Cross-Border Data Policy: Opportunities and Challenges

Robert D. Atkinson and Nigel Cory

Abstract *Data governance* and the *management of global digital data* flows pose immense challenges for *global governance.* International digital data agreements must be embedded in revisions of the *global "rules based" order* that emerged out of *Bretton Woods* in the aftermath of World War II to manage global economic issues. In that spirit, the countries that value a *rules-based global digital economy* need to come together to enact *new global data management rules.* It is becoming more and more critical to treat data as the key driver of today's global economy. Creating new rules will require policymakers to alter their current approaches, which have led to a stalemate in making progress on *frameworks for the global internet*. China should revise its restrictive approach so that it can play a more constructive role in debates and negotiations between like-minded countries. On *China and internet rules*, if the Chinese Government retains its restrictive approach to data, AI, and digital trade, it will increasingly find itself excluded or marginalized in global discussions on digital issues. Many other countries see the Chinese approach as far from the baseline of emerging global norms and as self-serving for China from a trade perspective.

Keywords Data governance · Management of global digital data · Global governance · Global "rules based" order · Bretton Woods · Rules-based global digital economy · New global data management rules · Global internet frameworks · China and internet rules

1 Introduction

Global data and digital economy governance are increasingly critical to every country's efforts to support innovation and productivity. Yet, it is an area where little progress has been made at the international level in building a framework for an open, rules-based global digital economy.

R. D. Atkinson (✉) · N. Cory
Information Technology and Innovation Foundation (ITIF), Washington, DC 20001, USA

H. Wang and A. Michie (eds.), *Consensus or Conflict?*, China and Globalization,
https://doi.org/10.1007/978-981-16-5391-9_20

These conflicts arise over a myriad of issues, such as free speech, intellectual property, privacy, cybercrime, consumer protection, taxation, commercial regulation, and others. This means the Internet has ended up being guided by both formal and informal rules by international, national, and subnational bodies (whether governmental or non-governmental) throughout its history (Castro 2013).

How a country's domestic regulations impact how its firms and consumers can access and use the Internet and other digital technologies is emerging as a key differentiator in the global race of economic and innovation advantage—which both China and the United States want to win. However, China's restrictive approach to data governance and the digital economy needs to change if it wants to win that race.

China's approach to digital policy is one among many. The key question today is how a world, extremely diverse in income levels, cultures, and types of government, will deal with global technologies and global firms. The differences are significant. Some, including China's data and digital economy governance framework, prioritizes government control, domestic firms and domestic digital economic growth and innovation. The United States and many other nations more easily allow firms and consumers to freely access global markets, platforms, and new and innovative digital products. China should rebalance its approach to allow greater openness for commercial and trade-related digital engagement, lest it miss out on maximizing the benefits of the Internet and working with trading partners on building a new open, rules-based digital economy.

2 The Need for a Universal Internet Architecture

There has not been much progress on building a framework for a global digital economy as the push for a single, universal approach to the Internet is embedded within many early discussions, initiatives, and frameworks for the global digital economy. As this essay explains, a universal approach to managing the technical architecture of the Internet is needed, otherwise the Internet will not work. However, as it relates to the policy layer in how laws and regulations affect how people and firms use the Internet, data, and digital technologies, there can be policy differences in how countries manage the Internet. However, where there are substantive shared interests—whether for economic or social reasons—countries should ensure these are aligned. In the global digital economy, key areas for cooperation involve cross-border data flows related to trade, actions against cyber crime, and competition policy.

The United States and China are both leaders in the global digital economy. The reason is that they have a key natural advantage in the global digital economy—scale of their economies and populations. Because digital industries, especially information (including search engines and social networking) and e-commerce, are characterized by scale and network effects, US and Chinese firms are able to capitalize on early leads to be competitive in the global market (Foote and Atkinson 2020). Yet, despite their success, China and the United States' conflicting approaches to managing the domestic and global digital economy demonstrate the current stalemate

over Internet policy. China's domestic data governance and digital economic policy is based on state control and keeping most data inside China's borders, while the United States' approach is defined by openness, light-touch regulation, and digital globalism. Yet, these differences do not mean that a new mutually beneficial and acceptable approach to the global digital economy cannot be developed—one that more specifically acknowledges that countries can take conflicting approaches to Internet policy, while working together where there are shared economic benefits.

Every country benefits from a global digital economy framework that supports data-driven innovation and digital trade. While China's digital economic model differs from that of the United States (as well as the European Union), it does not mean that these nations and regions cannot find areas—such as digital trade—that are mutually beneficial, and thus, worthy of building alignment. This essay makes the case that China should reform its current approach to build a clear, mostly open, and innovation-friendly data and digital economy governance framework. China's current model will entail growing costs in the future, as more and more countries seek to work with like-minded partners to build an open and rules-based global digital economy. China's impressive digital economic development would be at a disadvantage if it were to miss the chance to compete in the next phase of the global digital economy.

3 Why China Needs to Help Build a Clear, Mostly Open, and Innovation-Friendly Data Governance Framework: A State-Controlled Internet Only Goes so far

China should revise its current approach—with restrictive national security interests outweighing economic competition, innovation, and trade interests—as the cost of this approach will only grow as digital technologies become central to global innovation and trade (Shen 2016). A number of nations, including Australia, Canada, Chile, Peru and Singapore, are pursuing new international digital economy agreements to put in place new rules and regulatory cooperation to ensure their firms and digital economies are more integrated, innovative, and competitive. As domestic digital economic frameworks become more common and mature around the world, more countries will be looking to see which of their trading partners are willing to work together on mutually beneficial digital economy arrangements. Piece-by-piece, these represent an emerging opportunity for countries like China to ensure its firms and consumers can benefit from access to each other's digital economies.

There are also increasing discussions around a global digital trade framework such as former Japanese Prime Minister Shinzo Abe's initiative for "data free flow with trust," launched at the G20 (Cory et al. 2019). More countries are joining the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules, which is an adaptable approach to ensure that firms are held accountable for managing local data wherever they transfer it. In addition, there are ongoing negotiations among 70-plus countries

at the World Trade Organization (WTO) on new e-commerce and digital trade rules.[1] And the Organization for Economic Co-operation and Development (OECD), has emerged as a central hub for research and debates about many global digital economy issues.

A common theme among all these initiatives is that countries can maximize the benefits of the digital economy when they cooperate. However, China is not central to these initiatives. As such, it risks being left behind.

4 Key Internet Conflicts

The key question is how different countries deal with the internet and global firms using it. There are several areas of conflicts over global Internet policy: internet governance, data and AI governance and ethics, content moderation, and government surveillance or censorship. To build a new global digital economic framework, countries will need to address these by building compatible approaches that are not overly restrictive of digital trade and data-driven innovation. China, the European Union (EU), and the United States provide three differing models and approaches.

4.1 Internet Governance—Differences Between China, the US, and the EU

Internet governance refers to the norms, rules, and technologies that govern the working of the Internet internationally. China advocates for a state-controlled Internet, including at the International Telecommunication Union and other forums it supports, such as the China-hosted World Internet Conference (Segal 2020; Eichensehr 2014). China's limits on allowing free flow of data across borders means it largely avoids making any commitments on these issues in its trade agreements. It has also opposed language on these issues at the G20 and elsewhere.

The United States advocates for a multi-stakeholder-based approach to the Internet that is based on a voluntary, industry-based, and bottom-up standards process, which pushes back against government efforts to dictate how the global internet should work. It advocates for this approach at the ITU, the Internet Corporation for Assigned Names and Numbers (ICAAN, responsible for coordinating databases related to the namespaces of the Internet), and the Internet Governance Forum (Yang 2019). The United States also pursues new trade rules to support data flows and digital trade in bilateral, regional, and multilateral forums and agreements, such as the United

[1] "Australia-Singapore Digital Economy Agreement," https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement; "Digital Economy Partnership Agreement," https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement.

States–Mexico–Canada trade agreement. The United States' global digital economic policies are often fused with broader efforts to support human rights, like freedom of speech, on the Internet.

At the heart of the EU's international strategy is the push for other countries to also adopt the precautionary principle and to harmonize their data privacy laws to its General Data Protection Regulation (GDPR). GDPR imposes a general prohibition on transfers of EU personal data to only a small group of foreign countries (mainly former colonies) it has determined provide an "adequate" level of protection equal to data protection at home (Atkinson 2015). The EU also supports certain policies that it wants applied to global Internet, such as the impact that GDPR has had on certain ICANN functions (such as identifying domain name holders for criminal investigations and other purposes) and the "right to be forgotten" (which allows a person to have private information removed from Internet searches and other directories, which the EU wants applied not just domestically, but to the global Internet). Overall, the EU tends to support the multi-stakeholder approach to other global Internet issues, but where these conflict with its own laws, it is willing to undermine global cooperation to enact its own (conflicting) approach.

4.2 Data and AI Governance Conflicts

Data governance is the most prominent global conflict within Internet policy. This involves data privacy and protection, portability and sharing, cybersecurity, and government access to data (whether for law enforcement investigations, national security, or political purposes). However, AI governance is also fast emerging as a growing flashpoint. This involves debates about AI development, ethics, and accuracy and explainability.

China's domestic data governance is based on the goal of "cyber sovereignty." China's commercial data privacy framework is evolving and rebalancing from a largely laissez faire approach to how firms use data by adding greater consumer protection (Shi 2020). China requires a range of data to only be stored locally and for the government to have wide ranging access and control over it and the broader digital economy.[2] While the desire for government access to data can make sense, China can achieve this goal by requiring copies of data to be maintained in China, while still allowing data "exports." China also has pursued an active "digital industrial policy" to support growing digital economy firms. However, this has usually meant that Chinese firms have benefited more than foreign digital firms. Some of the world's leading digital firms, including many from the United States, are banned or blocked in China (Cory 2020). While China's approach to AI ethics/governance is still at a

[2]Recently reinforced in the draft Personal Information Protection Law, which would expand data localization requirements beyond the "critical information infrastructure" (CII) operators covered in the Cybersecurity Law, requiring non-CII operators in general to store personal data locally if the amount of such data reaches certain thresholds set by the government (Article 40); Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules."

very early stage, it is heading in a similar direction, given its focus on self-sufficiency (Laskai and Webster 2019).

The United States is focused on a light-touch approach to Internet regulations, such as privacy and AI. From the Clinton administration Internet governance principles crafted by Ira Magaziner, to efforts by the Trump White House supporting a light-touch approach to AI regulation, the US government has generally avoided innovation-harming regulatory regimes and sought to convince other nations of the wisdom of this approach (Thierer 2012).

The EU has embraced the "precautionary principle" where new innovations are approached from a "glass half empty" view, with the urgent need to form a commission of experts—largely academics and "civil society" representatives with little connection to actual R&D and commerce—to study the innovation and how it could be harmful (Kop 2020). The dominant narrative in Brussels is that the strict regulation of privacy, AI, and other emerging technologies is required in order to boost consumer trust, which in turn will give EU firms a leg up over their American and Chinese competitors (McQuinn and Castro). The EU's emerging AI governance framework is applying a similarly restrictive and protectionist approach in favoring local (over foreign) AI and standards.

The EU's all-consuming fears about government surveillance—following the European Court of Justice decisions in *Schrems I* and *II*—means that its evolving data governance framework makes it increasingly difficult to transfer EU personal data outside the region, which acts as a barrier to trade for foreign firms (Cory et al. 2020). The EU singles out the United States for actions that it does not even restrict among its own member states (in terms of surveillance and government access to data). However, recent data and AI-related policies show that this is expanding to include firms from China and other countries. In the context of foreign AI developed by foreign firms (especially China), Commissioner for the Internal Market, Thierry Breton, said firms that develop and use AI could be forced to "retrain algorithms locally in Europe with European data," adding that, "We could be ready to do this if we believe it is appropriate for our needs and our security." Mobike and TikTok have already attracted greater regulatory scrutiny. This will likely continue as Chinese tech firms and their products become more prominent in Europe and elsewhere around the world.

4.3 Content Moderation and Censorship

The conflict over online content moderation and censorship is essentially a proxy for the broader conflict over the role of government and human rights in the digital economy. How countries define what content is legal and illegal online and assign legal responsibility (or protection from liability) to Internet platforms and other intermediaries is changing around the world. This is a massive challenge: every minute, more than 500 hours of video are uploaded to YouTube, 350,000 tweets are sent, and 510,000 comments are posted on Facebook (Karanicolas 2020). Yet,

how countries go about making their respective approaches as clear, predictable, and as targeted as possible is necessary. This is due to the growing role that digital (creative) content creators and Internet platforms and intermediaries play in global trade and innovation.

Many countries are trying to address a range of legitimate issues, such as hate speech, disinformation, copyright infringing material, child pornography, terrorism-related material, and other issues (Liang and Lu 2012). But beyond efforts to address specific types of content, many democratic nations share a concern about countries like China that remove or block access to content for political purposes (Rayburn and Conrad 2014; Zittrain and Edelman 2003). Conflicts arise as the global nature of the Internet means that content that is legal in one country can be illegal in another. For example, content that is considered hate speech in Germany or is considered politically sensitive in China or Vietnam would be protected as free speech in Australia, the United States and many other countries.

The clearest conflict between the United States and China is over free speech and political censorship. The United States advocates an open internet where nearly all content on the Internet is available to citizens, because of the belief in the ultimate democratizing and empowering force of information. The United States has also created a legal framework that provides legal liability protection for Internet-based intermediaries if they take reasonable steps to remove illegal content, such as via the Digital Millennium Copyright Act and Section 230 of the Communications Decency Act. However, the debate in the United States (and internationally) is often about where to draw the lines around legal and illegal content online. This dialogue is distorted as many cyberlibertarians and open Internet advocates misguidedly equate any efforts to address, block, or remove illegal content online as censorship.

While both the United States and China block content that they deem illegal, the definition of that content is much broader in China. The 'Great Firewall' of China blocks thousands of foreign websites and limits domestic content (Griffiths 2019). Even though political and social concerns may be a central motivation, some have argued that China's internet censorship has served its economic ends in blocking foreign platforms and digital goods.[3]

4.4 Government Surveillance and Requests for Data for Law Enforcement Investigations

Government access to data—both law enforcement and surveillance-related—is emerging as a major point of conflict.

[3]Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade | ITIF.

Countries have used the specter of foreign government surveillance—both real and imagined—to justify restrictions on data and international data flows.[4] Policymakers fear that data is being accessed directly through a firm's in-country facilities or indirectly via extraterritorial requests for data or operations that target data transferred and stored overseas.

The 2013 Snowden disclosures about US surveillance were the initial catalyst for policy changes around the world, especially in China and Europe. (In 2013 Edward Snowden leaked a vast amount of secret data from the US National Security Agency). The irony is that many of the same Western and democratic countries that denounced US surveillance on the behalf of their citizens, have enacted their own surveillance regimes (Cate and Dempsey 2017). Furthermore, the debate on national security and data flows is often misleading and disingenuous, as countries use national security in a broad and vague manner to enact restrictions on a growing range of data and digital services that are largely commercial, and not directly tied to national security.

Some countries have used the fear of foreign government surveillance to enact restrictive data governance systems that help them control data for political and social ends, which at times means cutting themselves off from the global Internet. China's broad use of national security permeates its data governance, cybersecurity, and related laws.[5] The vague and sweeping nature of Chinese law, combined with the lack of legal checks and balances, gives China the capability to pursue a broad range of data, but it is unclear as to what extent it actually uses this power.

Government concerns over cross-border access to data for law enforcement investigations is another emerging point of conflict. As the threat of global cybercrime rises, there is an increasing need for a better process to manage cross-border requests for data. Yet, cross-border digital law enforcement cooperation is complicated. Requests can involve data that implicates multiple stakeholders, people, and jurisdictions. This may cover the nationalities of the individuals or organizations that own the data, the service providers storing the data, the individuals or organizations accessing the data and, if the data contains personally identifiable information (PII), the individuals described in the data. In today's digital world, it is not hard to see how criminal investigations in one country may involve an email stored in another country and a bank account in yet another.

There are significant differences in how different countries' legal systems facilitate data sharing for law enforcement purposes. Existing legal tools (such as mutual legal assistance treaties) are out-of-date and slow, yet new tools are emerging, such as the US's CLOUD Act agreements (which will make the process much more efficient, while keeping legal safeguards in place) (McQuinn and Castro 2017). Rather than seeking to improve domestic and international legal frameworks to improve cross-border law enforcement cooperation, some policymakers in Brazil, China, India and

[4]Surveillance is defined as: "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction (Lyon 2007)."

[5]China's Cybersecurity Law states that key IT services only store "important data" within China, which includes "data that, if divulged, may directly affect national security, economic security, social stability, or public health and safety" (Creemers et al. 2018); Although China's government tries to caveat this by stating it does not generally include firm-related data (Tai et al. 2019).

elsewhere have supported data localization as they think it is the only way to get local and foreign firms to respond to requests for data from law enforcement and other agencies. This stems from the mistaken belief that firms can avoid oversight and requests for data by simply transferring data out of the country.

5 What is at Stake—A More Integrated and Prosperous Global Digital Economy or Chinese Digital Mercantilism?

Maximizing the benefits of digital technologies will take countries working together to create new norms, rules, and frameworks. On one side: China, the EU and Russia are creating their own walled-off digital economies. On the other side: Australia, Canada, Chile, Japan, Mexico, New Zealand, Peru, Singapore, the United Kingdom, the United States and others are working towards new rules and governance. In the middle: the vast majority of countries who have not yet decided which model they want to follow.

Central to China's challenge is the recognition that its domestic economic interests—characterized by the rise of Baidu, Alibaba, Tencent and other innovative firms—increasingly align with the needs to create a framework that allows greater global data flows and digital trade (Ramamurti and Hillemann 2018; Xinyi and Gereffi 2018). The alternative—a "Balkanized" fragmented global Internet that gives nations the right to act as they please—will inevitably hurt China and its firms.

6 Building a More Pragmatic and Integrated Global Digital Economy

Nations are struggling to address cross-border Internet policy issues. One reason is that efforts are not guided by a coherent policy framework. Four principles should guide these efforts.

6.1 Principle 1: Adopt a Pragmatic Framework for Cross-Border Internet Policy

Countries need to recognize that when it comes to policies about how the Internet is used, there can be differences among nations. Figure 1 offers a four-cell typology of issues where there can and cannot be consensus and policy issues that involve public benefits and public harms. An example of a policy that can be based on consensus, and involves harms, is restricting child pornography. Every nation agrees with this

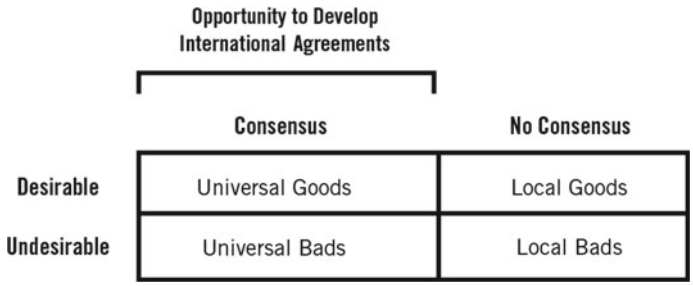

Fig. 1 Typology of Internet policy goals affecting individuals outside the country

goal. The clearest example of a universal good, and thus the need for universal rules, pertains to frameworks on core Internet architecture and protocols, as the Internet needs commonly shared global standards. A multi-stakeholder approach to maintaining this goal is desirable, as debates and disagreements over the technical architecture and protocols of the Internet can only be resolved with stakeholder consensus. Because there is a presumed global consensus on trade—as evidenced by membership in the World Trade Organization—there should, at least in theory, be able to be a consensus on digital trade issues.

In contrast, issues of data privacy involve a local good, and will be difficult to generate global consensus. Likewise, Internet content moderation is usually a local bad (blocking harmful or objectionable content), but there is unlikely to be consensus among countries (besides on specific content, like child pornography) on what content should be blocked. However, policymakers can still agree that whatever framework a country adopts does not act as a barrier to trade.

A central challenge is that many countries associate data governance with political and social control. Therefore, these countries will oppose global efforts to harmonize rules on data privacy (such as the EU's GDPR). Given the current values-based approach to global Internet policy, these countries are likely to be intractable in coming up with principles and mechanisms that allow robust encryption, privacy, and content moderation and related issues. Every nation needs to recognize that not every country it deals with on the global digital economy will share its values. This is a distinction that policymakers already acknowledge offline with traditional trade.

Ultimately, policymakers need to recognize the critical policy distinction—between policies with global consensus and those without. In many cases, this consensus will (at best) be widespread but not unanimous. Given this reality, it is better that a consensus-based approach be ambitious, but pragmatic, in seeking shared principles and agreements among a like-minded group of countries that represent a substantial part of the global economy and value a mostly open, rules-based global digital economy (see Fig. 1) (Castro and Atkinson 2014).

6.2 *Principle 2: Data Governance—Focus on Accountability and Legal Nexus, not the Geography of Data Storage*

Perhaps the most challenging global internet policy issue relates to cross-border data flows. Rather than tell firms where they can store or process data, policymakers should hold firms that have legal nexus within their borders accountable for managing data they collect, regardless of where they store or process it. This expectation could be made clear in law by declaring that companies doing business in a country are legally responsible for any failures to manage data from that country, regardless of whether those failures are the fault of the firm in that country or abroad, or an affiliate or business partner in that country or abroad. In other words, a country's data-protection rules would travel with the data. The accountability principle is based on the fact that modern technology, especially the Internet and cloud data storage, means that each country's domestic regulatory regime for data (such as for privacy) needs to be globally interoperable given that each country faces the same challenge in applying its laws to firms that may transfer data between jurisdictions. Interoperable privacy frameworks are the international extension of this accountability-based approach such that data is still able to flow between different privacy regimes, and countries data protection rules flow with it.

Interoperability is already at the heart of many countries' data privacy frameworks and at global discussions on data privacy, such as at the OECD and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules system.[6] As per ITIF's typology, interoperability is fighting to be the global consensus, as it is a mutually acceptable and beneficial principle to countries, regardless of their political system, their approach to data privacy, or level of development (as opposed to the disadvantages of harmonization and localization). Such an interoperable system would focus on "global protections through local accountability."

While the EU's data protection rules have gained some global traction over the past year (in its efforts to push for a global, harmonized approach to data privacy), there is no reason to suspect that in the future another country or region might not put forth competing rules. For example, imagine if China created its own set of data protection rules and declared that any country wanting to do business in China must have identical data protection laws. Such a scenario would potentially force countries to choose one privacy regime or another. Such a clear divergence would simply deepen the splinternet. This is why it is unrealistic and impractical to demand universal rules on privacy. A better option would be to create an interoperable, accountability-based system that works for all countries and the various ways they enact data privacy and protection.

---

[6] "OECD Privacy Guidelines," https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm; "Current Developments in Privacy Frameworks: Towards Global Interoperability," OECD website, November 1, 2011, http://www.oecd.org/digital/ieconomy/currentdevelopmentsinprivacyframeworkstowardsglobalinteroperability.htm.

6.3 Principle 3: Apply Domestic Regulation to Address Challenges of Unwanted Digital Services and Products

Many nations and regions, especially Europe, are pushing for a regime of global AI regulation, rightly understanding that not all AI systems will comport with EU values or laws.[7] And while global efforts to develop and implement AI governance principles (such as that AI systems should minimize undesirable AI bias) are useful and warranted, going further and codifying these into some kind of international legal agreements would be not only difficult to do, but also likely harmful to innovation. It would be difficult to do because just like privacy, it is unlikely that all nations will agree to a single standard. It would be potentially harmful because it is likely that the most restrictive rules would be put in place, limiting the ability of digital and AI developers to innovate.

Just as nations now have the right to regulate the safety of material products (such as cars, food, pharmaceutical drugs) and limit imports that do not meet these standards, they have the same right to do the same with digital products, including ones with AI in them. There is no global standard on genetically modified organisms (GMOs), for example, which is a good thing because it means that countries that take a science-based approach to GMO-based crops, are able to produce and sell to other like-minded nations. While there is no single, harmonized approach to regulating these and other trade-related issues, countries have shown that they can agree upon shared principles and processes in how they regulate these issues so that they share commonalities and that a country's system is generally interoperable with those in other countries. For example, the World Trade Organization's core principles of non-discrimination, most-favored-nation, and transparency and the OECD's privacy principles.[8] These shared principles help ensure countries can address legitimate public policy objectives, but in a way that ensure that domestic regulation is not used as a de facto trade barrier. For digital issues, this would mean that countries could pursue different domestic policy regulatory regimes that are interoperable and supporting digital trade as they form part of an integrated global digital economy.

6.4 Principle 4: Recognizing, Reconciling, and Addressing Conflicts over Valued-Based Digital Content

It is critical to recognize that countries can have conflicting rules and regulations regarding values-related digital content (in terms of how each country determines what is and is not illegal online). Countries that are realistic about the task of building

[7] https://www.sciencemag.org/news/2020/02/europe-plans-strictly-regulate-high-risk-ai-technology.

[8] "OECD Privacy Guidelines," https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm; "Principles of the trading system," World Trade Organization website, https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm.

a broad rules-based global digital economy need to accept (even if they do not necessarily like) the fact that some countries censor information on the Internet for political and social purposes. Indonesia blocks websites and apps for displaying "harmful" material, such as pornography, terrorism-related material, or that related to the lesbian, gay, bisexual, and transgender community (Davies and Silviana). The EU does not have the same commitment to freedom of speech as the United States does. For example, online access to *Mein Kampf* is blocked in Germany, but not in the United States. Any global solution imposed on either country would violate key principles and values. Policymakers and advocates also need to recognize that the practice of authoritarian nations to limit access to certain websites and web pages does not constitute the breaking of the internet. The architecture is still the same and enables cross-border communication, just not all of it.

This principle is also based on the central recognition that not all website blocking constitutes a threat to the open internet. When talking about a data-driven global digital economy, it is important to recognize that not all data flows should be treated the same, as some data flows are rightly illegal. For example, over 30 countries (including many democratic, rule-of-law countries) use website blocking to prevent access to websites engaged in large-scale copyright infringement, illegal gambling services, financial fraud, and child pornography (Cory 2018).

A pragmatic global digital economy strategy will require changes from everyone. The United States needs to move away from an idealist view of digital international relations to a realpolitik one, which is focused more on protecting key economic interests rather than acting as a global ambassador of complete and unfettered Internet openness. Countries do and will continue to take differing approaches to moderating and blocking content online. Countries should develop clear, predictable, and non-discriminatory legal and administrative frameworks for all firms—both foreign and domestic—to use so that they know what online content is and is not illegal.

7 Conclusion

Just as there was a set of institutions, agreements, and principles that emerged out of Bretton Woods in the aftermath of World War II to manage global economic issues, the countries that value the role of an open, competitive, and rules-based global digital economy need to come together to enact new global rules and norms to manage a key driver of today's global economy: data. But doing so will require policymakers to make careful changes to their current approaches, which in many instances, have led to the current stalemate in terms of making progress on new rules, norms, and frameworks for the global Internet.

China should revise its restrictive approach to data and digital policies so that it can play a constructive role in debates and negotiations between like-minded countries. If China retains its restrictive approach to data, AI, and digital trade, it will increasingly find itself excluded or marginalized in global discussions on digital issues as other

countries will see its approach as far from the baseline of emerging global norms and as self-serving (and not mutually beneficial) from a trade perspective.

References

Atkinson R (2015) Don't just fix safe harbor, fix the data protection regulation. Euractiv. https://www.euractiv.com/section/digital/opinion/don-t-just-fix-safe-harbour-fix-the-data-protection-regulation/. Accessed 18 Dec 2015

de Bossey C (2005) Report of the working group on internet governance (ITU). https://www.wgig.org/docs/WGIGREPORT.pdf

Castro D, Atkinson R (2014) Beyond internet universalism: a framework for addressing cross-border internet policy (ITIF). http://www2.itif.org/2014-crossborder-internet-policy.pdf. Accessed Sep 2014

Castro D (2013) A declaration of the interdependence of cyberspace. ComputerWorld. https://www.computerworld.com/article/2494710/a-declaration-of-the-interdependence-of-cyberspace.html. Accessed 8 Feb 2013

Cate F, Dempsey J (2017) Bulk collection: systematic government access to private-sector data. Oxford University Press, Oxord. https://www.oxfordscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515

Cory N (2018) The normalization of website blocking around the world in the fight against piracy online. Innovation Files, blog post. https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online. Accessed 12 June 2018

Cory N (2020) Testimony to the U.S. Senate Subcommittee on trade regarding censorship as a non-tariff barrier to trade (ITIF, testimony). https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff. Accessed 30 June 2020

Cory N, Atkinson RD, Castro D (2019) Principles and policies for "Data Free Flow With Trust" (ITIF). https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust. Accessed 27 May 2019

Cory N, Dick E, Castro D (2020) The role and value of standard contractual clauses in EU-U.S. Digital Trade (ITIF). https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade. Accessed 17 December 2020

Creemers R, Triolo P, Webster G (2018) Translation: cybersecurity law of the People's Republic of China. DigiChina blog post. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Accessed 29 June 2018

Davies E, Silviana C (2018) New Indonesia web system blocks more than 70,000 'negative' sites. Reuters. https://www.reuters.com/article/us-indonesia-communications/new-indonesia-web-system-blocks-more-than-70000-negative-sites-idUSKCN1G30KA. Accessed 19 Feb 2018

Eichensehr K (2014–2015) The cyber-law of nations. Georgetown Law J 103:317–380

Foote C, Atkinson R (2020) Chinese competitiveness in the international digital economy (ITIF, November 23, 2020)

Griffiths J (2019) The Great firewall of China: how to build and control an alternative version of the internet. Zed Books Ltd.

Karanicolas M (2020) Moderate globally, impact locally: a series on content moderation in the Global South. Yale Law School. https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/moderate-globally-impact-locally-series-content-moderation-global-south. Accessed 5 Aug 2020

Kop M (2020) Quantum technology and the law. European Commission website. https://futurium.ec.europa.eu/en/european-ai-alliance/document/quantum-technology-and-law. Accessed 16 Nov 2020

Laskai L, Webster G (2019) Translation: Chinese expert group offers 'Governance Principles' for 'Responsible AI'. DigiChina blog post. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/. Accessed 17 June 2019

Liang B, Lu H (2012) Fighting the obscene, pornographic, and unhealthy: an analysis of the nature, extent, and regulation of China's online pornography within a global context. Crime Law Social Change 58(2):111–130

Lyon D (2007) Surveillance studies: an overview. Polity Press, Cambridge

McQuinn A, Castro D (2017) How law enforcement should access data across borders (ITIF). https://itif.org/publications/2017/07/24/how-law-enforcement-should-access-data-across-borders. Accessed 24 July 2017

McQuinn A, Castro D (2018) The scholarly evidence is quite clear that strong regulations deter innovation and don't spur more adoption. ITIF. https://itif.org/publications/2018/07/11/why-stronger-privacy-regulations-do-not-spur-increased-internet-use. Accessed 11 July 2018

Ramamurti R, Hillemann J (2018) What is "Chinese" about Chinese multinationals? J Int Bus Stud 49:34–48. https://doi.org/10.1057/s41267-017-0128-2

Rayburn M, Conrad C (2014) China's internet structure: problems and control measures. Int J Manag 21(4):471–480

Segal A (2020) China's alternative cyber governance regime (Council on Foreign Relations). https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.Accessed 13 Mar 2020

Shen H (2016) China and global internet governance: toward an alternative analytical framework. Chin J Commun 9(3):304–324. https://itif.org/publications/2020/11/23/chinese-competitiveness-international-digital-economy

Shi M (2020) China's draft privacy law both builds on and complicates its data governance. DigiChina blog post. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-privacy-law-both-builds-on-and-complicates-its-data-governance/. Accessed 14 Dec 2020

Tai K, Laskai L, Creemers R, Shi M, Neville K, Triolo P (2019) Translation: China's new draft 'Data Security Management Measures'. DigiChina blog post. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/. Accessed 31 May 2019

Thierer A (2012)15 Years on, President Clinton's 5 principles for internet policy remain the perfect paradigm. Forbes. https://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm/?sh=30b1c6fb7170. Accessed 12 Feb 2012

Xinyi W, Gereffi G (2018) Amazon and Alibaba: internet governance, business models, and internationalization strategies. Int Bus Inf Digit Age 13:327–356

Yang Y (2019) Mixed messages at China's tech summit. Financial Times. https://www.ft.com/content/b7d48d5e-ff65-11e9-be59-e49b2a136b8d. Accessed 6 Nov 2019

Zittrain J, Edelman B (2003) Internet filtering in China. IEEE Internet Comput 7(2):70–77

Robert D. Atkinson is the Founder and President of the Information Technology and Innovation Foundation (ITIF), a global top think tank for science and technology policy. He is an internationally recognized scholar and author whom The New Republic has named one of the "three most important thinkers about innovation." He holds a Ph.D. in city and regional planning from the University of North Carolina, Chapel Hill, where he was awarded the prestigious Joseph E. Pogue Fellowship. He earned his master's degree in urban and regional planning from the University of Oregon, which named him a distinguished alumnus in 2014.

Nigel Cory is an associate director covering trade policy at (ITIF). Cory holds a master's degree in public policy from Georgetown University and a bachelor's degree in international business and commerce from Griffith University in Brisbane, Australia.