Data Trafficking and the International Risks of Surveillance Capitalism:
The Case of Grindr and China

Abstract

This article offers a framework to discuss when a community’s data is moved abroad without their informed consent, a practice I term data trafficking. I analyze Grindr, an LGBTQIA+ dating platform that has changed hands between China and the United States to demonstrate what data trafficking is, how it undermines national sovereignty, and how it erodes human rights. In the United States, corporate policies are the leading indicator for data governance practices, influencing a system known as multi-stakeholderism (DeNardis, 2013). In China, forced localization to government servers drives data governance practices (Mueller, 2017; Zeng et al., 2017; Kokas, 2018; Kokas, 2019; Kokas, 2022). This article extends how we think about transnational consumer data security by examining how weak data security designed to support the growth of Silicon Valley firms amplifies the capacity of extra-territorial data governance practices asserted by the Chinese government.
1. Introduction.

Since 2013, when Edward Snowden and reporters from The Guardian and Washington Post revealed practices of ‘dataveillance,’ or the leveraging of US corporate data gathering about US, UK, and Brazilian citizens, scholars have tried to understand how we are tracked online and where that data goes (Lyon 2016, 2015, 2014a; Seemann 2015). Following the Snowden revelations, sociologist David Lyon argued that despite data aggregation, users are ‘so far from conforming to the abstract, disembodied image of both computing and legal practices’ (Lyon 2014a, 1). Yet, as users remain on the platforms, they are also increasingly ‘known’ by those platforms (Gillespie 2014).

The objective of this article is to offer a framework for analyzing the implications of when a community’s data is moved abroad without their informed consent. How do we conceive of security violations of aggregated data when this data crosses borders? I argue that this movement of personal data across borders without fully informed consent, a practice I term data trafficking, is akin to human trafficking but in the form of a data security practice. While the consequences of data trafficking are not as direct as that of human trafficking, data trafficking similarly stems from users entering into an exploitative agreement when they share their data and reflects the ways in which data can also increasingly be tied back to the human body and experience.

I use the case of Grindr, an LGBTQIA+ dating platform which changed ownership between firms in the United States and China and then back again, to demonstrate what data trafficking is, how it undermines national sovereignty, and how it erodes human rights. Grindr exemplifies the challenges of regulating user data movement between the system of laissez-faire data governance like that in the US to one with extensive government oversight as
The Grindr case stands out because it underscores how it is impossible to rectify damage after data has been gathered and moved abroad, particularly with sensitive data such as personal images or sexual content. Once data has been moved across borders, the possibilities for retrieval diminish perilously. The Grindr case underscores the importance of protecting sensitive data when it moves across borders due to differing legal protections. The rights of LGBTQIA+ communities globally differ by country. Those rights often do not align with the protections for user data. For example, in the United States, legal protections for the LGBTQIA+ community domestically far outstrip protections for their data. LGBTQIA+ individuals in China, by contrast, have few legal rights, but China offers much more robust data protections for users from Chinese corporations (though not necessarily from the Chinese government). I thus analyze the case of Grindr to theorize data trafficking.

The data of individuals alone is not necessarily revealing, but all data can be sensitive when combined as part of a profile in what scholars term “mosaic theory” (Kerr 2012), the idea that individual types of data may not be particularly useful to create products, map a community, or develop a profile of an individual, but when combined at scale can be highly impactful. While the Grindr case is particularly evocative, it is only one part of a larger data trafficking landscape that includes everything from telecommunications infrastructure to biodata to consumer appliances.

**What is data trafficking?**

Data trafficking is the movement of corporate and government data between nations without fully informed consent. The idea of data trafficking builds on three key uses of the term traffic. First, there is the idea of drug trafficking, a trade practice that undermines national
borders through robust grey market trade in addictive substances (Amaya 2020). Next, there is the idea of human trafficking, where user data replicates our human experience. Scholars have identified user data as a way of writing oneself into the digital environment (Boyd 2010) as “data doubles” (Lyon 2014b), “algorithmic identities” (Cheney-Lippold 2018), and the “quantified self.” (Neff and Nafus 2016). Each of these permutations of one’s digital identity draws on user data to create a digital version of the self, which is then vulnerable to trafficking. Finally, the idea of data trafficking draws on the idea of traffic, a metric for measuring the movement of data on networks.

Data trafficking occurs in a space lacking a clear international consensus, where industry standards are evolving, inchoate, or dispersed. It is essential to have a language to theorize the aggregated data that is being moved across borders to fully understand data trafficking.

When corporations and governments set industry standards, citizens are stripped of their rights to their data through unclear consent agreements and government policies that privilege corporations over citizens. Data trafficking is the movement of data across borders for political and/or financial gain without explicit consent (also called unconscionability). US courts use unconscionability to monitor and control contracts (DiMatteo and Rich 2005). In Rowe v. Great Atlantic & Pacific Tea Co., the New York Court of Appeals explained unconscionability regarding the signing of contracts as quoted by DiMatteo:

> There exists an unavoidable tension between the concept of freedom to contract, which has long been basic to our socioeconomic system, and the equally fundamental belief that an enlightened society must to some extent protect its members from the potentially harsh effects of an unchecked free market system. [T]he law has developed the concept of unconscionability so as to prevent the unjust enforcement of onerous contractual terms which one party is able to impose under the other because of a significant disparity in bargaining power (DiMatteo and Rich 2005).
Unconscionability is closely related to the uneven power dynamic between users and tech firms. The less power users have, the more unconscionable the contract becomes. Data trafficking exists within a larger constellation of concepts related to the security of user data, specifically sovereign control of personal data within specific countries.

Why data trafficking is a necessary concept

The ways in which data circulates depends on who is storing that data, which in turn has profound social impacts. As Jacquelyn Schneider noted at the Council on Foreign Relations in 2019, sectors such as the US financial system rely entirely on data. Uncertainty about where that data is stored or who controls it can lead to long-term system degradation. Data trafficking is crucial to understanding which sectors are most vulnerable, how to build systemic resilience in response, and how to protect individuals from systems that operate outside of their control.

One of the reasons why there has been resistance to designate the movement of data across borders as a problem is because limited data governance facilitates the growth of the digital economy. Regulations that require companies to track the lineage of the data that they gather are expensive, difficult to implement and have the potential of limiting trade. Arguing against the movement of data across borders with uninformed consent undermines many corporate business models. Labeling it as data trafficking, which connotes a violation of rights, could harm investments in these firms.

Regulating the data trade is likely to have financial impacts. As the digital economy becomes the economy, our digital lives become our personal lives. As the ways in which governments use our data become politicized, we do not have the luxury of prioritizing the
economic value of data above its other values.

The openness of digital trade is making personal data a vulnerable target for export between countries with different levels of data protection. Data trafficking offers a way to discuss the implications of moving data across borders while considering the unconscionability of current consent practices in the United States. In the US, there is often a focus on how much information a company accumulates, rather than how that company may subject the data to the laws of another political entity with competing interests.

This article has two key identifiable contributions. First, it extends how we think about the relationship between the commercial data and data generated by individuals. In 2008, communications scholar Anthony Fung asserted that global capital would “devise new local strategies to produce programs in cultures palpable to the changing values of the new generations in China in parallel with the strategies of how Chinese authorities have shaped, distorted, and even dictated the production, distribution, circulation, and consumption of culture” (Fung 2008, 22). Those same forces extend global corporate influence and Chinese government influence. Communications scholars Weiyu Zhang and Taberez Neyazi argue that a central feature of China’s communication landscape is the balance of social pluralism (in this case, the acquisition of Grindr by a private sector firm) and state authoritarianism (forced localization of Grindr). Defining data trafficking within the US-China context is central to understanding the risks to platform users and US national sovereignty, and to understanding China’s evolving communication system. The Grindr case shows us how those strategies have come to fruition in ways that not only shape China’s digital landscape, but also that of the United States.

Second, this work illustrates the relationship between aggregated personal data and national sovereignty. As Rebecca MacKinnon notes in her book, ‘Consent of the Networked’
(MacKinnon, 2012), the idea of the ‘consent of the governed’ emerged in the latter part of the twentieth century (MacKinnon, 2012, p. 11). MacKinnon designates a relationship between the social contract between citizens and their government and the legal consent contracts that they sign for internet providers and social platforms. Data trafficking describes the policy failure that occurs when the consent of the networked and the consent of the governed simultaneously break down.

Data capitalism, often also referred to as surveillance capitalism, the monetization of human life as raw material, produces three key threats (Zuboff 2019; Sadowski 2020, 2019). First, one country can take advantage of asymmetric data access, making economic dominance by one country over another in data-driven industries easier, then deepening such asymmetries using market-based tools. Economic dominance in strategic industries allows for competitive advantage and forms the foundation of dependency and leverage, where one country can limit access to key technologies.

The second threat is the insecurity of data-driven infrastructure as it relates to stability and national security in areas like telecommunications, agriculture, mobility, health, and city management, and consumer products ((Pal et al. 2021; Cosgrove et al. 2020) AUTHOR 2022). By the time these threats manifest, regulations must catch up. As Nora Draper, Philip Napoli, and others have demonstrated, regulation of technology lags the technology itself (N.A. Draper 2019; Napoli 2019). Companies aggregate health data from heart rates and blood sugar. Intimate images, from explicit photos to baby monitor feeds, are tools for building machine learning algorithms and deep fakes. With limited US domestic oversight, national-level data security is an issue.

Finally, surveillance capitalism presents significant privacy risks to individuals.
Corporations have clear incentive to gather as much data as they can about users to extract the maximum number of resources. Such privacy concerns are significant in one national context, but with the mismatch of user data protection and LGBTQIA+ rights, protecting user data privacy between national contexts becomes particularly important.

Grindr underscores the risks of transnational data movement between the US and China without clear user consent particularly with respect to the second two threats. First, opaque corporate governance can permit surveillance and misinformation, decreasing the security of platforms like Grindr that serve as important communications platforms (AUTHOR 2022). The platforms can potentially be used by government agents for intelligence or counter-intelligence purposes. Second, consumers face the risk of data extraction in a context where activities that are legal in one context face legal scrutiny in another (Cinnamon 2017). The Grindr case is particularly illustrative because LGBTQIA+ community members face heightened vulnerability in many countries and face significant risks in China. Greater vulnerabilities online and the unevenness of laws in place to protect users make the Grindr case a leading indicator of the differential risks that different communities face amidst data trafficking.

2. Case Study – Grindr.

Founded in 2009, Grindr is a social networking app for gay, bi, trans, and queer people with ‘millions of daily users who use…location-based technology in almost every country in every corner of the planet’ (Grindr 2019a). In 2016, Chinese company Beijing Kunlun Tech Co Ltd. acquired 60% of the firm (Wang 2019), then wholly acquired it in 2018 (Wang 2019). The site is an important place for the performance of cosmopolitan identity and the cultivation of
community (Ong 2017). The firm collects a wide range of intimate user data, from HIV status and sexual preference to images shared in the hook-up process (Grindr). Protecting user data is incredibly important because of the vulnerabilities the platform can expose, as identified by communications scholar Safiya Noble whose work reveals the racial biases in social algorithms (Noble 2018).

In addition to personal profile information, Grindr has been solidified as a repository of ‘dick-pics,’ or erotic images of men, but the platform’s importance extends far beyond its role in image-sharing. Rather, it is a crucial site for communication and community-formation in the LGBTQIA+ community. Informatics scholar Amanda Karlsson has argued that dick-pics are an important form of communication on dating platforms, and that they can be used as a way to share humor, harass, or seduce (Karlsson 2018). Film scholar Evangelos Tziallos argues that the nude images and erotic chat produced while assessing the viability of an in-person meeting are the actual rewards of the platform for users. Thus, Grindr’s importance is not just as a tool for eventual in-person connection, but rather a site for online community-building.

Grindr ultimately yields an environment in which users revel in their sexuality under presumed anonymity (from other users), as the platform gathers extensive information about their likes, looks, and preferences. Grindr is a platform for intimate trade between individuals, a fact which users understand as they trade images and texts. Like most digital trade, practices of consent are, at best, under-developed, and, at worst, deeply exploitative. Grindr’s gathering and sharing of intimate data violates what legal scholar Danielle Citron identifies as “sexual privacy,” or “the behaviors, expectations, and choices that manage access to the human body, sex, sexuality, gender, and intimate activities” (Citron 2019, 1870).

Citron’s discussion of sexual privacy focuses on privacy law within the United States.
However, what is less apparent to individuals is that Grindr is also a platform for intimate trade between nations. The Grindr case underscores the weakness of what legal scholar Maryann Franks terms “cyberspace idealism,” where social, historical, and physical constraints do not apply (Franks 2011, 225). When Grindr moved its engineering facilities to China in 2016, it stored data from other countries in its Chinese server farms and made real not only the fragility of commercial user data, but also how market power of corporations can extend government power in the identity-industrial complex (Mac 2019). The combination of data security policies from Beijing Kunlun Tech Co. Ltd, the 2017 PRC Cybersecurity Law requiring data localization, and the lack of US data regulations means that user data has been trafficked across borders to Chinese government-owned servers. Now, rather than intimate trade between individuals, we are seeing intimate trade between countries.

While Grindr’s community standards articulate ways for users to keep themselves safe while using the app, the firm’s privacy policy is much opaquer regarding the safety of a user’s data. The privacy policy asserts that users should not share information that they do not want to end up in the hands of a third-party contractor, with the exception of HIV status (Grindr).

Noting the security risk presented by the movement of Grindr data, the United States government referred the case to the Treasury Department’s Committee on Foreign Investment in the United States. In 2019, using the authority conferred by the Foreign Investment Risk Review Modernization Act (FIRRMA), the US government examined Beijing Kunlun’s acquisition of Grindr (Wang 2019). FIRRMA was passed in 2018 to expand government oversight of foreign acquisitions. CFIUS forced Beijing Kunlun Tech Co. Ltd. to divest its holdings in Grindr by June 2020 (Wang 2019), then unwound the Grindr acquisition by requiring Beijing Kunlun Tech Co. Ltd. to divest itself from the firm. In March 2020, Grindr agreed to divest to the private fund San
However, the data had already been transferred to Chinese government-run servers before the CFIUS review began. Even with new requirements for examination of transactions, there remain huge gaps in oversight. Reuters reported that two key figures in Beijing Kunlun Tech Co. Ltd.’s initial acquisition of Grindr were also involved with the San Vicente deal (Wang, Alper, and Oguh 2020). The clear linkages between Grindr’s original Chinese owner and its new US-based buyer suggest that even with divestment, currently generated data may still have weakened protections due to pre-existing corporate alliances. Weak platform-level consent paired with the movement of data guided by corporate interests and a confidential US government committee left no space for what Ruha Benjamin terms “informed refusal,” the avoidance of “techno-scientific conscription” of individual biodata (Benjamin 2016, 967-968). The multiplicity of user data conscription sites—at the level of user consent, how the platform uses data, how the platform sells that data, and how the data is “recovered” through yet another deal with private capital—underscores the importance of MacKinnon’s prescient call in the “Consent of the Networked”. MacKinnon argues for governance practices to align with the rapidly transforming data environment. It also highlights that intimate data has already been drawn into the data corpora of multiple states against the will of users.

Notably, Grindr is not a platform that has ever been widely used in China, except through virtual private networks (Chen 2022). As such, users can be forgiven for not understanding that it was held, in part or whole, by a Chinese firm for four years. Thus, the risk presented by Grindr’s relationship with the Chinese government was not necessarily one that widely impacted Chinese users, but rather users in other countries whose data became subject to Chinese laws.

The Grindr case is illustrative of the harms users face in an environment that enables data
trafficking. When users consented to sharing their data with the platform, the fact that their data was shared with a government lacking in the same human rights protections for the LGBTQIA+ community was obscured. Users who shared their data with Grindr as well as those who used the platform while it was under Kunlun’s ownership were penalized for not tracking international tech acquisitions nor understanding the close data-sharing relationship between Chinese corporations and the Chinese government. The Grindr case presents a particular issue because the transfer of user data occurred, in many cases, after users signed the platform’s terms of service.

This level of required understanding of the nuances of the international tech sector to protect one’s user data seems almost unimaginable to expect, let alone unconscionable.

Grindr’s user data has multiple uses that could generate harm, not just for users, but for communities worldwide. First, there is the personal risk that individuals face, with respect to potential harm. This is particularly true for US government officials facing Chinese government scrutiny. However, the personal harms are only the most discrete, not the most profound.

User data also offers a rich technological foundation for other interventions that complicate relations between countries with a contentious relationship. Social platform user data offers source material for disinformation campaigns (Howard and Bradshaw 2018) or source material for generating deep fakes (Whitaker 2021).

Yet the risks of data for disinformation campaigns and deep fakes are small when compared to the risks of long-term asymmetrical data gathering. In the Chinese case, parent companies of tech firms like WeChat’s owner Tencent have been hand-picked to work on the Chinese military’s AI efforts (Lee 2018). Other Chinese firms must share their technology with Chinese government regulators as part of China’s civil-military fusion efforts. Ultimately, data
trafficking is not just about the implications for the rights of individuals, but how practices shift global norms of power and data gathering between different systems of government.

3. **Global and Domestic Data Governance**

**Data Governance and the Individual**

Scholars have theorized why consumers fail to fight back against extensive corporate data gathering. Communications scholars Joseph Turow and Nora Draper refer to ‘digital resignation’ as ‘the condition created when people desire to control the information and data digital entities online marketers have about them, but feel unable to exercise that control’ (N. Draper and Turow 2019). Communication scholars Esther Hargittai and Alice Marwick found evidence of a ‘privacy paradox,’ through which young adults claim to care about privacy while also sharing private information online (Hargittai and Marwick 2016; Barnes 2006). The authors emphasize that users disclose data due to a lack of understanding of risk (Acquisti & Gross, 2006), a lack of knowledge of behaviors for privacy protection (Hargittai & Litt, 2013; Park, 2011), or the social benefits offered by self-disclosure online (Hargittai & Litt, 2013). Digital resignation and the privacy paradox overlook the geopolitical risks of data movement. Individuals have some understanding of the privacy practices of platforms that they use. However, geopolitical risk calculation is largely confined to corporate offices, the intelligence community, and Congressional hearings.

**Global Data Governance**
As early as 1984, popular science writer Eric J. Lerner wrote about the need to protect privacy in the exchange of data between the United States and the European Union (Lerner 1984). Since then, global policies have been enacted regarding the protection of data flow to enhance commerce. The European Union’s General Data Protection Regulation aims to define an individual’s relationship to their data—namely, that an individual could compel a company to remove their data (2014). However, this right does not offer guidance on what the company can do when they already have that data (2014).

Most of the policy focus on managing the movement of data has been to assure its commercial transfer. 1996’s World Trade Organization Information Technology Agreement ensures the smooth commercial transfer of hardware across borders (World Trade Organization 2015). 1997’s General Agreement on Trade in Services (GATS) Annex on Telecommunications guaranteed market access for digital services (Organization 2020). The United States International Trade Commission study *Digital Trade in the United States and Global Economies* reported digital trade as an export valued at USD 296.4 billion in 2014, a number which has since risen (Arona, Stamps, and Coffin 2014).

Simultaneously, the ways in which individuals’ data are traded have become increasingly insecure. As legal scholar Jennifer Daskal notes, the United Kingdom, Brazil, and other countries have argued that they can ‘unilaterally compel Internet Service Providers (ISPs) that operate in their jurisdiction to produce the emails and other private communications that are stored in other nation's jurisdictions, without regard to the location or nationality of the target’ (Daskal, 2015). Increasing international consensus to compel the production of private information underscores the changing norms regarding individual data in relation to governments. We are seeing now
how the openness of digital trade makes aggregated personal data a vulnerable target for export
between countries with different levels of data protection.

Communications scholar Tarleton Gillespie distinguishes between the governance of platforms and the governance by platforms (Gillespie 2018). The former refers to how governments and non-government organizations set standards for platforms. The latter refers to how platforms themselves manage their available resources. Platforms govern users via labyrinthine consent agreements. Data trafficking occurs because countries like China have identified how to leverage governance by platforms for the governance of platforms.

**Data Governance in the United States**

In the United States, few types of personal data have protections regarding how it can be gathered and moved. The Snowden disclosures of FISA court abuses (Krishnan 2021) and the Cambridge Analytica scandal (Hinds, Williams, and Joinson 2020) have revealed how the tech sector undermines liberalism within the United States. The lack of transparency surrounding data gathering paired with the monopolistic tendencies of digital feudalism have bolstered illiberalism in the US tech sector.

This leads to a patchwork coverage that is ineffectual at protecting user data. Health data has limited protections through the Health Information Portability and Accountability Act of 2013 (HIPAA), which protects the sharing of oral, written, or electronic medical records (Paulsen 2013). Even with HIPAA, health data is still vulnerable (Rubenfire 2015). Collaborations between insurer Anthem and tech firm Alphabet undermine these limited protections (Moses, Matheson, and Poste 2019). Cyber risk insurance, which reimburses claims
for cybersecurity attacks, significantly undercompensates the cost of a major hack (Vicevich 2018). Collaboration between Apple and Google for COVID-19 surveillance threatens to further undermine these limited protections (Apple Newsroom 2020).

The data of children under 13 has limited protections through the Child Online Privacy Protection Act (COPPA), which requires parental consent for self-disclosure of information by young people (Rush 2019). However, enforcement through the Federal Trade Commission has been limited to only the most egregious cases (Zavaletta 2001; Finnegan 2019).

In California, the California Consumer Privacy Act (CCPA) became law in January 2020 (California Consumer Privacy Act 2020). The act creates new rights for consumers in California relating to data gathering, including the right to request deletion of data, information about the sharing of data, and ways to provide access to data. The act also advises businesses on how to comply with the new Act (California Consumer Privacy Act 2020). However, corporations have stated that they will not comply until court cases force enforcement (Whittaker 2020).

New York State has protections for financial data. The 2017 New York Department of Financial Services Cybersecurity Regulation (23 NYCRR 500) requires financial services entities to expand their capabilities to prevent potential cyberattacks on institutions in New York State (New York State Department of Financial Services 2017). The regulation does not give individuals more control over their data (New York State Department of Financial Services 2017). In short, US government efforts to manage data rely on a patchwork of local regulations and an industry with little incentive to cooperate.

**Data Governance in China**
China, by contrast, urges Chinese firms to keep data in Chinese government-run servers (中华人民共和国网络安全法 [Zhongguo Renmin Gongheguo Wangluo Anquanfa] 2016) (Sacks and Li; Selby 2017; Kokas 2019). The Chinese military also has access to this data as a result of the Chinese government policy of civil-military fusion (军民融合) ("深入实施军民融合发展战略" 2017).

China’s national system creates a foundation to expand its sovereign territory in order to become what the Theoretical Studies Center Group of the Cyberspace Administration of China terms a “cyber superpower” (Kania et al. 2017) (Theoretical Studies Center Group of the Cyberspace Administration of China). The Chinese government developed a response to the emergence of a new potential sovereign landscape called cybersovereignty, the idea that a country’s national borders extend to the data gathered within its terrestrial borders by its military and by corporations headquartered on its land.

Massive data aggregation in China facilitates corporate growth, development of government technological capabilities, intelligence gathering, and surveillance (O'Leary 2013). In AI Superpowers: China, Silicon Valley, and the New World Order, Kai-Fu Lee argues that China will lead the global AI race because of the lack of constraints involved in aggregating Chinese consumer data (Lee 2018). The concepts of data trafficking and the data corpus give us a new understanding of what happens when consumers sign away the rights to their data in one country and that vulnerability is exploited in another country. The national data corpus, which contains the data of a nation’s citizenry and is a “data double” of the nation, builds on Simone Browne’s conception of the epidermalization of data, where user data becomes a product of what she terms the “identity-industrial complex,” where digital identity functions not only as part of
for-profit identity management through platforms, but extends into a tool for governments extending the scope of their power (Browne 2010).

To be clear, this is not an effort to advocate for the exploitative American model, nor a critique of China’s efforts to build its national sovereign data-state. Rather, it highlights the importance of monitoring global data hegemons to evade a system where the exploitative practices of one system amplify the exploitative practices of another.

**The US-China Relationship Clarifies the Risks of Data Trafficking**

The foundational risks of data capitalism expand in magnitude when they operate in a US-China context. The US data security landscape created a system that supports data extraction. This landscape has conditioned consumers to mindlessly assent to obscure terms of service. This conditioned inattention has produced the surveillance capitalism, the commodification of personal data for profit, that Shoshanna Zuboff first outlined (Zuboff 2019). When paired with Chinese firms' ambition to gather and transport data to China, surveilled capital responds to the Chinese government’s national security demands.

In the United States, corporate policies structure data governance practices, influencing a system known as multi-stakeholderism (DeNardis 2013). US-based tech firms drive policy to suit their economic interests, creating what critic Jodi Dean refers to as “neo-feudalism,” where tech platforms enable exploitation of labor (Dean 2020). The most egregious abuses by US tech firms emerge from their reliance on profit-generating algorithms. Even in the US criminal justice system and US-Mexico border, where an unholy alliance between the tech sector and the government extends oppressive government surveillance, corporations choose to participate
based on financial motives (Brayne 2017).

In China, forced localization to government servers drives data governance practices (Mueller 2017; Zeng, Stevens, and Chen 2017; AUTHOR 2018, 2019). While the United States and China have different data governance models, both leverage government and corporate influence to alienate citizens from their data. China’s model of Internet sovereignty, what Sarah McKune and Shazeda Ahmed refer to as “the regime’s absolute control over the digital experience of its population,” represents a new dimension of centralized sovereignty (McKune and Ahmed 2018). Chinese cybersovereignty operates under what communications scholar Min Jiang refers to as “authoritarian informationalism,” a blending of capitalism, authoritarianism, and Confucianism through which the Chinese government preserves social control and political legitimacy (Jiang 2010; Creemers 2020). China’s tech industry growth and fragmented US regulations have created a world in which consumers generate data for tech firms in the United States, but also for the Chinese government.

In China, neither corporate autonomy nor widespread individual rights protections exist due to the illiberalism of the system. Illiberalism is a thought system that aims to “undermine autonomous legal processes and individual rights protections,” according to legal scholar Samuli Seppänen (Seppänen 2019). Prioritizing political leadership over legitimate legal processes is a central feature of Communist Party regulations (Seppänen 2019). Political scientist Rachel Odell argues that China’s illiberalism is rooted in “a deep-seated insecurity about the Party’s ability to effectively maintain and exercise power as it seeks to reform China’s economy in order to ensure long-term growth” (Odell 2019). Efforts to enhance corporate autonomy or individual rights contradict Party efforts to retain control.

The US and Chinese models for data security exist at the intersection of two competing
visions of the relationship between data and the state. Both approaches alienate users from their data. However, fragmented corporate governance practices in the US allow the Chinese model to amplify the weaknesses of the US system. Chinese firms and the government can leverage poor US data security practices to enhance the government’s command of global data.

US industry is vulnerable to US government data gathering, but it is far more vulnerable to Chinese government data gathering. Whereas Apple successfully resisted sharing the passcode for the San Bernardino shooter (Apple Newsroom 2016), it gladly shared the accounts of Chinese iCloud users with Chinese government servers (Favreau 2018). While data can be generated across a range of platforms with little data privacy oversight in the United States, that same data can be moved and aggregated with comparative ease in China.

This issue has come to the forefront in China’s current technological expansion abroad. Chinese firms must localize data in response to China’s 2017 Cybersecurity Law, a law which urges companies to store personal data in China. Countries like the United States that lack adequate data protections face the potential for massive amounts of data to move across borders. The US-China relationship is the most impactful context to appreciate the role of data trafficking due to these uneven data security practices. Data trafficking reflects the alliance between data capitalism and techno-authoritarianism. The principles of data capitalism enable expanded government surveillance not just in local territories, but globally. In the US-China case, this produces not just transnational power for corporations, but extraterritorial oversight by the Chinese government.

4. Conclusion.
This paper focuses on a discrete example of data trafficking, namely, the movement of data from the United States to China as part of a major corporate acquisition, but data trafficking occurs in less obvious ways as well. The concept of data trafficking provides an original, holistic way to think about the different standards of data storage, security, and movement across different countries in relation to our dataified humanity. Each of these could be explored in greater depth in future studies. While countries enact policies about what data standards should or should not be, there is little global consensus on the matter. This paper problematizes the movement of data between different national data security standards, rather than the standards themselves. This paper urges governments, corporations, and individuals to address the consequences of a lack of consistent standards. Data trafficking helps us conceptualize how consumer data gathering is a function of economic growth and a factor in complicating how we understand our own humanity and how countries constitute national borders.

Consumer products and toys share user data to Chinese servers controlled by Chinese government entities. Subcontracting data management also presents a risk, A Japanese subcontractor of Line shared user data with a Chinese firm to outsource AI service development, subjecting unknowing Line users to Chinese government surveillance. These and other instances of data trafficking present opportunities for subsequent studies on challenges of managing consent for data gathering as it crosses international borders.

This article deepens understandings of the field by connecting data management and user consent with national sovereignty. It argues that countries without a robust national data governance structure like the United States are instead creating a power vacuum that enables data gathering by other countries with more assertive systems of data oversight. Just as labor
standards and characterizations of human trafficking differ between countries, data trafficking evolves in spaces between clear international norms (Shamir 2012). The multi-stakeholder model of data governance in the United States allows for corporate influence on data governance. It also facilitates data trafficking with its corporate-led data standards. By contrast, the Chinese approach facilitates forced data localization in government platforms.

Data trafficking poses a risk for large numbers of individuals in a community and for the modeling of social behaviors. Data trafficking undermines national sovereignty by facilitating the movement of personal data from one location with loose controls to another site with stronger controls. Such a system ensures that data generated in nations with robust data localization requirements can maintain sovereign control of their data to a greater extent than countries with more corporate-driven data governance structures.

The implications of data trafficking extend beyond the erosion of national sovereignty. Data trafficking places the data of individuals at risk when they document parts of their life that are legal in one country and illegal in another, as in the case of gay men sharing dick pics on Grindr. The movement of data thus exposes users to a different legal and social risk landscape than if their content had remained within the country in which it was generated.
Reference List


files/6321/8540.html.


World Trade Organization. 2015. Information Technology Agreement.

https://heinonline.org/HOL/P?h=hein.journals/scclj17&i=278

https://doi.org/10.1111/polp.12202.


https://baike.baidu.com/reference/16924056/524ei24C6zCKM7aptazZ2T6lJGblsR_TxuVaBmxczqYDQHq3krVwb 2s5aYRIVHiDNLw0KY8pYKxagNzXkJPoAL5e8jeT0cgX3xlfkJIB8wRdllA3X28ZGZ.