Grindr and the Data Corpus:Theorizing Consent in Data Localization

Aynne Kokas
ak3ff@virginia.edu
University of Virginia

Abstract

This article offers a framework to discuss when a community's data is moved abroad without their clear, informed consent, a practice I term data trafficking. I offer a comparative policy analysis of the case of 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 asmulti-stakeholderism [1]. In China, forced localization to government servers drives data governance practices [2-5]. This article extends howwe think about the relationship between the commercial data generated by individuals across multiple platforms, and how we understand transnational consumer data security.

1. Introduction.

The objective of this article is to offer a framework for how to discuss when a community's data is moved abroad without their clear, informed consent. We have a great deal of language to discuss violations of privacy, but the implication is that these are violations that occur because of corporate or government intrusions into one's private life. 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.

I use the case of Grindr, an LGBTQIA+ dating platform which 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. I use a comparative policy analysis of the Grindr case to demonstrate that the most potent context to appreciate the role of data trafficking is in the US-China relationship.

The US-China relationship is one of the largest trade relationships in the world. The US and Chinese models for data security exist at the intersection of two competing global visions of the relationship between data and the state. Both the US system. Chinese firms and the Chinese government can leverage poor US corporate data security practices to enhance the Chinese government's command of global data.

In the United States, corporate policies are the leading indicator for data governance practices, influencing a system known as multi-stakeholderism [1]. US-based tech firms can drive policy to suit their economic interests, creating what critic Jodi Dean refers to as a sort of "neo-feudalism," where tech platforms enable rampant exploitation of labor [6]. The most egregious instances of abuse by US tech firms emerge from their mercenary reliance on profit-generating algorithms, from the promotion of genocidal rhetoric against the Rohingya people in Myanmar [7] to amplifying popular misinformation in the 2016 US Presidential election [8]. Even in areas like the US criminal justice system and US-Mexico border, where an unholy alliance between the US tech sector and the US government extends oppressive US government surveillance, corporations choose to participate based on financial motives [9]. Competing interests complicate digital policymaking, oscillating between concerns about US-China competition and efforts to prioritize tech sector growth.

In China, forced localization to government servers drives data governance practices [3, 10-12]. While the United States and China have different models for data governance, both models leverage the combined power of 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 [13]. The Chinese system of cybersovereignty operates under what communication scholar Min Jiang refers to as "authoritarian informationalism," a blending of capitalism, authoritarianism, and Confucianism through which the Chinese government balances social control and efforts to preserve political legitimacy [14, 15]. China's tech industry growth paired with fragmented US data regulations have created a world in which consumers generate data not just for tech firms operating in the United States, but to another, particularly when those nations have also for the Chinese government.

In China, neither corporate autonomy nor widespread individual rights protections exist due to the illiberalism of the Chinese system. Illiberalism is

URI: https://hdl.handle.net/10125/79681
978-0-9981331-5-7

a thought system that is set out to “undermine autonomous legal processes and individual rights protections,” according to legal scholar Samuli Seppänen [16]. Prioritizing political leadership over legitimate legal processes is a central feature of Communist Party regulatory illiberalism [16]. 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” [17]. Thus, efforts to enhance corporate autonomy or individual rights contradict Party efforts to retain national control.

This article has two key identifiable contributions. First, it extends how we think about the relationship between the commercial data generated by individuals across multiple platforms.

Understanding data trafficking is essential to understanding global movement of data in general, and data security in China in particular. 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” [18]. This article articulates how those same forces extend the global corporate influence and Chinese government influence in concert. Communications scholars Weiyu Zhang and Taberez Neyazi argue that a central feature of understanding China’s communication landscape is appreciating the balance of social pluralism (in this case, the commercial acquisition of Grindr by a Chinese private sector firm) and state authoritarianism (forced localization of Grindr’s data corpus). Defining data trafficking within the US-China context is thus central not only to understanding the potential risks to platform users and US national sovereignty, but to understanding the evolution of China’s communication system.

Second, this work enhances an understanding of the relationship between aggregated personal data and national sovereignty. It explains the impact on the rights of individuals and states when data moves across borders without well-informed consent. As Rebecca MacKinnon notes in her landmark book, ‘Consent of the Networked’ (MacKinnon, 2012), the idea of the ‘consent of the governed’ only emerged on a global scale in the latter part of the twentieth century.[19] MacKinnon designates a relationship between the social contract that citizens have with their government and the legal contracts for notice and consent that they sign for internet service providers and social media 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 trafficking produces two key threats. First, economic dominance in data-driven strategic industries becomes easier when one country can take advantage of a massive asymmetry of data access, as in the case of China’s advantageous access to the US tech sector where US firms gathering data in China either are blocked or must share their data with the Chinese government. Economic dominance in strategic industries allows for not just competitive advantage in economic growth. It also 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. In the case of a communications platform like Grindr, this falls into three areas of risk. First, opaque corporate governance can permit surveillance and the circulation of misinformation. Second, the threat – not even the reality – of a data exploitation can lead to the misallocation of scarce financial and regulatory resources for the tech sector. Finally, there is the real risk that the platform can be used by government agents as a backdoor for hacking into other systems, most obviously phones.

The main challenge is that by the time these threats become manifest, the regulations must catch up. As communications scholars Nora Draper, Philip Napoli, and others have demonstrated, the regulation of technology lags the technology itself [20, 21]. Companies gather and aggregate health data from heart rates and blood sugar. Images of intimate life, from explicit photos to baby monitor feeds, flood servers as tools for building machine learning algorithms and deep fakes. Yet, in the United States, safeguards related to the utilization of that data are scarce. With limited US domestic data oversight, national-level data security is an issue. However, when data is moved from one sovereign nation divergent data security regimes, the data corpus becomes an international security issue.

The US data security landscape laid the groundwork for data trafficking by creating a system that supports data extraction. This landscape has conditioned consumers of US tech products to ignore the question of where their data goes, and to mindlessly assent to obscure terms of service. In the US context, this conditioned inattention has produced the debilitating phenomenon of surveillance capitalism, the commodification of personal data for profit, that Shoshanna Zuboff first outlined.[22] When paired with Chinese firms' ambition to gather and transport data to China, surveilled capital feeds the Chinese state sector by responding to the Chinese government's national security demands.

2. Literature Review.

The datafied self as a feature of social media has a longstanding history in communications research. Silvia Livingstone examined how young people balance intimate disclosure with privacy standards as a practice of identity formation in relation to the public and the platforms on which they display their social lives [23]. Communications scholar danah boyd (2011) argues that creating digital profiles are a way of writing oneself into the digital environment [24]. In follow-up work, boyd and Nicole Ellison note that social media profiles are essential for functioning on platforms [25]. In the context of data trafficking, self-disclosure becomes not merely a question of disclosure to a perceived public or known corporate entity, but also to national servers in different countries with different affordances for privacy and data security.

Beyond the profiles that individuals create for themselves exist the domain of data gathered by the corporation that accrues to those profiles. 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 among others, scholars have tried to understand how we are tracked online and where that data goes [26-29]. In his seminal study of big data and surveillance following the Snowden revelations, sociologist David Lyon made the case that despite data aggregation, users are 'so far from conforming to the abstract, disembodied image of both computing and legal practices' [28]. Yet, as users remain on the platforms, they are also increasingly 'known' by those platforms.

Within his theorization of the datafied self, David Lyon refers to the agglomerations of data about individuals in databases as 'data doubles.' Lyon's 'data doubles' are 'based on their activities, connections, performances, transactions, and movements that relate to government' [30]. Lyon's framing reflects the relationship between individuals and their government but eschews the focus on the relationship between individuals and corporations.

Other scholars have come up with related terms to describe the relationship between an individual's data and the self. American culture scholar John Cheney-Lippold argues that 'We are ourselves, plus layers upon additional layers of what I have previously called "algorithmic identities."' [31] Cheney-Lippold views the algorithmic identity as one that exists on top of, but not distinct from, our human identity. In her theorization of web search Media Studies scholar Kylie Jarrett conceives of the identities that emerge from data generated by search engines as a database of intention [32]. Jarrett introduces the idea of a self who exists as part of one's data, but the database of intention emerges from a proactive exchange with the search engine [32].

Communication scholar Gina Neff and anthropologist Dawn Nafus delve into the idea of dataifying the self by highlighting the ways in which individuals track their own data to monitor and self-discipline themselves, what they refer to as "self-tracking."[33] The body of data they engage with is the discourse of the "quantified self."[34] Quantified self-discourse refers to data that individuals gather about their own activities via platforms [34]. The quantified-self discourse does not delve into what happens when other groups aggregate data about those individuals.

Each of these scholars identify important ways that we dataify and quantify the lives of individuals. However, within the US-China context, the distinct contribution is the fact that the data corpus in aggregate is gathered and moved. The movement of data en masse becomes particularly crucial for the purposes of modeling communities for national security purposes, or for building new products at economies of scale.

3. Global & Domestic Data Governance.

Scholars have theorized why consumers fail to fight back against extensive data gathering by corporations. Communications scholars Joseph Turow and Nora Draper refer to 'digital resignation', what the authors term as 'the condition created when people desire to control the information and data digital entities such as online marketers have about them, but feel unable to exercise that control' Communications scholars Esther Hargittai and Alice Marwick demonstrate a similar phenomenon in experimental data with young people. Hargittai and Marwick's research found evidence of Barnes' 'privacy paradox', through which young adults claim to care about privacy while also sharing private information online. The authors emphasize that users disclose data due to a lack of understanding of risk,[35] a lack of knowledge of behaviors for privacy protection [36]; [37], or the social benefits offered by self-disclosure online.[36] I argue that digital resignation and the privacy paradox overlook the geopolitical risks of aggregated data movement. Individuals interact with their privacy settings or have some reputational understanding of the policy practices of individual platforms that they use. However, geopolitical risk calculation is largely confined to corporate regulatory affairs offices, the intelligence community, and Congressional hearings.

As early as 1984, popular science writer Eric J. Lerner wrote in IEEE Spectrum about the need to protect privacy in the international exchange of data between the United States and the European Union [38]. Since then, global policies have been enacted regarding the protection of data flow to enhance commerce. For example, the European Union's General Data Protection Regulation is an effort at defining an individual's relationship to their data—namely, that an individual could compel a company to remove their data [39]. However, this right does not offer any guidance on what the company can do when they already have that data [39].

Indeed, most of the policy focus on managing the movement of data across borders has been to assure its seamless commercial transfer. 1996's World Trade Organization Information Technology Agreement ensures the smooth commercial transfer of hardware across borders [40]. 1997's General Agreement on Trade in Services (GATS) Annex on Telecommunications guaranteed market access for digital services [41]. Digital trade is big business. The United States International Trade Commission study *Digital Trade in the United States and Global Economies* reported digital trade as an export at a value of USD 296.4 billion in 2014, a number which has since risen [42].

At the same time, the ways in which individuals' data are traded across borders have become increasingly insecure. As legal scholar Jennifer Daskal notes, countries like the United Kingdom, Brazil, and others 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 international norms regarding individual data in relation to governments. While much attention has been paid to commercializing digital trade, we are seeing now how the openness of digital trade makes the data gathered about individuals on platforms a vulnerable target for export between countries with different levels of data protection, especially when aggregated.

Communications scholar Tarleton Gillespie makes a key distinction between the governance *of* platforms and the governance *by* platforms [43]. The former refers to how governments and non-government organizations set standards for platforms. The latter refers to how platforms themselves manage the resources available to them. Platforms govern users via labyrinthine consent agreements and opaque privacy policies. Data trafficking occurs because countries like China have identified how to leverage governance by platforms for the purposes of the governance of platforms.

Data Governance in the United States

In the United States, few types of personal data have nationwide privacy protections regarding how such information can be gathered and moved. The Snowden disclosures of FISA court abuses [44], and the Cambridge Analytica scandal [45], among others, have revealed how the tech sector undermines liberalism within the United States. The lack of transparency surrounding data gathering and by US tech firms paired with the monopolistic tendencies of digital feudalism has resulted in a rise in illiberalism in the US tech sector. Proprietary corporate algorithms and opaque terms of service mask how corporations gather user data.

This leads to a patchwork coverage that is ineffectual at protecting user data. Health data has some limited protections through the Health Information Portability and Accountability Act of 2013 (HIPAA), which protects the sharing of oral, written, or electronic medical records [46]. Even with HIPAA, health data security is still vulnerable [47]. Collaboration between Apple and Google for COVID-19 surveillance, for example, threatens to further undermine these limited protections [48].

The data of children under 13 has some limited protections through the Child Online Privacy Protection Act (ChOPPA), which requires parental consent for self-disclosure of information by young people [49]. However, enforcement of the act through the Federal Trade Commission has been spotty and limited to only the most egregious cases.

States like New York and California have their own rules. The California Consumer Privacy Act (CCPA) became law in January 2020 [50]. The act creates new rights for consumers in the state of California relating to data gathering about consumers online including the right to request deletion of data, information about the sharing of data, and ways to provide access to data. The 2017 New York Department of Financial Services Cybersecurity Regulation (23 NYCRR 500) requires financial services entities to expand their cybersecurity capabilities to prevent potential cyberattacks on institutions operating in New York State [51]. The regulation does not give individuals more access to or ability to control their data [51]. US government efforts to manage data rely on a patchwork of local regulations and an industry with little incentive to cooperate. Such an approach fails to protect consumers domestically, let alone internationally.

Data Governance in China

China, in comparison, urges Chinese firms not just to keep data in Chinese domestic servers [52]. Those servers must also be government-run [5, 12, 53, 54]. In addition to government-run servers, the Chinese military has access to this data for military purposes as a result of the Chinese government policy of civil-military fusion (军民融合) [55].

China's national system creates a foundation for data and the nation to expand the range of its sovereign territory, to become what the Theoretical Studies Center Group of the Cyberspace Administration of China terms a "cyber superpower"[56] [57]. The Chinese government has developed a sophisticated response to the emergence of a new potential sovereign landscape, cybersovereignty, the idea that a country's national borders extend to the data gathered within its terrestrial borders, by its military, and—in an increasing number of circumstances—by corporations headquartered on its land. What this generates is the foundation of a national data corpus, a connected system structured to gather and integrate a national digital footprint of consumer and government data.

Massive data aggregation in China facilitates corporate growth, as well as the development of government technological capabilities, intelligence gathering, and surveillance [58]. In his book *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 [59]. Critics have argued that Lee's theory does not apply because Chinese firms would be building a Chinese data corpus, not a universal one. We need language to discuss what it means to move data across borders with limited consent. The concepts of data trafficking and the data corpus give us a new framework for understanding what happens when consumers sign away the rights to their data in one country and that vulnerability is exploited in another country. This idea of the national data corpus both contains the data of a nation's humans and is also a "data double" of the nation, builds on Simone Browne's conception of the epidermalization of data where biometrics operate as a site for the production of citizenship.[60]

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 own national sovereign data-state. Rather, it highlights the importance of monitoring the interaction between global data hegemons to evade a system where the exploitative practices of one system amplify the exploitative practices of another.

4. What is the Data Corpus?

This paper proposes a framework for understanding the aggregate commercial data about individuals as part of a sovereign state, and what the implications for this framing are within the context of global tech sector acquisitions. Whereas scholars have developed clear frameworks for understanding questions of affirmative profile-making by individuals, less attention has been paid to the aggregate sum of data gathered by companies and governments that then becomes the data corpus of a nation.

For the purposes of this article, I use the term data corpus to refer to consumer data aggregated and generated across a wide range of private firms. This is the type of data that is most likely to be trafficked from the US due to unclear notice and consent practices. The data corpus also refers to the comprehensive data gathered about an individual that can then be aggregated by government and corporate partners under favorable politico-economic circumstances. For example, a data corpus for an individual in the context of US-China relations could include data legally gathered and localized in China, such as data from TikTok accounts paired with Chinese visa application data [61]. This article considers the data corpus and data trafficking as they occur in the US context and beyond, but the act of moving aggregate data about individuals can occur in any nation where there is weak domestic data governance and security.

Rich scholarship exists focusing on corporate data-gathering about individuals. However, the impact of data aggregation by firms has equally, if not more, potent implications. As such, I provide an overview of how to assess the data aggregated by a corporation as part of its engagement with the consumer. This is the data corpus.

Most people understand that some of their data are being gathered by consumer platforms. Far fewer people are aware of the potential risks posed by the aggregation of that data. While some individuals care about the security of their individual data, corporations, researchers, and governments are particularly interested in the economies of scale that result from massive data corpora.

The idea of the data corpus is original in its examination of the combined impacts of consumer data aggregation. It is precisely at this crux, the intersection of corporate and governmental data gathering, that the data corpus emerges. It is only with the combined data of the state and the private sector that a more complete vision of the human data corpus emerges.

5. What is Data Trafficking?

Data trafficking is the movement of the data corpus between nations without fully informed consent. Like human trafficking, data trafficking evolves in spaces between clear international norms and laws, just as labor standards and characterizations of human trafficking often differ between countries [10, 62]. The practice occurs in a space where industry standards are evolving, inchoate, or dispersed, and where there is not a clear international consensus. To fully understand data trafficking, it is essential to have a language to theorize the aggregation of data that is being moved across borders.

When corporations and governments set industry standards, citizens are stripped of their rights to the data corpus through unclear consent agreements, labyrinthine corporate partnerships, and government policies that privilege corporations and access to data over the rights of citizens. Data trafficking is what happens to the data corpus without clear consent and control of data. Data trafficking is the movement of human data across borders for political and/or financial gain without explicit consent (also called unconscionability).

US courts use unconscionability to monitor and control contracts [63]. In Rowe v. Great Atlantic & Pacific Tea Co., the New York Court of Appeals explained unconscionability as a principle "so as to prevent the unjust enforcement of onerous contractual terms…because of a significant disparity in bargaining power." [63]

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 storage and security of user data; specifically sovereign control of the data generated by individuals within specific countries.

The ways in which data is stored and how it circulates are a result of who is storing that data, which ultimately shape the structure of our society. As Jacquelyn Schneider noted at the Council on Foreign Relations on January 7, 2019, sectors such as the US financial system rely entirely on data. Uncertainty about where that data is stored or who has control over it can lead to long-term degradation of the system. Understanding data trafficking is crucial to understanding which sectors are most vulnerable and how to build systemic resilience in response. It is also essential to protect individuals from systems which operate outside of their direct 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 carefully track the lineage or provenance of the data that they gather are expensive. Such regulations are technically difficult to implement, and they have the potential of limiting trade. As such, arguing against the movement of data across borders with uninformed consent undermines the business models of many firms. Labeling it as data trafficking, which connotes a violation of rights, has the potential to harm investments in these firms.

Regulating the data trade is likely to have financial impacts. However, 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 all its other values.

Increasingly, the openness of digital trade is making the rich data gathered about individuals a vulnerable target for export between countries with different levels of data protection. Data trafficking offers a way to discuss what it means to move data across borders while considering the unconscionability of current notice and consent practices in the United States. The concept of data trafficking provides a new framework for understanding what happens when consumers sign away the rights to their data in one country, and that policy vulnerability is then exploited in another country. In discussions of the type of data gathered within the US, there is a focus on how much information an individual company accumulates, rather than the fact that that company may subject the data to the laws and interests of another political entity with competing interests.

The concept of data trafficking is original because it provides a holistic way to think about the different standards of data storage, security, and movement that are evolving across different countries in relation to our dataified humanity. While we see a great deal of countries enacting policy 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 standards for data security, rather than the standards themselves. By articulating the problem of data trafficking, this paper further urges governments, corporations, and individuals to address the human consequences of a lack of consistent data standards between countries.

From an understanding of the data corpus and data trafficking, we can conceptualize the ways in which consumer data gathering is not only a function of economic growth, but a factor in complicating how we understand our own humanity and how countries constitute national borders.

6. Why focus on the US & China?

I focus on the data corpus in a US-China context for a few key reasons. 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 [64], it shared the accounts of Chinese iCloud users with Chinese government servers in the same year [65]. The US-China context elucidates the data corpus by showing how data can be generated with little data privacy oversight in the United States can be moved to and aggregated in China.

While data trafficking has been with us for as long as countries have had different standards for data security, this issue has come to the forefront in the current environment of China's technological expansion abroad. Chinese firms must localize data in China in response to China's 2017 Cybersecurity Law, a law which urges companies to store personal data and important information in China. Countries like the United States that lack adequate data protections instead face the potential for massive amounts of data to move across borders from the US to China. The most impactful context to appreciate the role of data trafficking is within the US-China relationship, due to uneven data security practices.

Moving data across borders includes the aggregation of data corpora into government-run servers. However, the bulk of the data corpus is generated from consumer data, which is why the data is so vulnerable. Within the US system, the same practices that allow for the full exploitation of data as a resource for generating revenue fail to protect the humans who generate that revenue. In this sense, data trafficking evolves from similar capitalist principles as human trafficking. The lack of oversight of labor systems in the United States facilitates the exploitation of laborers. The US-China relationship is one of the largest trade relationships in the world. It is also the intersection of two competing global visions of the relationship between data and the state.

7. Case Study – Grindr.

One of the most notable examples of data trafficking is the case of the Chinese-owned social media platform, 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' [66]. The site is an important place for the performance of cosmopolitan identity and the cultivation of community [67]. The firm collects a wide range of intimate data on its users, from HIV status and sexual preference to images shared between users in the hook-up process [68]. Protecting user data is thus incredibly important because of the individual vulnerabilities the platform can expose, as identified in the work of communications scholar Safiya Noble whose work reveals the racial biases in social algorithms.[69] In 2016, the Chinese company Beijing Kunlun Tech Co Ltd. acquired 60% of the firm.[70] Beijing Kunlun Tech Co Ltd. then wholly acquired Grindr in 2018. [70]

In addition to personal profile information, Grindr's place in the population imagination has been solidified as a repository of 'dick-pics,'or erotic images of men. Informatics scholar Amanda Karlsson has argued that dick-pics are an important form of communication on dating platforms like Grindr, and that they can be used as a way to share humor, harass, or seduce [71]. Film scholar Evangelos Tziallos argues that the nude images and erotic chat produced while individuals are assessing the viability of an in-person meeting are the actual rewards of the platform for users.

What Grindr ultimately yields is an environment in which users revel in their sexuality under presumed anonymity (from other users), as the platform gathers extensive intimate information about individual users and their likes, looks, preferences, and more. Grindr is a platform for intimate trade between individuals, a fact which users plainly understand as they trade images and texts. Like most digital trade, practices of consent for sharing information 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."[72]

Citron's discussion of sexual privacy focuses on privacy law domestically within the

United States. However, what is less apparent to individuals as they self-represent through their profiles 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.[73] When Grindr moved its engineering facilities to China in 2016, it stored data from other countries in its Chinese server farms, it subjected that user data to new regulatory regimes driven by Chinese sovereignty [74]. The combination of data security policies from its home company, Beijing Kunlun Tech Co. Ltd, the 2017 PRC Cybersecurity Law requiring data localization, and the lack of US data protection 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 due to a lack of data security in one and an excess of data security in the other.

While Grindr's community standards articulate ways for users to keep themselves physically safe while using the app, the firm's privacy policy, located on a separate page, is much opaquer regarding the safety of a user's data. Notably, the firm's privacy policy asserts that users should not share any information that they do not want to end up in the hands of a third-party contractor, with the exception of HIV status [75].

Noting the security risk presented by the movement of Grindr data, the United States government referred the Grindr 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 [70]. FIRRMA was passed in 2018 by the United States Congress with the aim of expanding US government oversight of foreign acquisitions in the United States. As a result of the CFIUS review, CFIUS forced Beijing Kunlun Tech Co. Ltd. to divest its holdings in Grindr by June 2020 [70]. CFIUS 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 Vicente Investments [76].

However, the data had already been transferred to Chinese government-run servers before the CFIUS review began. Even with new FIRMMA individual transaction requirements, there remain huge oversight gaps. 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 [77]. The links 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. The Grindr case allowed no space for what Ruha Benjamin terms "informed refusal," the avoidance of "techno-scientific conscription" of individual biodata [78]. User data conscription, at the level of user consent, how the platform uses data, how the platform sells that data into another data governance regime, and how the data is supposedly "recovered" through yet another secret deal with private capital underscores the importance of MacKinnon's prescient call in the for governance practices to align with the rapidly transforming human data environment.[19] It also, sadly, highlights that private, intimate, data has already been drawn into the data corpora of multiple states against the will of users.

8. Interventions.

This article deepens understandings of the field by drawing together questions of data governance and human rights by connecting the management of data with national sovereignty. Just as labor standards and characterizations of human trafficking often differ between countries, data trafficking evolves in spaces between clear international norms [79]. Data trafficking occurs in a space where industry standards are evolving, inchoate, or dispersed, and where there is not a clear international consensus. The multi-stakeholder model of data governance embraced in the United States allows for strong corporate influence on data governance. By extension, it also facilitates data trafficking with its wide-ranging corporate-led data standards. By contrast, the Chinese approach to sovereign control of data facilitates forced data localization in government platforms.

Data trafficking poses a risk not just for large numbers of individuals in a community, but for the modeling of community and social behaviors. Data trafficking undermines norms of national sovereignty by facilitating the movement of personal data from one location with comparatively loose controls over data to another site with stronger controls. Such a global system of data governance ensures that data generated in nations with robust data localization requirements can maintain sovereign control of their data to a much greater extent than countries with more corporate-driven data governance structures can.

The implications of data trafficking extend beyond the erosion of national sovereignty. Data trafficking places the data of vulnerable 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 participating in community-building activities to a different legal and social risk landscape than if their content had remained within the country that it was generated.

Reference List

1. DeNardis, L., *Multi-Stakeholderism: The Internet Governance Challenge to Democracy.* Harvard International Review, 2013. **34**(4): p. 40-44.
2. Mueller, M., *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. 2017: John Wiley & Sons. 140.
3. Zeng, J., T. Stevens, and Y. Chen, *China s Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty".* Politics & Policy, 2017. **45**(3): p. 432-464.
4. Kokas, A., *Platform Patrol: China, the United States, and the Global Battle for Data Security.* The Journal of Asian Studies, 2018. **77**(4): p. 923-933.
5. Kokas, A., *Cloud Control: China's 2017 Cybersecurity Law and its Role in US Data Standardization.* 2019: p. 32.
6. Dean, J., *Neofeudalism: The End of Capitalism?* Los Angeles Review of Books, 2020.
7. Douglas, S., *Preventing Genocide: Reigniting the Staying Power of the Convention.* Dalhousie Journal of Legal Studies, 2020. **29**: p. 75.
8. Persily, N. and J.A. Tucker, *Social Media and Democracy: The State of the Field, Prospects for Reform*. 2020, Cambridge, UK: Cambridge University Press.
9. Brayne, S., *Big Data Surveillance: The Case of Policing.* American Sociological Review, 2017. **82**(5): p. 977-1008.
10. Mueller, M., *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. 2017, Malden, MA: John Wiley & Sons.
11. AUTHOR, 2018.
12. AUTHOR, 2019.
13. McKune, S. and S. Ahmed, *Authoritarian Practices in the Digital Age| The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda.* International Journal of Communication, 2018. **12**(0): p. 21.
14. Jiang, M., *Authoritarian Informationalism: China's Approach to Internet Sovereignty.* SAIS Review of International Affairs, 2010. **30**(2): p. 71-89.
15. Creemers, R., *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, in *Governing Cyberspace: Behavior, Power and Diplomacy*, D. Broeders and B.V.D. Berg, Editors. 2020, Rowman & Littlefield: Lanham, MD.
16. Seppänen, S., *Interrogating Illiberalism Through Chinese Communist Party Regulations.* Cornell International Law Journal, 2019. **52**(2): p. 267-311.
17. Odell, R.E., *Chinese Regime Insecurity, Domestic Authoritarianism, and Foreign Policy*, in *Artificial Intelligence, China, Russia, and the Global Order*. 2019, Air University Press. p. 123-128.
18. Fung, A.Y.H., *Global Capital, Local Culture: Transnational Media Corporations in China*. 2008, New York: Peter Lang International Academic Publishers. 208.
19. MacKinnon, R., *Consent of the networked: the world-wide struggle for Internet freedom*. 2012: Basic Books.
20. Draper, N.A., *The Identity Trade: Selling Privacy and Reputation Online*. 2019, New York, NY: NYU Press. 283.
21. Napoli, P.M., *Social Media and the Public Interest: Media Regulation in the Disinformation Age*. 2019, New York, NY: Columbia University Press. 472.
22. Zuboff, S., *The Age of Surveillance Capitalism*. The Fight for a Human Future at the New Frontier of Power. 2019, New York: PublicAffairs.
23. Livingstone, S., *Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression.* New Media & Society, 2008. **10**(3): p. 393-411.
24. Boyd, D., *Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications*, in *A Networked Self: Identity, Community, and Culture on Social Network Sites*, Z. Papacharissi, Editor. 2010, Taylor & Francis: New York. p. 20.
25. Boyd, D.M. and N.B. Ellison, *Sociality through social network sites*, in *The Oxford Handbook of Internet Studies*, W.H. Dutton, Editor. 2013, Oxford University Press: Oxford. p. 151-172.
26. Lyon, D., *Big data surveillance: Snowden, everyday practices and digital futures*, in *International Political Sociology: Transversal Lines*, T. Basaran, et al., Editors. 2016, Routledge: New York, NY. p. 268-285.
27. Lyon, D., *Surveillance after Snowden*. 2015, Malden, MA: Polity Press.
28. Lyon, D., *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique.* Big Data & Society, 2014. **1**(2).
29. Seemann, M., *Digital Tailspin: Ten Rules for the Internet After Snowden*. Network Notebook, ed. G. Lovink and M. Rasch. Vol. 9. 2015, Amsterdam: Institute of Network Cultures. 63.
30. Lyon, D., *Surveillance, Snowden, and Big Data: Capacities, consequences, critique.* Big Data & Society, 2014. **1**(2): p. 2053951714541861.
31. Cheney-Lippold, J., *We Are Data: Algorithms and the Making of Our Digital Selves*. 2018, New York: NYU Press. 320.
32. Jarrett, K., *A Database of Intention?*, in *Society of the Query Reader: Reflections on Web Search*, M. Rasch and R. König, Editors. 2014, Institute

of Network Cultures: Amsterdam, Netherlands.

33. Neff, G. and D. Nafus, *Self-tracking*. 2016, Cambridge, MA; London, UK: MIT Press.
34. Neff, G. and D. Nafus, *Self-Tracking*. The MIT Press Essential Knowledge Series. 2016, Cambridge, MA: The MIT Press. 247.
35. Acquisti, A. and R. Gross. *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. in *International Workshop on Privacy Enhancing Technologies*. 2006. Berlin and Heidelberg: Springer.
36. Hargittai, E. and E. Litt, *New strategies for employment? internet skills and online privacy practices during people's job search.* IEEE Security Privacy, 2013. **11**(3): p. 8.
37. Park, Y.J., *Digital Literacy and Privacy Behavior Online.* Communication Research, 2011. **40 (2)**(22): p. 22.
38. Lerner, E.J., *International data wars are brewing: U.S. telecommunications deregulation, Third World protectionism, and European privacy regulations may complicate or curtail data flow across borders.* IEEE Spectrum, 1984. **21**(7): p. 5.
39. Official Journal of the European Union, *Judgment of the Court (Grand Chamber) of 13 May 2014 (request for a preliminary ruling from the Audiencia Nacional — Spain) — Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*. 2014, the European Union: Brussels, Belgium.
40. World Trade Organization, *Information Technology Agreement*. 2015.
41. Organization, W.T., *Services: Annex on Telecommunications*. 2020, World Trade Organization.
42. Arona, B., J. Stamps, and D. Coffin, *Digital Trade in the US and Global Economies, Part 2*. 2014, United States International Trade Commission: Washington D.C. p. 331.
43. Gillespie, T., *Chapter 14: Regulation of and by Platforms.* SAGE handbook of social media, 2018: p. 30.
44. Krishnan, M., *The Foreign Intelligence Surveillance Court and the Petition Clause: Rethinking the First Amendment Right of Access.* The Yale Law Journal Forum, 2021: p. 21.
45. Hinds, J., E.J. Williams, and A.N. Joinson, *"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal.* International Journal of Human-Computer Studies, 2020. **143**: p. 102498.
46. Paulsen, E., *H.R.3119 - 113th Congress (2013-2014): Health Information Privacy Protection Act of 2013*, in *H.R.3119*. 2013.
47. Rubenfire, A. *Anthem hack will shake up market for cyber risk insurance*. Modern Healthcare 2015 February 5, 2015 [cited 2020 May 7]; Available from: https://www.modernhealthcare.com/article/20150205/NEWS/302059939/anthem-hack-will-shake-up-market-for-cyber-risk-insurance.
48. Apple Newsroom, *Apple and Google partner on COVID-19 contact tracing technology*, in *Apple Newsroom*. 2020: Mountainview, CA.
49. Rush, B.L., *Text - H.R.3900 - 116th Congress (2019-2020): To amend the Children's Online Privacy Protection Act of 1998 to strengthen protections relating to the online collection, use, and disclosure of personal information of children and minors, and for other purposes*, in *H.R.3900*. 2019, House of Representatives: Washington D.C.
50. *California Consumer Privacy Act*, in *AB*. 2020.
51. New York State Department of Financial Services, *Cybersecurity Requirements for Financial Services Companies*, in *23 NYCRR 50*. 2017. p. 14.
52. 中华人民共和国网络安全法 *[Zhongguo Renmin Gongheguo Wangluo Anquanfa]*. 2016, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm: China.
53. Sacks, S. and K.M. Li, *How Chinese Cybersecurity Standards Impact Doing Business In China.*
54. Selby, J., *Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? | International Journal of Law and Information Technology | Oxford Academic.* International Journal of Law and Information Technology, 2017. **25**(3): p. 213-232.
55. 深入实施军民融合发展战略, in 光明日报. 2017: 北京.
56. Kania, E., et al., *China's Strategic Thinking on Building Power in Cyberspace.* New America, 2017.
57. Theoretical Studies Center Group Cyberspace Administration of China 中央网信办理论学习中心组, "*Shenru guanche xijinping zongshuji wangluo qiangguo zhanlue sixiang zhashi tuijin wangluo anquan he xinxihua gongzuo*" 深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作 *[Implementing General Secretary Xi Jinping's strategic thinking on strengthening China through the Internet to make solid progress in cyber security and IT application]*. 2017, QSTheory.cn: Beijing, China.
58. O'Leary, D.E., *Artificial Intelligence and Big Data.* IEEE Intelligent Systems, 2013. **28**(2): p. 96-99.
59. Lee, K.-f., *AI Superpowers: China, Silicon Valley, and the New World Order*. 2018, New York: Houghton-Mifflin Harcourt.
60. Browne, S., *Digital Epidermalization: Race, Identity and Biometrics.* Critical Sociology (Sage Publications, Ltd.), 2010. **36**(1): p. 131-50.
61. Neyaz, A., *Security, Privacy and Steganographic Analysis of FaceApp and TikTok.* 2020: p. 22.
62. Mueller, M.L., *Networks and States: The Global Politics of Internet Governance*. 2010, Cambridge, MA: MIT Press. 320.
63. DiMatteo, L.A. and B.L. Rich, *A Consent Theory*

of Unconscionability: An Empirical Study of Law in Action. Florida State University Law Review, 2005. **33**(4): p. 1067-1118.

64. Apple Newsroom, *A Message to Our Customers*. 2016.
65. Favreau, J., *Apple's China iCloud data migration sweeps up international user accounts*, in *TechCrunch*. 2018.
66. Grindr, *About us*, in *Grindr*. 2019.
67. Ong, J.C., *Queer cosmopolitanism in the disaster zone: 'My Grindr became the United Nations'.* International Communication Gazette, 2017. **79**(6-7): p. 656-673.
68. Grindr, *Community guidelines*, in *Grindr*. 2019.
69. Noble, S., *Algorithms of Oppression: How Search Engines Reinforce Racism*. 2018, New York: New York University Press.
70. Wang, E., *China's Kunlun Tech agrees to U.S. demand to sell Grindr gay dating app*, in *Reuters*. 2019: New York, NY.
71. Karlsson, A., *Understanding of bold social media content : A study of dick-pics as a way to communicate*. 2018, Umeå University: Sweden.
72. Citron, D.K., *Sexual Privacy.* Yale Law Journal, 2019. **128**(7): p. 1870-1960.
73. Franks, M.A., *Unwilling Avatars: Idealism and Discrimination in Cyberspace.* Columbia Journal of Gender and the Law, 2011. **20**(2): p. 23.
74. Mac, R., *Grindr Had Dreams Of Making The World Better For Queer People. Then A Chinese Gaming Company Bought It*, in *BuzzFeed News*. 2019.
75. Grindr, *Privacy Policy*, in *Grindr*. 2019.
76. Fontanella-Khan, J. and Y. Yang, *Grindr sold by Chinese owner after US national security concerns.* Financial Times, 2020.
77. Wang, E., A. Alper, and C. Oguh, *Exclusive: Winning bidder for Grindr has ties to Chinese owner*, in *Reuters*. 2020: New York/Washingtion.
78. Benjamin, R., *Informed Refusal: Toward a Justice-Based Bioethics.* Science, Technology, & Human Values, 2016. **41**(6): p. 967-90.
79. Shamir, H., *A Labor Paradigm for Human Trafficking.* UCLA Law Review, 2012. **60**(1): p. 62.