shows, there is considerable potential in facilitating new transnational coalitions involving governments, companies, and civil society organization that can push together for desirable political outcomes, including a better international economic data law. To assess the impact of any such rulemaking effort, the persistent and paradoxical lack of data about state of the global digital economy ought to be addressed, if necessary by mandating data disclosures from those who control large-scale data generating infrastructures for statistical purposes.

Neither our panel nor this introductory essay could address all these important questions and rough ideas in depth. But raising them is a first step to design better international economic data law in future.

National Security, Investment Review, and Sensitive Data

doi:10.1017/amp.2021.103

*By Sarah Bauerle Danzman**

As a scholar of the politics of the nexus of national security and investment policy, I can best add to the discussion on the issue of data and digital tech restrictions mostly from a foreign investment regulation and investment screening vantage point.

The politics of investment review for national security purposes points to three central issues. First, a growing number of high-income countries increasingly view large volumes of consumer data as a potential vulnerability that threat actors can exploit. While Europe has been a leader on stricter data privacy regulation, the United States has arguably the most assertive position on screening foreign investment acquisitions for national security concerns arising from sensitive personal data. This is clear from the very public dispute over ByteDance's ownership of TikTok[1] and also reporting in the news that the U.S. screening mechanism—the Committee on Foreign Investment in the United States (CFIUS)—required a Chinese business to divest from the gay dating app, Grindr, in 2019.[2] But many other advanced economies are expanding their screening authorities to also include data privacy issues.[3] So, we should not see this as a purely American phenomenon.

Second, sensitive personal data can create multiple national security concerns that governments must contend with. At the most basic level, when foreign firms own and control large amounts of personally identifying and sensitive information on domestic persons, host countries may face legitimate concerns that the foreign firms' government may be able to gain access to those data repositories for intelligence purposes. Governments may be especially wary if there is a lack of trust as to whether the foreign business that controls access to sensitive personal data will protect it from authorities or share it with their home country government if asked or demanded to do so. Third, host countries are frequently worried that many businesses in the digital era have the capacity to engage in targeted data collection may be used to collect sensitive information that borders on intelligence such as troop movements or the activities of diplomats, or used to blackmail or recruit

* Assistant Professor of international studies at Indiana University Bloomington.

[1] Echo Wang & David Shepardson, *China's ByteDance Challenges Trump's TikTok Divestiture Order,* Reuters (Nov. 11, 2020), *at* https://www.reuters.com/article/usa-tiktok/chinas-bytedance-challenges-trumps-tiktok-divestiture-order-idUSKBN27R07W.

[2] Carl O'Donnell, Liana B. Baker & Echo Wang, *Exclusive: Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App*, Reuters (Mar. 27, 2019), *at* https://www.reuters.com/article/us-grindr-m-a-exclusive/exclusive-told-u-s-security-at-risk-chinese-firm-seeks-to-sell-grindr-dating-app-idUSKCN1R809L.

[3] Sarah Bauerle Danzman & Sophie Meunier, *The Big Screen: Global Crises and the Diffusion of Foreign Investment Review* (unpublished manuscript, on file with author).

government employees as sources. When countries of concern engage in repressive tactics against political enemies, democratic governments might evaluate whether a commercial actor based in a repressive regime might provide their home government access to data that could then be used to target specific vulnerable groups, particularly dissidents in a diaspora community.

An even more challenging component of assessing national risk is how data issues intersect with technology issues. Emerging technologies, especially artificial intelligence and biotechnology, are very hard to separate from data because these technologies depend on harvesting data to perfect algorithms and investigate sources of genetic abnormalities. Appealing to national security concerns based on whether bulk data collection provides an adversary with a competitive advantage in sensitive technology innovation is likely to render a very large portion of the national economy as off-limits to foreign ownership, and in the service of mitigating a rather attenuated risk. It is incredibly challenging to determine which emerging technologies have solely commercial applications and which are truly dual use. And so, with these expansive risk concepts, it is increasingly difficult to narrowly scope limitations on ownership of businesses with access to sensitive data. When everything is potentially military use, then it becomes nearly impossible to get comfortable with foreign ownership. This problem of expanding scope intersects with observations that data is increasingly a competitive asset, and therefore combines economic competitiveness issues with national security concerns in ways that are hard to disentangle.

Third, it is important to contextualize the issue of data and digital tech in a broader regulatory regime. The ability to continue to engage in robust cross-border economic exchange in an era of increased contention over who can control data will rest upon some cooperation over data privacy laws and shared regulatory expectations around digital trade, including data localization requirements. One other area that I think deserves particular mention is the global information communications technology infrastructure. Here, the United States' campaign against Huawei is instructive because it showcases how, from a political perspective, governments are increasingly thinking about how network structures provide both opportunities and vulnerabilities when it comes to data flows.[4] This concern is fundamentally rooted in matters of trust. You can have very strong privacy laws, but these laws cannot be meaningfully enforced if the infrastructure on which private data flow is not secure. Without shared trust that vendors are not misusing their access to networks, there will be conflict. And so, when thinking about paths toward more cooperative outcomes internationally, policymakers need to pay careful attention about how to build trust among key global actors.

I. The Political Economy of Investment Screening

The political economy of investment screening today, and particularly in the United States is fascinating and puzzling. There has been far less pushback, at least publicly, from the domestic business community than standard political economy theory would predict. The Foreign Investment Risk Review Modernization Act of 2018, or FIRRMA,[5] which substantially strengthened the powers of CFIUS, easily passed the U.S. Congress on a broadly bipartisan basis and with little formal counter-lobbying from business groups. Where we do see concern from the business community is typically not on whether to create stronger investment screening mechanisms or not but rather how to implement these rules in a way that will not harm domestic industry. FIRRMA provided CFIUS with the ability to review non-controlling, non-passive investment in U.S. critical

[4] Colin Lecher, *White House Cracks Down on Huawei Equipment Sales with Executive Order: The Latest in the Escalating Battle*, Verge (May 15, 2019), *at* https://www.theverge.com/2019/5/15/18216988/white-house-huawei-china-equipment-ban-trump-executive-order.

[5] Title XVII, Pub. L. 115-232.

https://doi.org/10.1017/amp.2021.103 Published online by Cambridge University Press

technology, critical infrastructure, and sensitive personal data businesses. This authority is the first time that CFIUS has jurisdiction over non-controlling investments. And this particular provision generated substantial comment from the business community and especially the venture capital community.[6] At issue was the concern that a too strict screening process for small investments in the most dynamic industries of the U.S. economy would create binding financial constraints on the most innovative start-ups. While the business community was not successful in preventing FIRRMA from extending CFIUS authority to non-controlling investments, the rulemaking process shows that the U.S. government did take into consideration some technical guidance about how to legally define a foreign investor that did not inadvertently cast too wide a net. The industry concern that stringent investment screening could slow down the innovation economy by starving it of capital highlights that regulating inward investment in high tech and digital industries is a balancing act. Academics—in economics, political science, law, and public policy, should explore in greater detail how the U.S. government interacts with the business community over issues that are branded as national security.

II. Geopolitics and the Emerging Biden Agenda

We should expect that the Biden administration will carry forward with relative continuity a tough stance on investment from adversarial capital, and especially from Chinese entities. It is important to remember that FIRRMA was a broadly bipartisan bill, and one of only a handful of bipartisan pieces of legislation that passed during the Trump administration. It is easy to think of the Trump administration's handling of China and economic policy more generally as being exceptional, and it was outside of the norm in terms of process and some tactics. But, the underlying concerns about the People's Republic of China (PRC) and growing strategic competition are bipartisan concerns. I expect a Biden administration to continue to project a tough on China stance, but with a smoother policy process and more emphasis on multilateral actions to create a broader coalition of allies and partners to counter the most aggressive of Chinese actions.

The concerns that underpin hawkish attitudes toward the PRC are numerous and challenging to fully consider in any one discussion. However, there are genuine and understandable concerns related to data that the U.S. government must respond to. First, there are real human rights concerns when we are discussing policy toward a country with a problematic human rights record and especially one in which there are credible reports of human rights abuses that are being carried out through digital authoritarian means. These human rights concerns are amplified by the fact that the PRC does not have legal system in which it is possible to obtain impartial judicial review. If the PRC demanded that a domestic company hand over data on U.S. persons collected through the company's U.S. subsidiary, it would be unlikely that this demand would be made public. Further complicating the risk calculus is that the separation between the state and private firms is much more tenuous in China than in the United States or other market-based economies. The PRC often support nominally private firms in ways that may be seen as unfair. It also can exert much more levers of de facto control over these firms than is possible for the United State or European governments to do.

At the same time, the United States-China relationship is essential to get right because these two powers plus the European Union are the biggest economies and strongest political units in the world. We need to move forward in a way that builds trust and points of connections between these societies. We will not agree on everything. But, a bellicose approach to China is likely to

[6] Sarah Bauerle Danzman, *Protecting or Stifling? The Effect of Investment Screening on Technology Firms* (unpublished manuscript, on file with author).

https://doi.org/10.1017/amp.2021.103 Published online by Cambridge University Press

backfire for multiple reasons. First, the most pressing problem in the global system is climate change and we will not find a meaningful solution to the climate dilemma if we cannot cooperate with the PRC on this issue. Second, quite frankly, the United States no longer possess the degree of power preponderance contra the PRC that would be required for a more aggressive strategy to be effective. And so, the Biden administration will find that it needs to bring its partners along with it to successfully counter PRC actions of concern.

https://doi.org/10.1017/amp.2021.103 Published online by Cambridge University Press