

Proceedings of the ASIL Annual Meeting**Date of delivery:****Journal and vol/article ref:**

ampd

Number of pages (not including this page): 4

page 1 of 2

This proof is sent to you on behalf of Cambridge University Press.

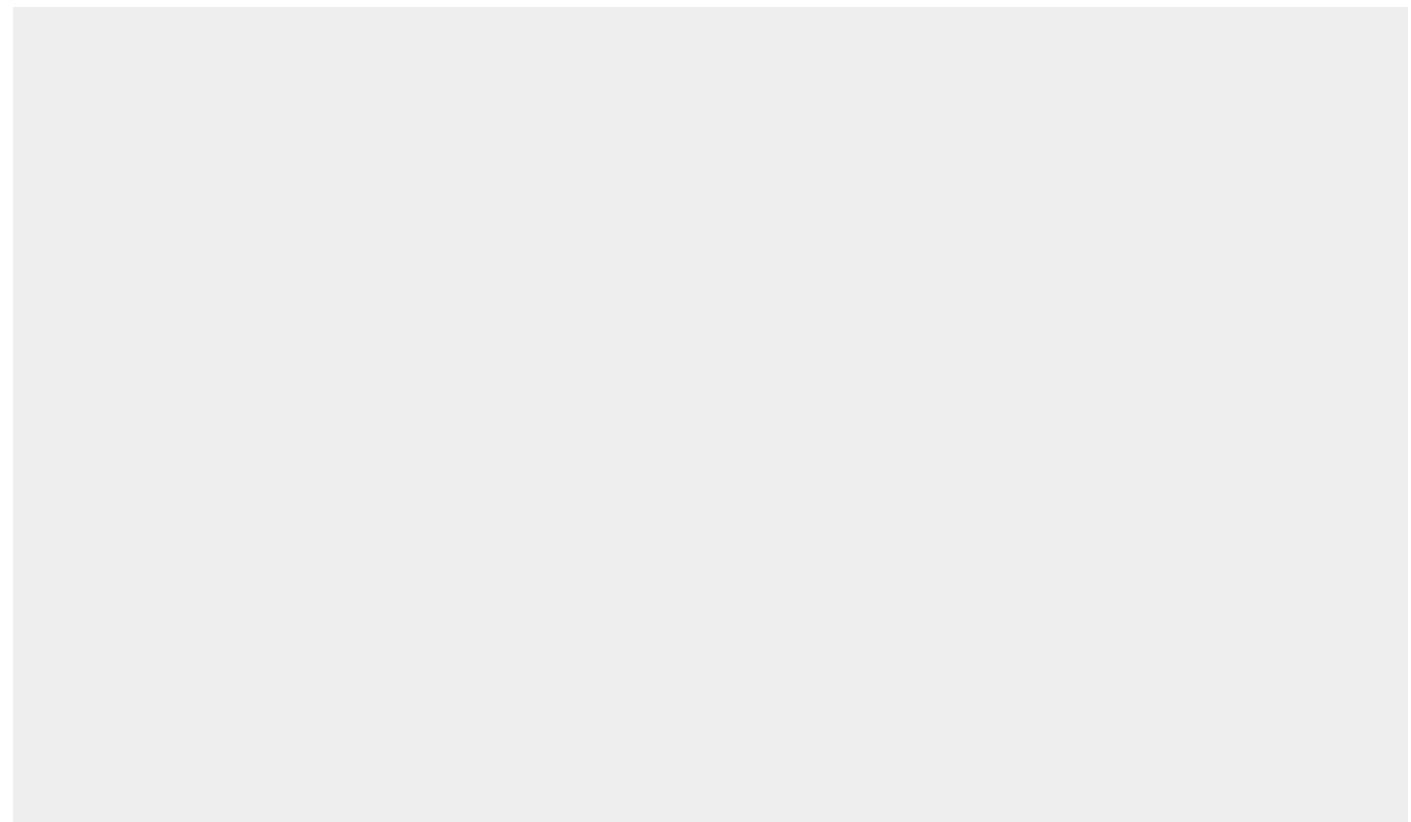
Authors are strongly advised to read these proofs thoroughly because any errors missed may appear in the final published paper. This will be your ONLY chance to correct your proof. Once published, either online or in print, no further changes can be made.

Please EMAIL your corrections within 3 days of receipt to:

Erin Lovall, Copyeditor <elovall@asil.org>
with a cc: to Brian Mazeski, Production Editor <bmazeski@cambridge.org>

You may provide your corrections using comment and markup tools in Adobe Reader, or you may list your corrections and responses to queries in an email or Word document, according to page and line number.

If you have no corrections to make, please also email to authorize publication.

Proceedings of the ASIL Annual Meeting

Please note:

- The proof is sent to you for correction of typographical errors only. Revision of the substance of the text is not permitted, unless discussed with the editor of the journal. Only **one** set of corrections are permitted.
- Please answer carefully any author queries.
- Corrections which do NOT follow journal style will not be accepted.
- A new copy of a figure must be provided if correction of anything other than a typographical error introduced by the typesetter is required.
- If you have problems with the file please contact **bmazeski@cambridge.org**

Please note that this pdf is for proof checking purposes only. It should not be distributed to third parties and may not represent the final published version.

Important: you must return any forms included with your proof.

Please do not reply to this email

NOTE - for further information about **Journals Production** please consult our **FAQs** at
http://journals.cambridge.org/production_faqs

Author Queries

Journal: AMP (Proceedings of the ASIL Annual Meeting)

Manuscript: S0272503721001026jra

- Q1** The distinction between surnames can be ambiguous, therefore to ensure accurate tagging for indexing purposes online (e.g. for PubMed entries), please check that the highlighted surnames have been correctly identified, that all names are in the correct order and spelt correctly.
- Q2** Please check all authors' names and affiliations to confirm they are correct and complete for publication.

1
2
3
4
5 **THE RISE OF RESTRICTIONS ON DATA FLOWS AND DIGITAL**
6 **TECHNOLOGIES: NATIONAL SECURITY, HUMAN RIGHTS, OR**
7 **GEO-ECONOMICS?**
8

9 This panel was convened at 12:30 p.m., Wednesday, March 24, 2021, by its moderator Thomas
10 Streinz of Guarini Global Law & Tech, who introduced the panelists: Sarah Bauerle Danzman of
11 Indiana University Bloomington; Yan Luo of Covington & Burling LLP; Maria Martin-Prat of the
12 European Commission Directorate General for Trade; and George Mina, Australian
13 Representative to the World Trade Organization.
14
15

16 **DESIGNING INTERNATIONAL ECONOMIC DATA LAW**
17 doi:10.1017/amp.2021.102
18
19

20 *By Thomas Streinz**

Q1
Q2

22 For a second year in a row, the American Society of International Law had to convene an all
23 virtual annual meeting because the COVID-19 pandemic made international travel and gathering
24 in cavernous ballrooms impossible. I had the pleasure of chairing a pre-recorded panel on the
25 rise of restrictions on data flows and digital technologies, which featured a stellar cast of experts
26 distributed across three continents and time zones.¹ This panel depended on the digital infrastruc-
27 ture provided by a private videoconferencing company on top of the public infrastructure of inter-
28 connectivity that the internet has supplied for more than three decades. As the pandemic forced
29 people around the world into lockdowns—albeit asynchronously and unevenly—it further main-
30 streamed the use of communications platforms for everyday interactions, whether public or pri-
31 vate, whether for business or leisure.

32 In this and other ways, the pandemic revealed how reliant the global economy has become on
33 digital data. Globally distributed networks of economic production have been enabled by informa-
34 tion and communications technology (ICT) for which digital data is a medium through which
35 information is being transmitted and shared transnationally. While companies have always relied
36 on information to gain comparative advantage and have exploited information asymmetries
37 accordingly, the use of “big data” promises new ways of gaining insight into business opportunities
38 and market conditions within and across sectors. Public discourse is often dominated by concerns
39 over global platform companies that generate vast amounts of personal data about their users in
40
41
42

43 * Adjunct Professor of Law and Executive Director of Guarini Global Law & Tech at New York University School of
44 Law. While the views expressed in this Article are personal, my thinking about these issues has been heavily influenced by
45 the Institute for International Law & Justice’s MegaReg project with Benedict Kingsbury, Paul Mertenskötter, and Richard
46 B. Stewart (www.iilj.org/megareg) and Guarini Global Law & Tech’s Global Data Law project (www.guariniglobal.org/global-data-law) with Angelina Fisher and Benedict Kingsbury.

47 ¹ The recording is publicly available on YOUTUBE (May 26, 2021) at <https://www.youtube.com/watch?v=xWN52rmDH8M&t=1s>.

pursuit of information capitalist business models.² Yet, non-personal data such as industrial or environmental data can also be leveraged for commercial gain transnationally. Contemporary advances in artificial intelligence technology have enabled unprecedented image, audio, and text recognition and are routinely used to create, shape, and “optimize” algorithmically mediated spaces. These forms of machine learning depend crucially on very large datasets to train algorithms through “deep” neural networks.

For these reasons, the generation, commercial exploitation, and unhindered transnational transfer of data have become hallmarks of today’s global digital economy. At the same time, deep digital divides persist and those who enjoy infrastructural control over the means of data production, not only attain de facto control over vast quantities of data but also determine qualitatively where and when what kind of data is being generated in what way and for what purpose.³

Concurrently with the digital transformation of economies and societies, transnational access, transfer, and use of data have increasingly become focal points during negotiations for “comprehensive” trade and investment agreements. While these efforts are often presented and discussed as negotiations about “electronic commerce” and “digital trade” that will “modernize” the *acquis* of international economic law, we are arguably witnessing the design of new international economic data law that is conceptually distinct from conventional international trade and investment law.

The design of this new international economic data law reflects a complex political economy. The world’s largest trading blocs—the United States, the European Union, and China—have pursued different strategies and are now engaged in plurilateral negotiations on “electronic commerce” under the World Trade Organization’s (WTO) plurilateral Joint Statement Initiative (JSI), which has attracted principal support from eighty-six WTO members, including all developed countries, but only five African countries and only three least developed countries.⁴ Meanwhile, Singapore, New Zealand, and Chile have crafted new modular templates with the Digital Economic Partnership Agreement (DEPA), which showcases the range of digital governance issues (including artificial intelligence)⁵ that instruments of international economic law can address, irrespective of a close nexus to traditional “trade” or “investment.” These initiatives respond to demands for international rule-making in the digital domain. By using venues and instruments of international economic law, they shape the meta-regulatory frames within which domestic regulators and other norm setters craft new rules governing data and digital technologies. When our panel diagnosed and analyzed a “rise of restrictions,” it implicitly acknowledged the absence of such restrictions as a default to be preserved rather than an ambition yet to be achieved. The internet affords a widespread, yet far from universal, ability for quasi-instantaneous transnational transmissions of data that departs from default parameters for which international economic law has historically been designed. Rather than enabling convergence in a world of regulatory divergence, international economic data law is designed to prevent such regulatory divergences from materializing by meta-regulating what and how governments can regulate in the digital domain.

² JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019).

³ Angelina Fisher & Thomas Streinz, *Confronting Data Inequality* (IILJ Working Paper 2021/1), at https://ssrn.com/abstract_id=3825724.

⁴ Yasmin Ismail, *E-commerce in the World Trade Organization: History and Latest Developments in the Negotiations Under the Joint Statement*, INT’L INST. SUSTAINABLE DEV. 14 (Jan. 2020).

⁵ Shin-yi Peng, Ching-Fu Lin & Thomas Streinz, *Artificial Intelligence and International Economic Law: A Research and Policy Agenda*, in ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ECONOMIC LAW: DISRUPTION, REGULATION, AND RECONFIGURATION 1, 18 (2021).

To this end, the United States pioneered new provisions on cross-border data transfers and requirements to use domestic computing facilities in the original Trans-Pacific Partnership (TPP), and subsequently—despite its withdrawal from TPP—in the U.S.-Mexico-Canada Agreement (USMCA) and a dedicated “digital trade” agreement with Japan. These provisions require countries to not restrict the “free flow” of data (including personal data), unless there is a legitimate public policy objective that is being pursued in a non-arbitrary, non-discriminatory, or disguisedly trade restrictive manner and that does not impose greater restrictions than necessary to achieve the objective.⁶ The resulting ability to transfer and store data transnationally is susceptible to regulatory arbitrage and de facto multilateralization due to the reliance on investment law categories which enable multinational corporations to benefit from these provisions even when their home jurisdiction is not or no longer a party to the agreement.⁷ The U.S.-designed model inaugurated in TPP was endorsed by the remaining eleven countries that resurrected the agreement as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). It reflects a “Silicon Valley Consensus” that favors private sector interest in transnational data mobility by constraining states’ ability to restrict and thereby regulate transnational “data flows.”⁸

The European Union has been apprehensive about these kinds of commitments due to concerns that they might interfere with its General Data Protection Regulation (GDPR), which restricts cross-border transfers of personal data to third countries.⁹ Initially, the EU took the position that the “free flow” of personal data was non-negotiable, because data protection and privacy are fundamental rights.¹⁰ After lengthy internal deliberations that revealed tensions between the competent authorities within the European Commission, the EU presented a new template of horizontal provisions for cross-border data flows *and* for personal data protection in EU trade and investment agreements.¹¹ This template reconciles the competing interests by only restricting the data localization measures the EU does not deploy while protecting its data protection law from challenges. The EU has since tabled negotiation proposals reflecting this template in various negotiations, including the WTO’s JSI initiative. However, the post-Brexit negotiations with the United Kingdom that culminated in the EU-UK Trade and Cooperation Agreement (TCA) revealed the limits of the EU’s ability to turn its template into treaty law. The United Kingdom managed to downgrade data protection and privacy to mere rights (rather than fundamental rights) and to insert a novel commitment that ensures that instruments under conditions of general application (and not just entity by entity) are available to facilitate cross-border transfers of personal data.¹²

China long refrained from designing new international economic data law in its preferential trade and investment agreements.¹³ Its intricate domestic data governance regime features various forms of data localization that not only restrict cross-border transfers of data, as the EU’s GDPR does, but may indeed require not just territorial storage and processing but also local ownership over the relevant infrastructure. Yet, in November 2020, China signed the Regional and Comprehensive Economic Partnership (RCEP) agreement between the ASEAN countries and its trading partners,

⁶ See, e.g., Trans-Pacific Partnership, Arts. 14.11, 14.13.

⁷ Thomas Streinz, *Data Governance in International Economic Law: Non-territoriality of Data and Multi-nationality of Corporations* (manuscript on file with author).

⁸ Thomas Streinz, *Digital Megaregulation Uncontested? TPP’s Model for the Global Digital Economy*, in MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP 312 (Benedict Kingsbury, et al. eds., 2019).

⁹ Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119/1, ch. V (May 5, 2016).

¹⁰ EU Charter of Fundamental Rights, Arts. 7–8.

¹¹ The template is available at <https://perma.cc/9R6Z-T7XW>.

¹² EU-UK Trade and Cooperation Agreement, Art. 202.

¹³ See, e.g., Protocol to Upgrade the Free Trade Agreement Between the Government of the People’s Republic of China and the Government of the Republic of Singapore, App. 6, new ch. 15.

which created yet another model for international economic data law. Ostensibly modeled after TPP, RCEP echoes the principal commitment toward “free data flows” but grants much more leeway to countries to decide for themselves—rather than under external scrutiny—which restrictive measures *they* deem necessary.¹⁴ Security-oriented measures, in particular, enjoy absolute protection.¹⁵ To the surprise of some, China eventually if only belatedly also joined the WTO’s JSI on electronic commerce, where it has advanced a relatively narrow conception of “electronic commerce” that focuses on Internet enabled trade in goods and related payment and logistics services. In line with RCEP’s model, China consistently pushes for strong exceptions to guarantee cybersecurity and to safeguard “cyberspace sovereignty.”¹⁶

Due to their different approaches to internal and external data governance that are also reflected in their submissions to the JSI, the United States, the European Union, and China are often portrayed as distinct “data realms” with different approaches to global data ordering.¹⁷ In this narrative, the United States advances the “Silicon Valley Consensus” favored by its dominant platform companies; the European Union pursues a stringent regulatory agenda gravitating around the GDPR’s protections of personal data as fundamental rights; and China maintains the legal-infrastructural protections of its “Great Firewall” which caters to authoritarian security interest as well as protectionist economic interests. While there is some truth to this narrative, designing new international economic data law may require a more nuanced and more complex account. While it is true that the United States championed an agenda of “internet freedom” since the 1990s, its restrictive measures leveled against Chinese telecommunications infrastructure (Huawei) and social media platform providers (Tencent’s WeChat and ByteDance’s TikTok) illustrate that its erstwhile and principal commitment to “free data flows” is contingent and certainly not absolute.¹⁸ While the GDPR remains at the heart of its supranational data law, the EU is crafting a broader array of regulatory instruments recalibrating data relations. These initiatives are not focused on protecting Europeans’ fundamental rights but seek to achieve a European version of “digital sovereignty” to regain regulatory control and to jumpstart the lagging European digital economy. Meanwhile, China is creating sophisticated data governance frameworks that often incorporate concepts from European data law. As the Chinese Communist Party seems keen on reigning in its powerful technology companies domestically, these same companies continue to play important roles in its ‘Digital Silk Road’ strategy which shapes data governance regimes abroad, especially in Central Asia, Latin America, and Africa, by supplying digital infrastructure.¹⁹

The United States, the European Union, and China—in distinctive yet sometimes functionally comparable ways—have exercised considerable influence over the digital destinies of people around the world. Designing new international economic data law is but one and certainly not the most important lever of influence. However, policymakers and civil society in other countries must be aware that long-lasting meta-regulatory frameworks are being created which may not cater

¹⁴ Thomas Streinz, *RCEP’s Contribution to Global Data Governance*, AFRONOMICS LAW (Feb. 19, 2021), available at <https://perma.cc/HQJ4-QN42>.

¹⁵ See Regional and Comprehensive Economic Partnership, Arts. 12.14, 12.15.

¹⁶ Henry Gao, *Across the Great Wall: E-commerce Joint Statement Initiative Negotiation and China*, in ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ECONOMIC LAW: DISRUPTION, REGULATION, AND RECONFIGURATION 295, 310 (Shin-yi Peng, Ching-Fu Lin & Thomas Streinz eds., 2021).

¹⁷ See, e.g., Susan Aariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. INT’L ECON. L. 245 (2018).

¹⁸ See also Sarah Bauerle Danzman, *National Security, Investment Review, and Sensitive Data*, 115 ASIL PROC. (2021).

¹⁹ Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China’s “Digital Silk Road” as Transnational Data Governance*, 54 N.Y.U J. INT’L L. & POL. __ (forthcoming 2021), available at <https://ssrn.com/abstract=3810256>.

193 to the rights, interests, and needs of the diverse publics they represent and serve. The design of new
194 international economic data law also presents an opportunity for other countries to challenge digi-
195 tal hegemony and to develop alternative proposals. India, which pursues a digital industrial policy
196 in tension with the anti-protectionism consensus enshrined in international economic law, and
197 South Africa, which is involved in the African Union's digital transformation strategy for
198 Africa that emphasizes digital sovereignty, have challenged the legitimacy and legal status of
199 the WTO's JSI.²⁰ The negotiations for a protocol on electronic commerce to be added to the
200 African Continental Free Trade Area (AfCFTA) may be an opportunity to develop an African
201 approach toward international economic data law outside the WTO.

202 If the WTO fails to engineer a compromise between its members that participate in the JSI on
203 "electronic commerce," attention and political support for designing new international economic
204 data law will likely shift toward bilateral and regional digital economy agreements (either stand-
205 alone or as part of "comprehensive" trade and investment agreements). Such efforts will continue
206 simultaneously and in continuous correspondence with domestic data regulation, which can have
207 significant transnational implications, as the EU's GDPR demonstrates.²¹ Private sector dominated
208 standard-setting organizations play outsized and expanding roles in the digital domain, which may
209 require a reckoning with how their activities interface with domestic law and international eco-
210 nomic law. To retain relevance and to contribute to human flourishing, the designers of new inter-
211 national economic data law may need to switch focus. Rather than leveraging hard to change and
212 even harder to leave treaty commitments to meta-regulate if, when, and how countries can regulate
213 and thereby self-determine their transition toward digitally mediated societies and economies,
214 international economic data law should focus on facilitating interoperability between different
215 data governance approaches without imposing uniformity. This kind of international economic
216 data law would allow for experimentation and flexibility while retaining compatibility and accept-
217 ing a certain degree of uncertainty.

218 In any case, as international economic law expands its remit to encompass a broad array of data
219 governance questions, its substance and design process warrant critical scrutiny. When designing
220 new international economic data law, one must ask which issues to address or prioritize and whose
221 interests are being served: Are novel restrictions imposed by governments the most pressing issue
222 or might quasi-monopolistic infrastructural control over "data flows" by platform companies war-
223 rant more attention? Is the traditional separation of trade and tax sustainable when sophisticated tax
224 avoidance schemes deprive governments of the public funds they might need to build critical digi-
225 tal infrastructure or to support those who are adversely affected as their lives become increasingly
226 datafied and algorithmically governed? Can international economic data law be designed to
227 encourage mitigation of the significant greenhouse gas emissions caused by energy-hungry data
228 centers? Finding answers to these and many other questions requires rigorous public debate within
229 and across countries and institutions, robust civil society involvement, and reliable data.
230 Unfortunately, the venues in which international economic data law is being designed tend to oper-
231 ate as if these were conventional trade negotiations in which offensive and defensive interests are
232 being traded off by adjusting market access commitments or tariff schedules. To gain (rather than
233 assume) institutional legitimacy, the design of international economic data law must be more trans-
234 parent and participatory in ways that help equalize power imbalances. While the fear that opening
235 up the design process in this way might complicate or derail negotiations is understandable, this is a
236 challenge to be embraced rather than a problem to be avoided. As the Paris Climate Agreement

237
238 ²⁰ WTO General Council, The Legal Status of "Joint Statement Initiatives" and Their Negotiated Outcomes, WTO Doc.
239 WT/GC/W/819 (Feb. 19, 2021).

240 ²¹ ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD, ch. 5 (2020).

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 rule-making 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* 

Q1
Q2

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 TikTok¹ 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-idUSKBN07W](https://www.reuters.com/article/usa-tiktok/chinas-bytedance-challenges-trumps-tiktok-divestiture-order-idUSKBN07W).

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](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).

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

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

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

322 I. THE POLITICAL ECONOMY OF INVESTMENT SCREENING

323 The political economy of investment screening today, and particularly in the United States is
324 fascinating and puzzling. There has been far less pushback, at least publicly, from the domestic
325 business community than standard political economy theory would predict. The Foreign
326 Investment Risk Review Modernization Act of 2018, or FIRRMA,⁵ which substantially strength-
327 ened the powers of CFIUS, easily passed the U.S. Congress on a broadly bipartisan basis and with
328 little formal counter-lobbying from business groups. Where we do see concern from the business
329 community is typically not on whether to create stronger investment screening mechanisms or not
330 but rather how to implement these rules in a way that will not harm domestic industry. FIRRMA
331 provided CFIUS with the ability to review non-controlling, non-passive investment in U.S. critical
332

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

335 ⁵ Title XVII, Pub. L. 115-232.

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 supports nominally private firms in ways that are seen as unfair. It also can exert much more levers of de facto control over these firms than is possible for the United States 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).

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

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432