn't address at least a bit of the more salient counterarguments presents an opportunity to talk past the dialogue. Regardless, this was a well-done research article. Nice work!

Big Tech and the Rise of Digital Infrastructure on Border Control

Reviewer feedback

Dear author, I commend you for your timely and important choice of topic! I greatly appreciated that you are delving into the shadowy yet omnipresent role of tech companies in mediating people's lived experiences, and taking a comparative approach between the US and China in order to demonstrate the pervasiveness of this trend. There are many positive things about this paper, including your thorough incorporation of secondary literature, illustration of specific technologies and human impact, and engagement with many different angles on this topic. The level of writing and overall tone is very good in many parts.

Clarifying the central argument

In its current state, it seems that the paper is mixing 1) the ways in which technology and tech companies play outsized roles in governance (including seemingly beyond the purview of government regulation) and 2) how governments increasingly rely on technology and tech companies to exercise control. The issue is that these two angles are very related but not the same (i.e. it is one thing to focus on how a government uses tech to govern, and another to talk about how private companies are superseding the role of traditional governments). You can and should talk about both, but you need to make this distinction very clear in your definitions of the topic and the paper structure. And, if you are arguing that tech companies are taking quasi-sovereign roles, you need to indicate in your actual examples how Amazon and Palantir (and others you mention) are exercising agency akin to governments rather than just following orders and fulfilling contracts.

Framing the function of the US/China case studies

In the intro, you've projected that this paper will offer a comparison of the digital infrastructures of state control between the US and China, but I think that these are more operating as illustrative case studies of different forms of state mediation of digital infrastructure since you are not truly putting them in conversation with one another or doing much comparative analysis. I would have liked to have had the discussion of the ways in the US and China would seem to be ideologically opposed societies, including on topics such as technological regulation, but are growing increasingly similar in their deployment of surveillance technologies—this discussion is currently lacking. More plainly, how are the situations in the US and China comparable, and in which ways are they different? If you are not going to engage in this comparison, then the paper needs to be differently framed in its stated aims.

Restructuring the paper for clarity

For this paper to be maximally effective and communicative for your readers, it needs some restructuring. The intro gets a bit bogged down with literature review/background material that then is repeated later in the paper, and is conversely missing some key definitions (ICE, Big Tech, Great Firewall, etc.) which should be there from the start but are only introduced much later. Section 3 is extremely short and does not provide the "theoretical framework" which its subtitle promises; if that

is going to be an aspect of the paper, that should be introduced very early on (in the intro or section 1). While the paper promises to draw comparisons between companies based in the US and China, the latter very much feels like an afterthought. The discussion of the surveillance system in China comes very late and is not well anticipated earlier in the paper, to the point that I began to imagine how this paper could work without attempting to do the US/China comparative approach. My point is not that I think you should remove the discussion of China—as you have written in lines 97 and 119, that is supposed to be a key offering of your paper—but rather that you need to make extremely clear from the outset why you are doing this and what you are trying to demonstrate.

In order to address these problems while maintaining the stated goal of the abstract/intro, I would suggest the following approach:

Intro:

- After the first paragraph, which is a lovely (horrific) anecdote about LA, consider incorporating a parallel anecdote from China
- keep lines 54-70, and move the rest of the paragraph to a literature review section (more on that in a moment); define Big Tech
- insert a few sentences expressing how many regard the US and China as diametrically opposite when it comes to their approach to governance, but that when one examines the policing of borders and mobility for role played by Big Tech***, there are similar playbooks being used in both nations
- Lines 96-103 can stay, but 103-118 don't belong here but rather in the later lit. review in section 1
- remainder of intro—the roadmap at the end needs to accurately reflect the structure of the remainder of the paper.
    Try this paper structure:
    - Overview of digital border regimes: literature review and theoretical framework
        - Role of traditional government and increasing use of technology to govern
        - Rise of tech companies which contribute technology used for governance and even act as powerful non-state actors themselves
    - Ethical issues of this phenomenon
    - Case study 1: China
    - Case study 2: US
    - Analysis of the similarities/differences of the US/China digital border regimes and their implications/consequences
    - Conclusion
- Intro also needs a methodology and to mention the sorts of sources which the paper relies on

Section 1: (rename sections without the words "Section 1")

- the first paragraph is a bit repetitive, but a streamlined version would be better placed in the roadmap of the intro

- start this section with paragraph 2 on line 145. Incorporate the literature review material from the intro in this section
- Lines 158-162: announcements of what each section will do would be better incorporated into the intro rather than the section itself--we are now reading the section, so you don't need to announce what it "will" do (but you should have strong thesis sentences for paragraphs! Line 163 is an example of where you have done this well)
- roughly towards the end of this section, you can incorporate the literature review bits from lines 103-108

Section 2:

- Move this to the intro after line 103

Sections 3 & 4: potentially could be combined, consider changing order

- As many of the aspects of the digital border regimes you mention in China predate those in the US, consider moving the Chinese case study before the US one
- Both sections require clearer discussions of the relationship between the government and private companies (again, this is why it's important to define "Big Tech" and show how that can entail very different power flows in different national contexts
- Given that your point is that there are striking resemblances between the situations of the US and China, there needs to be a thorough discussion of at least a paragraph or more which reflects on these similarities and what they imply about a growing global phenomenon towards digital governance (with outsized roles played by non-state actors in many cases)

Section 5:

- Move after Section 1: this seems to be a broader evaluation of the ethics of digital border regimes rather than specific to your US/China case studies and thus better suited earlier in the paper

Conclusion:

- Revise to reflect adapted aims and structure of the paper; notice that the "stated goals" put forth in the intro and conclusion currently don't match in terms of their focus
    - Intro: "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."
    - Conclusion: "The central thesis is that as **governments** embrace digital sovereignty and digital infrastructure, they **outsource and intensify border control in partnership with technology companies**, fundamentally altering the meaning of sovereignty and human mobility."

Other feedback:

- The term “Big Tech” seems to be used in this paper to refer to many different types of large companies whose products and features play certain roles in the policing of society AND the technologies themselves (including those which are primarily in the hands of governmental actors, such as the Great Firewall initiated and regulated by the Chinese state). You need to very clearly define how you are using the term Big Tech; you also need to indicate how varying levels of government involvement in Big Tech are similar or different in the US/Chinese contexts
- Citations: if you include the name of the author(s) in the sentence, you do not need to put their names in the citation’s parentheses, but can rather just put the year immediately after their name
    - like this: *For example, **"Latonero and Kift (2018)** comment on how...*
- There is a tendency to write “this paper does this” and “this paper will do that” throughout your paper. This is fine for the abstract and the roadmap of the intro, but in the body of the paper, I would avoid this phrase… at that point, show it, don’t say it. (For example, Section 1 works better when you start directly with paragraph 2!)
- Wikipedia, although it can be useful for informing oneself on an unfamiliar topic, is not a recommended source to cite in an academic paper

Some other comments…

Lines	**Comment**
6-11	Assume an educated but unfamiliar reader: specify a timeframe, geography, and what ICE stands for in the first instance. While this is probably evident to an American reader, imagine that this is being read 10 years from now by someone in a different country—we would want your paper to be intelligible to them as well. Consider also defining what is entailed by your use of the term “Big Tech”—do you refer to companies or technologies or both?
16	The companies are not acting as digital border regimes, but perhaps creating/enact/mediating the infrastructure of digital border regimes
18-20	“While scholars…” If scholars are framing tech firms as geopolitical actors, it is not a contradiction (as the term “while” suggests) to point out that their work is political.
1-28	Abstract would benefit from a statement about what sorts of sources precisely will be examined in the paper to make these assessments—a methodology statement
41	Define “ICE” the first time
55	not "that are" but "who are," or better yet delete
61	delete "around the world,"
70	delete "and other", and Narvaez needs a first name
75	briefly define the Great Firewall of China for the unfamiliar reader; "scholar" should not be capitalized

69	somewhere around here would be a good time to define how you are using the term "Big Tech" in the body of the paper. There are also very different types of companies you imply as contained under this umbrella (Amazon and Palantir are very different companies on the surface!) so please explain what you see as their commonalities for the purposes of this analysis
78-79	This sentence could be slightly more elegantly worded and more importantly provide a much stronger topic sentence for the material contained in the paragraph
Throughout paper (for example, 82)	Please note that if you are mentioning an author's name in the text, you can just stick the remainder of the citation immediately after their mention. For example, "Latonero and Kift (2018) comment on how..."
90-91	as above, please briefly explain how China has done this
94	"and his team" is strange wording; use et al and then cite with just the year in-text
134-144	This first paragraph gets a bit repetitive, especially after the "roadmap" of the intro--vary the language by moving away from "this section does this" (this is not bad, but not for every sentence!); I think this entire paragraph could be condensed and incorporated in the intro. Then you could open with the para. which starts on line 145
156	why is "Digital Border Regimes" capitalized?
Section 2	Does not need to be its own section
73 and 194	repetition of same material (hence the suggestion to move it down from the intro and consolidate)
241	ICE finally gets defined here
252	It's fine to use an advocacy report, but the report itself has no sources; look for another stronger source to support your claim about Amazon's earnings from contracts
312 and 327	Find non-Wikipedia sources
341	what is a splinternet?
429	delete "according to this study"
482-483	replace "it" with more specific referant
491	who is the "our" or "our responsibility"?
508	Source not properly cited (missing author, date, etc.) - they are in the top/bottom of article
518	Source not properly cited (missing author, date, etc.)
568	In addition to the Wikipedia sources, please look for a stronger source than the InCountry Staff one

I hope that this “instruction manual” is, well, instructive and helpful. Again, I congratulate you on your fine work! If you can move things around to improve the flow of the paper, it will shine through more clearly and make for a valuable contribution to the publication.

Reviewer recommendation: revise and resubmit

Big Tech and the Rise of Digital Infrastructure in Border Control

[Author name redacted by Managing Editor]
[Program name redacted by Managing Editor]
[School name redacted by Managing Editor]

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: controlling migrant populations. 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

Acknowledgements

I would like to express my sincere gratitude to [mentor name redacted by Managing Editor] in [department name redacted by Managing Editor] at [school name redacted by Managing Editor], and to [mentor name redacted by Managing Editor] in the [department name redacted by Managing Editor]at [school name redacted by Managing

Editor], for their invaluable mentorship and guidance through [program redacted by Managing Editor]. Their insights, encouragement, and critical feedback were instrumental in shaping the direction and depth of this research.

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 protestors 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 operate 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 collecting 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 out 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 a constant use of code, cloud servers, and biometric checkpoints as a government's tactic 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, 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 moniker 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 if 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.

The Rise of Digital Border Regimes

It is evident that governments are increasingly using technology to govern. An example of this is that the governance of movement is no longer constricted to existing territory, but now permeates within 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 practise 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, who 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.

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. Garcia (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 frame 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.

Ethical and Political Consequences of Digital Border Regimes

Traditionally, the role of states in border security is seen as protecting national sovereignty through controlling movement across borders of people and resources. 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…" Yet, the question arises: how far should this commonly accepted role of the state go before it impedes on 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. This can be made worse by digital tools. Algorithmic profiling, for instance, has a tendency 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 labelled ‘Black women’ 20 times more frequently than images labelled ‘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 in order 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 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 migrants 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).

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

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 the 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.

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. By building "cyberspatial ramparts" to regulate online flows, it 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).

Analysis of Similarities and Differences in 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 a 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 keep an eye on, 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 beings 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 digital and the physical are inextricably linked is what connects them rather than their ideology.

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 migration 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 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 partially share 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. More and more, 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 demanding access to personal devices or communication records, are now commonplace components of border screening. Data becomes a condition of mobility, 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 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. These judgments, once ingrained in infrastructure, follow migrants across institutions, service providers, and countries, influencing how they are treated long after they cross the border. In this situation, technology is not neutral; rather, it actively influences how migration and protection 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.

Reference List

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-a nd-it-discriminates?

Weizenbaum Institut. (n.d.). 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/

Alsabah, Nabil. (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-grea t-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-00 397401

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

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*. U.S. Air University. 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). https://doi.org/10.1007/s13347-024-00777-1

James Griffiths. (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. (2020, April 2). Amazon is the invisible backbone of 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*. *arXiv.org*. https://arxiv.org/abs/2106.02167

Israel, Tamir, *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond* (September 30, 2020). Samuelson-Glushko Canadian Internet Policy

& Public Interest Clinic (CIPPIC), 2020, Available at SSRN: https://ssrn.com/abstract=3714297

Kara. (2017, December 5). *For Refugees, a digital passage to Europe. Responsible Data.* https://responsibledata.io/2016/02/08/for-refugees-a-digital-passage-to-europe

Krishnamurthy, Vivek. (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). https://doi.org/10.1177/2056305118764432

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

Office of the United Nations High Commissioner for Human Rights (OHCHR). (2022). OHCHR assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China. In *OHCHR.org*. Retrieved November 9, 2025, from 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). 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. (2025, June 4). 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* [Google Books]. Oxford University Press.

https://www.google.com.br/books/edition/_/H3BoDwAAQBAJ?hl=en&gbpv=1&pg=PA 1&printsec=frontcover

Wee, S.-L. (2017). China's New Cybersecurity Law Leaves Foreign Firms Guessing Share full article. *The New York Times*. https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html#

Peer Reviewer 1 Feedback

- There are some occasional minor citation issues – you parenthetically cite Latonero and Kift but there is no information on this citation in your Reference List. This also is the case with Krishnamurthy.
  Reply: I corrected the citation entries and ensured Latonero and Kift, as well as Krishnamurthy, are fully included in the reference list.

- On Line 243 you should leave a space between the Haskins citation parentheses and the word.
  Reply: I adjusted the formatting to include the proper spacing after the Haskins citation.

- In the literature review portion, the information is intriguing – it would improve the paper to engage more with the academic, peer-reviewed work out there rather than commercial news articles and Wikipedia pages. This paper does this, but enhanced use of that would improve it.
  For example, the concepts of "the everywhere border" and "digital passages" that you reference on Lines 70, 71 and 73 come from commercial articles – these articles might be useful – please don't think that Wikipedia sources or commercial articles can't ever be used – but for an academic piece the primary engagement should be with peer-reviewed written work, especially in the literature review portion. If these scholars did coin these terms, then it would be better to source this information from their written, peer-reviewed work. You do this well with Achiume's work. When you work with Wikipedia, you should follow their sources, not use the article itself (for example as you seem to do on Lines 329 to 330). Not a huge deal, just something to consider.
  Reply: I have gone through the sources used, and replaced the wikipedia sources with academic articles. In regards to the other sources (ex: "the everywhere border" and "digital passages"), I double checked and these terms were sourced from a paper published by a research institute and a peer-reviewed article, respectively. I believe that these citations are satisfactory.

- Lines 121 – 128 are redundant, you can just state the contribution in one sentence once.
  Reply: I condensed these lines by stating the contribution once in a concise sentence.

- This is a stylistic and structural suggestion – for a paper of this size, you don't have to signpost what a section is going to do – just mention it in the introduction and then do it. For example, in Lines 134 through 144 and Line 158 you write in the future tense about what Section 1 is going to do. It's a good idea to be clear in what a paper is doing and you clearly are going for this, but with a paper that is less than 20 pages, this isn't necessary to the degree you are doing it and it can be distracting. Just a suggestion –

you should ultimately write in the voice and style you think works for you.
Reply: I removed forward-looking language that explicitly announces section content and streamlined transitions for smoother flow.

- Occasionally you describe the same concepts more than once in a way that is redundant. For example, you bring up the use of refugees' unwitting subjection to digital monitoring in Lines 112 through 115. You then use almost the same wording again in Lines 190 through 193. If an idea has already been explained, consider either deleting the redundant explanation, especially when you very recently already explained it.
Reply: I removed repetitive phrasing in these lines and consolidated the discussion into a single instance for clarity.

- You occasionally bring up the idea that digital border control technologies decide who is "visible", such as on Line 207. Could you elaborate on what you mean by that?
Reply: I removed the "visibility" phrasing and replaced it with more precise wording to avoid ambiguity.

- It's a great idea to consider using subheadings the way you do. As previously mentioned, you are clearly trying to do a good job of organizing the paper in a coherent manner. However, the asymmetry of length in the sections, such as one paragraph for Section 2, does the opposite. I would recommend condensing Sections 1 and 2 into one section and removing the redundancy previously mentioned in Section 2.
Reply: I combined the content from Sections 1 and 2 and removed redundant material to improve balance and cohesion.

- There is a lot of writing on theories of accountability and responsiveness in government. In the US, you identify a particular lack of accountability that contracted companies might have because they aren't "public" in a sense. It might enhance your theory to further explain what you mean by this. What is the difference between an Amazon contract to provide data services versus Microsoft or Blackberry providing computers for other government agencies? Why does a company contracted and oversought by a federal agency have less accountability than a federal agency itself in the US example? Accountability and responsiveness generally deal with the ability of a principal to directly control the agent and to get information on performance from the agent. Since no federal bureaucrats are directly elected, they are subject to levels of removal from accountability and responsiveness. You could improve your theoretical discussion by outlining the ways you think these levels of lack of responsiveness and accountability are distinct between Palantir and ICE or a Congressional committee (or Congressional leadership). You indicate this type of thinking in Lines 273 through 279, for example. What might a "traditional democratic system," to use the term you use on Lines 278–279, look like? When identifying stories about cause and effect or the mechanisms thereof (which is what a theory is), it can help to go into detail where appropriate in order to provide a clearer picture for the reader to assess the theory.
Reply:I expanded the discussion of accountability by explaining differences

between public agencies and contracted private firms, providing examples such as Palantir and ICE and clarifying characteristics of traditional democratic oversight.

- Similarly, in Section 4, it might help your article to go into more detail on how Chinese bureaucracies and companies are distinct from one another. This article makes the very intriguing claim that the conventional notion that there is a major difference between technology-driven surveillance regimes in the US and China are not particularly different. And I think your article does a nice job of that, so there is a possible opportunity to provide just a bit more detail. What arm of the Chinese state or the party that controls it is subject to the same lack of oversight that US contracts are not subject to? What is the nature of this lack of oversight? Answering these questions might enhance your argument.
  Reply: I expanded the China section to explain the structure and oversight mechanisms between state bodies and major technology companies, clarifying where accountability gaps emerge.

- In Section 5, a reader might raise the obvious questions – what, if anything, is the role of the state in securing a state's borders? If there is no role, what is the role of a border? If there is no role of a border, how might advocates of alternative policy recommendations be assuaged in their concerns about security? There are many possible answers to these questions, but this piece does not address the debate in detail. This paper intelligently brings up the concepts of normalization of surveillance and the rights of refugees, but it might address some of the counterpoints in debates regarding borders and border security. Not every argument can be addressed in every paper, and not every argument needs to be addressed, but it's worth considering whether to address some of these arguments.
  Reply: I added discussion of security-oriented perspectives and the role of the state in regulating borders, acknowledging competing arguments and situating refugee rights within sovereignty debates.

- Lines 385–388 make claims about rates of border phenotype error rates for facial recognition and digital processing. It would enhance the paper to cite empirical work on these claims.
  Reply: I added empirical sources that document differential error rates in facial recognition and digital processing of border subjects.

- The first paragraph of the conclusion beginning on Line 428 includes the claim that two case studies were examined – The China case was examined briefly, but the UNHCR biometric ID platform didn't have very detailed discussion – it would be better to talk about these as perhaps examples instead of case studies, which implies more in-depth analysis.
  Reply: I revised the conclusion to refer to the U.S. and China examples as

illustrative cases rather than formal case studies.

- It might help to elaborate what you mean on Line 478 of “mobility as steel.”
  Reply: I clarified the metaphor by explaining how digital systems rigidify mobility pathways and restrict movement through infrastructural controls.

- This paper does a nice job in the conclusion of pointing to future work that might advance the ideas presented in this paper, such as comparative studies in Europe.

- Overall, this paper’s idea is creative and interesting – it challenges the idea that there is a significant difference between Chinese and American digital surveillance policy regarding digital border architecture. In doing so, it brings up the ethics of human rights and ideas about democratic accountability.

- I recommend an accept with minor revisions – address some of the citation incongruity (there are some sources in the body whose citations are not included in the Reference List section), and the minor typographical error on Line 243. You can consider revisions in substance that I have outlined here, but they aren’t critical for publication in my view. The concept is creative, original, contributes and engages with the field (although I would recommend improving this), is clear enough and structured logically, writes in a way that reviews pertinent literature and theories, and is free of major grammatical, writing or typographical errors.

- As a final note, I just want to reiterate that it would enhance the paper to address counterarguments to the premises and claims of this paper – in human rights ethics, there is inherently a clash with democracy because the two are not compatible in their complete forms (pure democracy says that 50.0001% of the population can vote to literally organ harvest and cannibalize the other 49.99999%; liberal-influence human rights circumscribes limits to democracy). Refugee rights are considered with views on state sovereignty, national sovereignty and citizenship. This paper doesn’t address these counterpoints – perhaps it doesn’t want to, but a paper that doesn’t address at least a bit of the more salient counterarguments presents an opportunity to talk past the dialogue.
  Reply: I incorporated a brief discussion acknowledging tensions between democratic sovereignty and human rights principles, and highlighted how these tensions shape refugee protection and migration governance debates.

Peer Reviewer 2 Feedback

- Clarifying the central argument
  In its current state, it seems that the paper is mixing 1) the ways in which technology and tech companies play outsized roles in governance (including seemingly beyond the purview of government regulation) and 2) how governments increasingly rely on technology and tech companies to exercise control. The issue is that these two angles are very related but not the same (i.e. it is one thing to focus on how a government uses tech to govern, and another to talk about how private companies are superseding the role of traditional governments). You can and should talk about both, but you need to make this distinction very clear in your definitions of the topic and the paper structure.
  Reply: I revised the introductory framing and the theoretical section to clearly distinguish between state use of technology for governance and the growing quasi-sovereign authority exercised by private firms. The paper now outlines these as interconnected but distinct dynamics.

- And, if you are arguing that tech companies are taking quasi-sovereign roles, you need to indicate in your actual examples how Amazon and Palantir (and others you mention) are exercising agency akin to governments rather than just following orders and fulfilling contracts.
  Reply: I added analysis demonstrating how Amazon and Palantir shape enforcement practices through proprietary systems and design choices, emphasizing their independent decision-making power and influence over mobility governance rather than simple contract compliance.

- Framing the function of the US/China case studies
  In the intro, you've projected that this paper will offer a comparison of the digital infrastructures of state control between the US and China, but I think that these are more operating as illustrative case studies of different forms of state mediation of digital infrastructure since you are not truly putting them in conversation with one another or doing much comparative analysis. I would have liked to have had the discussion of the ways in the US and China would seem to be ideologically opposed societies, including on topics such as technological regulation, but are growing increasingly similar in their deployment of surveillance technologies—this discussion is currently lacking.
  Reply: I added an analysis section to explicitly compare the US and China, underlining shared logics and structural differences while situating the cases as illustrative of convergent digital governance trends.

- More plainly, how are the situations in the US and China comparable, and in which ways are they different? If you are not going to engage in this comparison, then the paper needs to be differently framed in its stated aims.
  Reply: I strengthened the introduction to explain why the US and China serve as meaningful contrasts and added discussion on how their approaches converge

despite divergent political systems.

- Restructuring the paper for clarity
  For this paper to be maximally effective and communicative for your readers, it needs some restructuring. The intro gets a bit bogged down with literature review/background material that then is repeated later in the paper, and is conversely missing some key definitions (ICE, Big Tech, Great Firewall, etc.) which should be there from the start but are only introduced much later.
  Reply: I reorganized the introduction to include key definitions (Big Tech, ICE, Great Firewall) up front and shifted extended literature review segments into a dedicated literature review section.

- Section 3 is extremely short and does not provide the "theoretical framework" which its subtitle promises; if that is going to be an aspect of the paper, that should be introduced very early on (in the intro or section 1).
  Reply: I moved the theoretical framework into the early literature review and expanded it to ground later sections.

- While the paper promises to draw comparisons between companies based in the US and China, the latter very much feels like an afterthought. The discussion of the surveillance system in China comes very late and is not well anticipated earlier in the paper, to the point that I began to imagine how this paper could work without attempting to do the US/China comparative approach. My point is not that I think you should remove the discussion of China—as you have written in lines 97 and 119, that is supposed to be a key offering of your paper—but rather that you need to make extremely clear from the outset why you are doing this and what you are trying to demonstrate.
  Reply: I incorporated references to China in the introduction and literature review to foreshadow its importance and avoid the "afterthought" effect.

In order to address these problems while maintaining the stated goal of the abstract/intro, I would suggest the following approach:

Intro:

- After the first paragraph, which is a lovely (horrific) anecdote about LA, consider incorporating a parallel anecdote from China
  Reply: I incorporated a parallel anecdote from Xinjiang immediately following the LA example to frame the global relevance of digital enforcement across democratic and authoritarian contexts.

- keep lines 54-70, and move the rest of the paragraph to a literature review section (more on that in a moment); define Big Tech
  Reply: I retained the foundational framing while moving the background discussion into the literature review and added a clear definition of Big Tech early

in the introduction.

- insert a few sentences expressing how many regard the US and China as diametrically opposite when it comes to their approach to governance, but that when one examines the policing of borders and mobility for role played by Big Tech***, there are similar playbooks being used in both nations
  Reply: In the new section I created, "Analysis of Similarities and Differences in US and China Digital Border Regimes," it is emphasized that although the US and China are typically viewed as ideologically opposed, both increasingly rely on similar digital surveillance architectures through Big Tech involvement.

- Lines 96-103 can stay, but 103-118 don't belong here but rather in the later lit. review in section 1
  Reply: I relocated the theoretical context originally in this section to the expanded literature review, where it now anchors the conceptual framework.

- remainder of intro—the roadmap at the end needs to accurately reflect the structure of the remainder of the paper.
  Reply: I revised the roadmap to accurately reflect the reorganized structure, including the shift to a dedicated literature review, early ethics discussion, and comparative case analysis.

Try this paper structure:
Overview of digital border regimes: literature review and theoretical framework
Role of traditional government and increasing use of technology to govern
Rise of tech companies which contribute technology used for governance and even act as powerful non-state actors themselves

Ethical issues of this phenomenon
Case study 1: China
Case study 2: US
Analysis of the similarities/differences of the US/China digital border regimes and their implications/consequences
Conclusion
Intro also needs a methodology and to mention the sorts of sources which the paper relies on

Section 1:

- (rename sections without the words "Section 1")
  Reply: I agree with and implemented this change to my paper.

- the first paragraph is a bit repetitive, but a streamlined version would be better placed in the roadmap of the intro
  Reply: I agree with and implemented this change to my paper.

- start this section with paragraph 2 on line 145. Incorporate the literature review material from the intro in this section
  Reply: I reorganized the opening of Section 1 and placed the literature review into its own new section at the appropriate position in the paper.

- Lines 158-162: announcements of what each section will do would be better incorporated into the intro rather than the section itself--we are now reading the section, so you don't need to announce what it "will"; do (but you should have strong thesis sentences for paragraphs! Line 163 is an example of where you have done this well)
  Reply: I agree with and implemented this change to my paper.

- roughly towards the end of this section, you can incorporate the literature review bits from lines 103-108
  Reply:

Section 2:

- Move this to the intro after line 103
  Reply: I merged the theoretical framing originally in Section 2 into the introduction and literature review for earlier conceptual grounding.

Sections 3 and 4:

- potentially could be combined, consider changing order
  Reply: I merged sections 3 and 4, and created subsections to maintain clarity.

- As many of the aspects of the digital border regimes you mention in China predate those in the US, consider moving the Chinese case study before the US one
  Reply: I evaluated switching sections but kept the U.S. case first to maintain argumentative flow

- Both sections require clearer discussions of the relationship between the government and private companies (again, this is why it's important to define "Big Tech" and show how that can entail very different power flows in different national contexts
  Reply: I expanded analysis of accountability structures and power dynamics in both contexts, emphasizing divergent state–platform relationships.

- Given that your point is that there are striking resemblances between the situations of the US and China, there needs to be a thorough discussion of at least a paragraph or more which reflects on these similarities and what they imply about a growing global phenomenon towards digital governance (with outsized roles played by non-state actors in many cases)
  Reply: I created a dedicated comparative analysis section that explains both similarities and differences in U.S. and Chinese digital border logics.

Section 5:

- Move after Section 1: this seems to be a broader evaluation of the ethics of digital border regimes rather than specific to your US/China case studies and thus better suited earlier in the paper
  Reply: I repositioned the ethical and political implications section before the case studies.

Conclusion:

- Revise to reflect adapted aims and structure of the paper; notice that the "stated goals" put forth in the intro and conclusion currently don't match in terms of their focus - Intro: "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." Conclusion: "The central thesis is that as governments embrace digital sovereignty and digital infrastructure, they outsource and intensify border control in partnership with technology companies, fundamentally altering the meaning of sovereignty and human mobility."
  Reply: I revised the conclusion to explicitly mirror the argument introduced at the beginning, stressing quasi-sovereign private power and convergent state practices.

Other feedback:

- The term "Big Tech" seems to be used in this paper to refer to many different types of large companies whose products and features play certain roles in the policing of society AND the technologies themselves (including those which are primarily in the hands of governmental actors, such as the Great Firewall initiated and regulated by the Chinese state). You need to very clearly define how you are using the term Big Tech; you also need to indicate how varying levels of government involvement in Big Tech are similar or different in the US/Chinese contexts
  Reply: Big Tech is now defined in the 2nd sentence of the abstract as "the world's largest and most influential technology companies". The paper now does a better job of describing how the US government outsources much of the enforcement to

US corporations while China uses legal, technical and political measures to involve Chinese Big Tech in enforcement.

Citations:

- if you include the name of the author(s) in the sentence, you do not need to put their names in the citation's parentheses, but can rather just put the year immediately after their name like this: For example, "Latonero and Kift (2018) comment on how…"
  Reply: I agree with and implemented this change to my paper.

- There is a tendency to write "this paper does this" and "this paper will do that" throughout your paper. This is fine for the abstract and the roadmap of the intro, but in the body of the paper, I would avoid this phrase… at that point, show it, don't say it. (For example, Section 1 works better when you start directly with paragraph 2!)
  Reply: I agree with and implemented this change to my paper.

- Wikipedia, although it can be useful for informing oneself on an unfamiliar topic, is not a recommended source to cite in an academic paper
  Reply: I removed all Wikipedia citations and replaced them with academic sources or reputable journalistic publications.

More Feedback:

- Lines 6 to 11: Assume an educated but unfamiliar reader. Specify timeframe, geography, and what ICE stands for the first time. Consider defining "Big Tech" here too.
  Reply: I removed ICE anecdote in the abstract due to word limit, but mentioned what ICE stands for and the definition of Big Tech at their first appearance.

- Line 16: Companies are not acting as digital border regimes, but rather creating or mediating the infrastructure of digital border regimes.
  Reply: I revised the sentence to clarify that companies are mediating digital border infrastructures rather than functioning as border regimes themselves.

- Lines 18 to 20: If scholars frame tech firms as geopolitical actors, it does not contradict the point that their work is political. Adjust wording.
  Reply: I agree with and implemented this change to my paper.

- Lines 1 to 28 (Abstract): Add a brief methodology. Specify what kinds of sources you will examine.
  Reply: I added a brief methodology sentence explaining that the paper draws on academic literature and reputable media reports.

- Line 41: Define ICE on first use.
  Reply: I now spell out Immigration and Customs Enforcement (ICE) at first mention.

- Line 55: Use “who are” instead of “that are,” or remove entirely.
  Reply: I agree with and implemented this change to my paper.

- Line 61: Remove “around the world.”
  Reply: I agree with and implemented this change to my paper.

- Line 70: Remove “and other.” Add first name for Narvaez.
  Reply: I agree with and implemented this change to my paper.

- Line 75: Briefly define the Great Firewall of China; “scholar” should not be capitalized.
  Reply: I added a brief definition of the Great Firewall of China and corrected “scholar” to lowercase.

- Line 69 (general spot in intro): Define the term “Big Tech” clearly, since companies like Amazon and Palantir differ significantly. Explain what they share for your purposes.
  Reply: I explicitly defined Big Tech as “the world’s largest and most influential technology companies” and explained the shared infrastructural power that connects firms like Amazon, Palantir, Tencent, and Alibaba.

- Lines 78 to 79: Strengthen topic sentence for clarity and flow.
  Reply: I agree with and implemented this change to my paper.

- Throughout (for example, line 82): If mentioning an author’s name in the sentence, place only the year in parentheses immediately after the name.
  Reply: I agree with and implemented this change to my paper.

- Lines 90 to 91: Briefly explain how China has implemented similar systems.
  Reply: I removed this anticipatory sentence because later paragraphs fully address China’s model, making this clarification unnecessary.

- Line 94: Replace “and his team” with “et al.” and cite with just the year.
  Reply: I agree with and implemented this change to my paper.

- Lines 134 to 144: This paragraph is repetitive after the intro roadmap; consider condensing and integrating.
  Reply: I deleted this paragraph and integrated necessary information elsewhere to avoid repetition.

- Line 156: Do not capitalize “digital border regimes.”
  Reply: I agree with and implemented this change to my paper.

- Section 2: Does not need to be its own section.
  Reply: I merged this content into the introduction and theoretical framing instead of treating it as its own section.

- Lines 73 and 194: Avoid repeating the same material. Consolidate.
  Reply: I eliminated duplicative phrasing and consolidated overlapping content.

- Line 241: ICE is finally defined here; move earlier.
  Reply: I moved the ICE definition to its first appearance near the beginning.

- Line 252: Replace advocacy report with a stronger source that contains citations, especially regarding Amazon’s earnings from contracts.
  Reply: I replaced the advocacy citation with verified reporting, including sources like *The Guardian*.

- Lines 312 and 327: Do not cite Wikipedia; find stronger academic or journalistic sources.
  Reply: I eliminated Wikipedia references and substituted peer-reviewed or established journalistic sources.

- Line 341: Define “splinternet.”
  Reply: I agree with and implemented this change to my paper.

- Line 429: Remove “according to this study.”
  Reply: I agree with and implemented this change to my paper.

- Lines 482 to 483: Replace “it” with a more specific noun.
  Reply: I agree with and implemented this change to my paper.

- Line 491: Clarify who “our” refers to.
  Reply: I clarified the referent for “our” to eliminate ambiguity.

- Line 508: Source missing author and date.
  Reply: I provided the author, but there is no date on the source.

- Line 518: Source missing author and date.
  Reply: I provided author and date to citation.

- Line 568: Replace Wikipedia and “InCountry Staff” source with stronger sources.
  Reply: I eliminated Wikipedia and “InCountry Staff” references and substituted with peer-reviewed or established journalistic sources.

Convergence Journal Review of

"Big Tech and the Rise of Digital Infrastructure in Border Control"

I recommend **accept as is.** The author has acceptably considered revision recommendations. The article is original, interesting, clear, coherent, uses research at an acceptable level for high school, and is written using grammatically correct and polished writing.

The introduction and setup do an effective job at identifying a puzzle of seemingly antithetical governmental systems behaving similarly when it comes to their use of electronic surveillance, the conclusion points to further research and the body sections and argument mostly convey a coherent thesis.

With this in mind, there are some recommendations to keep in mind for possible further research in the future:

In response to Peer Reviewer 2's Feedback recommendation that you should clearly distinguish between how technology and tech companies play an outsized role in governance and how governments increasingly rely on technology and tech companies to exercise control, the author claims that they revised the introduction and theory sections to address this. Peer Reviewer 1 also recommended more specificity about why contracted technology companies are less accountable than a government bureaucracy, party leadership or other non-directly elected elements of governance. The writer addressed these briefly in the new version in its US Case section and did a much improved job of identifying the legal limitations of, for example, FOIA requests over a contracted company compared to a federal agency.

There is a deeper philosophical tension underlying this paper, which need not be the focus of this paper but can be a consideration for future writing and research: if state sovereignty is subject to the limitations of human rights, where do human rights come from? If they are objective, what are they and where do they come from? If they are subjective, then what prevents a powerful state (US or China for example) from invading under the pretense of their framework of human rights? Similarly, there is a claim that normalizing surveillance erodes democracy. Is democracy unable to select increased surveillance? What other choices is a democracy not allowed to select as a group? If there are limitations on group choices, what are those, and why should those limitations exist?

Peer Reviewer 2's recommendation to consider counterarguments to this paper's normative claims have largely been undeveloped. This is fine – papers are not expected to necessarily address counterclaims much less focus on them. However, the claim of states towards sovereignty and security and the claims of migrants and refugees to the same can be in tension with one another, and the paper does not address this tension or demonstrate awareness of it.

Finally, this paper does a nice job of presenting a coherent argument. One minor thing to consider for improvement in the future is that the abstract says this paper's argument is that both China and the US use similar digital architectures to control migrant populations. However, the China case study focuses on China's digital sovereignty as it applies to policing the internet. The thesis seems to begin one way but end another. In the end, the takeaway seems to be that two nominally distinct government types both rely on technology to establish digital sovereignty, but the main thesis is slightly difficult to follow.

Nice work!