June 29, 2022
Australia's Department of the Prime Minister and Cabinet
Andrew Fisher Building
1 National Circuit
Barton ACT 2600

Re: ITIF Submission on the Australian Data Strategy

To whom it may concern,

Please find below the Information Technology and Innovation Foundation's (ITIF) submission to the Department of the Prime Minister and Cabinet's inquiry into Australia's National Data Security Action Plan. The submission addresses the conceptual framing of the strategy and its consideration of data localization.[1]

Please let me know if you have any questions.

Sincerely,

Nigel Cory
Associate Director, Trade Policy, The Information Technology and Innovation Foundation
Email: ncory@itif.org

Table of Contents

OVERVIEW – WHY DATA LOCALIZATION IS A FAULTY FOUNDATION FOR AUSTRALIA'S NATIONAL DATA STRATEGY

Australia's National Data Security Action plan includes many useful ideas and questions, but also some seriously problematic ones, especially its framing of data as a national asset and its consideration of data localization (forcing firms to store data within a country's borders).[2] This submission addresses issues with the Action Plan's conceptual framing, before moving toward a detailed analysis of its consideration of data localization (question 5 of the Action Plan).

Policymakers are often mistakenly told that "data is the new oil." Yes, like oil, data is a valuable input to the economy. But unlike oil, data is non-rivalrous—one party using data does not reduce the amount of data available for others to use. And unlike oil, data is non-fungible—one piece of data cannot be substituted for another the way barrels of oils are interchangeable. Unfortunately, the "data is oil" analogy has led to some poorly conceived policy ideas, in particular the idea of data localization and data sovereignty.

Unfortunately, many protectionist (and often authoritarian) countries advocate a policy of "data sovereignty," the concept that governments should keep all domestic data local to ensure it remains subject to domestic rules. These ideas directly follow the economic principles put forth in the 1974 Declaration for the Establishment of a New International Economic Order by the United Nations General Assembly that called for "full permanent sovereignty of every State over its natural resources."[3] Policymakers following this line of thinking believe governments should treat data like a finite natural resource that must be protected from foreign actors seeking to exploit it for profit. Those who espouse this view see data as no different than any other resources a country may be naturally endowed with like oil or minerals.

Australia's National Data Security Action Plan also reflects some of this muddled thinking. It declares that "Australia's data is a valuable national asset requiring robust security settings" and that "inadvertently allowing another country to access Australia's most critical data will erode our sovereignty and control over

that data in the long term." In other words, Australian policymakers are trying to lock down domestic data out of concern that foreign actors may exploit it for unfair economic gain. However, in all cases, data sovereignty is thinly disguised protectionism. Indeed, these policies often gain traction because many policymakers conflate data protection and data protectionism.

Data protection is a legitimate effort to ensure the confidentiality, integrity, and availability of data. For example, policymakers should seek to protect sensitive information from inadvertent disclosures. Sensitive information includes both personal data and non-personal data that, if revealed, undermines privacy, safety, economic, and security interests. For example, sensitive information could be personal data about a person's health that reveals information the individual would prefer to keep private; intellectual property (IP), including trade secrets, that businesses want to protect; or non-personal information such as classified government data that undermines national security. In these cases, stronger data protection measures, particularly enhanced technical safeguards and better cybersecurity practices, can help prevent data breaches or other unintentional disclosures of sensitive information, including to foreign governments or firms.

But data protectionism is not focused on preventing the disclosure of sensitive information. Instead, it is focused on preventing those outside the country from generating value from data. While the goal of these policies is to maximize value for domestic companies, the net impact of these restrictions is almost certainly negative. The problem is that most data has little to no value until businesses do something with it. Therefore, the more businesses can gain access to data, the more value can be generated. Restricting foreign firms from accessing domestic data limits the potential universe of businesses that can add value to data. That means data holders—whether they are consumers or businesses—miss out on opportunities to benefit, directly or indirectly, from their data.

Consider an Australian radiology lab that has thousands of medical images. Data protection rules are completely legitimate to ensure that personal medical records remain private. However, Australia's data protectionism rules (under section 77 of Australia's Personally Controlled Electronic Health Records Act) prohibit organizations from transferring health records overseas.[4] This limits radiology labs from using non-Australian AI systems that could be faster and cheaper and more accurately interpret diagnostic imaging results. These restrictions result in potentially higher costs for Australian businesses and consumers, in addition to worse health care outcomes. It also means that Australia would be in a position to contribute less to improvements in global health outcomes.

Moreover, data protectionism does nothing to enhance data protection. Requiring data be stored in-country (or with domestically owned companies) does not impact the overall security of data. Australian data, for example, is not more secure in an online service simply because that service is owned and operated by an Australian company rather than an American one. The security of the online service depends on a series of technical, legal, and physical controls at the company. Countries that pursue data protectionism risk reciprocal actions by other governments. For example, Australian mining giant Rio Tinto collects data from around the world as part of its smart mining program to analyze geology, optimize energy use, and automate its

autonomous equipment. If other governments prohibited Rio Tinto from sending data back to Australia it would have a negative impact on the company.

Unfortunately, policymakers in many countries associate data localization and protectionism with the concept of digital sovereignty, which is not only misleading but actually undermines governments' efforts to ensure local laws and regulations apply online. Digital sovereignty and associated terms such as 'cyber sovereignty' and 'data sovereignty' are commonly used pejoratively as catch-all phrases to encapsulate the adoption of data localization and other restrictive policies.[5] Many policymakers portray digital sovereignty as a strong yet nebulous concept, usually referring to the assertion of state control over data, data flows, and digital technologies.[6] More often than not, it's based on protectionist goals that it helps countries "take back control" and "sovereignty" from foreign technology firms and trading partners (mainly the United States, but increasingly China as well).[7] Misconceptions about data and cyber sovereignty miss the point that a complex interplay of economic, governance, social, and political factors determines a country's position on digital issues. Policymakers deliberately—and deceptively—use these concepts to condense complex phenomena into catchy phrases.

Proponents think that forcing firms to store data locally enhances the state's agency and that of their own firms and people. At best, the agency gained by data localization is illusory. In many cases, it is counterproductive. And in cases like Australia—which is a middle-sized economy that depends on global data flows and digital trade to build critical economies of scale and which has actively supported efforts to build an open, rules-based, and innovative global digital economy—data localization undermines other important economic goals as it reeks of hypocrisy and opens a loophole for other countries to enact broad digital protectionism policies. And in the case of authoritarian countries, it is predatory given the agencies data localization policies tend to support are those involved in surveillance and social and political control.

Even those policymakers and advocates who support narrow, limited data localization rules are still often misguided about how cloud services and cloud security functions. This submission analyzes several examples showing this, including the risk of having government agencies store data on premise in the misguided pursuit of cybersecurity.[8] Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored. If the Australian government wants to ensure its most sensitive data is especially secure, it can specify detailed technical and control requirements in its procurement contracts, such as the use of international standards for cybersecurity, the use of specific encryption, and cloud-based hardware security modules. Government policymakers need to appreciate that leading cloud service providers invest huge amounts of resources in designing and maintaining cutting-edge cybersecurity measures as their business depends on it. The dynamic nature of cyber risks means that they need to do this continuously. Furthermore, the global operations of leading cloud firms actually improves their ability to protect data as they have to defend against all manner of threats (as compared to just a local firm) and can leverage their global services to secure data, such as through the use of "data sharding" and other technologies.

The Australian government should obviously choose cloud providers based on their commitment to best-in-class cybersecurity measures and transparency and auditability about how they manage and protect data. As part of this, it can review their commitment to aiding by local laws and regulations and pushing back on unwarranted foreign government requests for data. Australia should use all the tools it has to address its cybersecurity concerns. For example, Australia already uses security reviews under its foreign investment screening framework to ensure cloud service providers from countries like China do not manage sensitive government data (which is fair enough).[9]

The challenge for Australian policymakers is putting the right policy pieces together to best protect sensitive government data and services and protect and support the use of data by Australian businesses and citizens, while avoiding misguided and counter protective ones like localization. Australia is already well on its way in doing this in many areas, but including data localization in its National Data Strategy would be a critical misstep that would undermine what it's otherwise working to achieve at home and globally in terms of digital policy. This is why the OECD's "Assessing Digital Strategies and their Governance" report counts localization as a detrimental factor in its comparative assessment of different countries' strategies.[10] Australia scores relatively well at the moment, but if it took into consideration the National Data Strategies proposal for data localization it'd inevitably effect Australia's score across all categories and overall given data and data governance policies are part of all categories.[11]

QUESTION 5: DOES AUSTRALIA NEED AN EXPLICIT APPROACH TO DATA LOCALISATION?

No. Data localization does not provide better data privacy or data protection, or cybersecurity. Nor does it provide the basis for digital development. Nor does it provide the silver bullet for government agencies that want to require data localization to ensure they have access to data for law enforcement, financial oversight, and other concerns. This section analyzes and refutes the key (misguided) motivations policymakers use to justify data localization.

Misguided Data Privacy, Protection, and Cybersecurity Concerns

As more countries enact updated data protection frameworks it is nearly inevitable (like Australia and its National Data Strategy) that some policymakers will propose data localization as they reflexively and mistakenly believe that data is more private and secure when it is stored within a country's borders. This misunderstanding remains at the core of many data localization policies. However, in most instances, data localization mandates do not increase commercial privacy nor data security.[12]

Evidence showing that data localization does not provide greater data privacy or security has only become starker in recent years. Firstly, most companies doing business in a nation—all domestic companies and most foreign ones—have "legal nexus," which puts the company in that country's jurisdiction. This is crystal clear for firms in financial, payment, and other heavily regulated sectors, given the need to apply for licenses to operate. Whichever sector a firm is in, a central basic fact remains: companies cannot simply escape from complying with a nation's data-related laws by transferring data overseas.

Second, policymakers focusing on geography to solve privacy and cybersecurity concerns misunderstand how these play out in today's digital economy. Or they're disingenuous. Consumers and businesses rely on contracts or laws to limit voluntary disclosures to ensure that data stored abroad receives the same level of protection as data stored at home. In the case of inadvertent disclosures of data (e.g., security breaches) and other cybersecurity issues, to the extent nations have laws and regulations, again, a company operating in the country is subject to those laws, regardless of where the data is stored.

Despite it being perhaps one of the most clearly misguided motivations, the mistaken notion about localization and data security persists. Having complete and direct ownership and control of the IT systems "stack," from the building floor and walls to the software on the servers, makes people feel that their data is as secure as possible. But this is a false sense of security. Most cybersecurity vulnerabilities are exploited remotely, so the physical location of data has little to no impact on cyber threats (as demonstrated by the hack of the U.S. Office of Budget and Management).[13] Furthermore, inadvertent disclosures of data are the result of security failures, such as hackers breaking into a corporate network to steal data, government agencies tapping into telecommunications links, or employees mistakenly posting sensitive data in a public forum. If IT systems are in any way connected to the Internet, they are at some risk.

Policymakers misunderstand that the confidentiality of data does not generally depend on which country the information is stored in, only on the measures used to store it securely. A secure server in Malaysia is no different from a secure server in the United Kingdom. Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored.

Policymakers' focus on the location of data storage, in part, as they do not want to tackle the more challenging factors that actually contribute to good cybersecurity, such as building greater cybersecurity awareness by users and firms and encouraging firms and government agencies to adopt and remain committed to best-in-class cybersecurity practices and services. Good cybersecurity is just as much about the people involved in managing, protecting, and accessing the data as it is about the data itself, as personnel are central to most cybersecurity incidents, such as the failure to update vulnerable systems or credentials being lost via phishing attacks.

Moreover, data localization actually undermines cybersecurity. First, it prevents the sharing of data to identify IT system vulnerabilities and help firms detect and respond to cyber attackers. For example, in 2020, India's Securities and Exchange Board released a cybersecurity circular that required financial firms to localize a broad range of data that would do just this.[14] Firms need to share data to reconcile if cyberattacks (such as in India) are new or known. Sharing system vulnerability information also allows cybersecurity providers to identify vulnerabilities.

Second, data localization precludes cloud service providers from using cybersecurity best practices, such as through "sharding," where data is spread over multiple data centers. This gets to the broader point—while

cloud computing does not guarantee security, it will likely lead to better security because implementing a robust security program requires resources and expertise, which many organizations (especially small and medium-sized ones) lack. But large-scale cloud-computing providers are better positioned to offer this protection. For example, advanced cloud providers provide their users with advanced encryption tools to allow them to retain and use the keys before data is uploaded, thereby preventing third parties, including the cloud companies themselves, from accessing their data.[15]

Data Localization for Digital Protectionism: The Mistaken (and Costly) Focus on the Geography of Data Storage

Data innovation—the use of data to create value—has become increasingly important to economic growth, competitiveness, scientific discovery, and social progress as new technologies and methods have made it easier to collect, store, analyze, share, and use information.[16] However, as policymakers around the world grapple with the challenge of leveraging digital technologies to drive development, many are being seduced by the misguided and costly fallacy that it is the location of data that matters—i.e., that countries can best serve their economic interests by forcing firms to store data locally instead of focusing on the fundamentals of information and communications technology (ICT) adoption, education, digital infrastructure, and data governance policies, which are necessary to maximize the economic and societal benefits of data and digital technologies.[17]

Many policymakers mistakenly believe that requiring data to be stored and processed domestically (i.e., data localization) is a shortcut to high-tech jobs, investment, and innovation.[18] This represents a new form of protectionism, similar to how countries use local content requirements and tariffs to protect local manufacturing operations.[19] Given that traditional trade-protectionism tools, such as tariffs, do not work as readily on digital economic activity, countries pursuing digital mercantilism are reverting to "behind-the-border" regulations and technical requirements, such as data localization.

Data localization's use for protectionism has evolved in recent years. More and more policymakers look to use it to favor local firms as they realize that data-driven innovation is at the heart of modern competitiveness and they haven't made the long-term investments in education, infrastructure, and other enabling factors that actually help firms and economies become more competitive.[20] For example, India's Non-Personal Data Governance Framework initially included a proposal to force firms to share anonymized datasets (undoubtedly to help local firms). Europe, India, South Africa, and others use localization to target U.S. firms explicitly.[21]

These supposed benefits of data localization policies, including the stimulus to jobs, are incorrect. One expected benefit is that forcing companies to store data inside a country's borders will produce a boom in domestic data center jobs. In fact, while data centers contain expensive hardware (which is usually imported) and create some temporary construction jobs, they employ relatively few staff.[22] Data centers are typically highly automated, using artificial intelligence, which allows a small number of workers to operate a large facility.[23] In a 2015 review of data center operations across the United States, CBRE Data Center Solutions Group (a U.S. real estate firm) estimated that a typical data center creates between 5 and 30 permanent jobs.[24]

For example:

- Microsoft's data center in Quincy, Washington had as many as 500 workers at a time onsite during the construction process, but now employs just 50 full-time staff to operate the center.[25]
- In 2011, a $1 billion data center that Apple built in North Carolina created only 50 full-time jobs and another 250 support jobs in the local community in areas such as security and maintenance.
- Google invested $1.2 billion in a data center in Oregon in 2016, yet only hired 175 employees.[26]
- In 2018, Facebook started construction on a $750 million data center in Utah, which will employ 30-50 people full time once completed.[27]

Policymakers should realize that data center customers need to be free to make their own decisions based on market factors and should not be compelled to purchase local data center services due to government restrictions. Data center operators may open new facilities to meet large and growing demand for data-related services, to be closer to customers so they can provide an improved service (e.g., reduced latency in the time it takes to execute instructions to store or retrieve data), or to take advantage of cheap and reliable electricity (both critical to data centers). In this case, instead of compulsion, countries should adopt an attraction strategy toward data centers and other ICT companies (domestic and foreign alike) by addressing business environment and regulatory conditions that affect their decision to operate in a market, including ensuring that the country has a robust fiber-optic communications backbone.

More importantly, data localization undermines a country's digital development as it affects the price, availability, and range of ICT services that all firms, in all sectors, rely on. A growing body of literature shows that data localization policies increase the costs of cloud computing services, which has a broader effect on an economy's productivity as it affects all users of these IT services. A 2015 study by Leviathan (an information security company) shows that local companies could have to pay significantly more for cloud services in Brazil, Europe, and elsewhere if data localization policies cut them off from the most cost-competitive global cloud providers.[28] A 2016 study from the Center for International Governance Innovation (CIGI) and Chatham House shows that restrictive data regulations, including forced data localization, are likely to lead to increased prices and decreased productivity in Brazil, China, the European Union, India, Indonesia, Russia, South Korea, and Vietnam.[29] Likewise, the European Center for International Political Economy (ECIPE) has conducted several econometric studies about the costs of data localization and data regulations in the European Union, Russia, Brazil, China, India, Indonesia, South Korea, and Vietnam.[30] A 2021 ITIF econometric study estimates that a one-unit increase in a country's data restrictiveness index (DRI) results (cumulatively, over a five-year period) in a 7 percent decrease in its volume of gross output traded, a 1.5 percent increase in its prices of goods and services among downstream industries, and a 2.9 percent decrease in its economy-wide productivity.[31]

Data Localization and Data/Cyber Sovereignty

Digital protectionism remains a key motivation behind many countries enacting data localization policies, but it has been subsumed into a broader narrative around digital/cyber sovereignty and control in recent years.

This a broader trend that Australia should both avoid and be actively working to counter given the threat it poses to its interests in building an open, rules-based global digital economy at the WTO and via other bilateral and regional trade agreements.

As detailed in the overview, many policymakers and governments around the world are pursuing a data, digital, and cyber sovereignty approach that is often built on the misguided attraction to the false sense of "control" and sovereignty provided by data localization. It's no surprise that authoritarian countries like China and Russia are the most significant users of these concepts (and data localization practices) as it aligns with their main political interests—maintaining power through access and control over data. Both countries frequently cite sovereignty as part of advocacy to create a top-down, state-directed global Internet (as opposed to the open, multi-stakeholder-based approach favored by democratic countries).

However, the spread of this concept among other countries that are not inherently authoritarian (like Australia, if it uses data localization) is most worrying for countries that support an open, rules-based, and multi-stakeholder-driven global digital economy.

Europe is a lead offender. European leaders like former Germany Chancellor Merkel and French President Macron have explicitly called for both digital protectionism and data sovereignty.[32] The fact that senior European policymakers think that data stored on a foreign cloud service represents lost sovereignty shows how little some understand about how firms manage data and how much they prioritize this misguided sense of control.[33] Europe tries to position itself as a moral leader of digital regulation, using concerns over data privacy and artificial intelligence (AI) to cloak discriminatory and restrictive policies. Europe's protectionist intent appears in nearly every digital policy proposal. Europe's General Data Protection Regulation (GDPR) is evolving into the world's most significant de facto data localization framework. Europe's draft data strategy pushes for data localization and asserts that the EU needs cloud providers owned and operated in Europe.[34] Similar points are made in Europe's white paper on artificial intelligence.[35] It is also evident in the proposal for a European cloud via GAIA-X.

Using Data Localization as a Cudgel for Surveillance and Censorship

While Australia may not be considering using data localization for surveillance or censorship purposes, it needs to realize the implications of it using localization for other (similarly misguided reasons) as inevitably this will provide cover for other countries to use it for these purposes. This is a spillover of the EU's General Data Protection Regulations' (GDPR) role as a de facto data localization framework, in that as other countries have adopted parts of GDPR, they also include localization requirements (for supposed privacy purposes, but the actual intention is for surveillance). Australian policymakers need to be aware of the broader signal its National Data Strategy sends to other countries and the second- and third-order effects from this signal, especially if it's the wrong one.

Countries use data localization as a cudgel to force foreign firms to provide easier access to data for surveillance and political purposes and to force compliance with censorship requirements. Commonly mixed

into this rationale is the specter—both real and imagined—of foreign surveillance as a rationale for data localization when it actually enables their own surveillance.

Digital authoritarian governments—led by China and Russia—see physical access to data centers as a critical enabler of surveillance and political control. Data localization enables political oppression by bringing information under government control and allowing the government to identify and threaten individuals, impacting privacy, data protection, and freedom of expression.[36] China retains broad and vague legal authority in its laws to potentially access data for national security, public interest, and political purposes.[37] The lack of an independent judiciary and the opaque nature of these laws make it hard to judge how China uses these broad powers.[38] Yet, this doesn't stop these countries from referring to "data privacy" as a motivation for localization.[39]

Recent laws enacted in Vietnam and Pakistan highlight how data localization does not lead to greater data privacy—but the exact opposite in making it easier for governments to access a small number of servers. Related, but different, from this authoritarian motivation, is when countries, like India, enact short deadlines for firms to respond to content takedown requests that create a de facto localization requirement. Firms have to do this; otherwise, they would not be able to comply (and thus avoid fines and other legal consequences).[40]

Data localization is central to Vietnam's evolving online censorship and surveillance regime. Vietnam's Law on Cybersecurity requires online firms to store personal and other data types locally and establish a local office in Vietnam. Its motivation is broad and vague: to protect national security, social order and safety, social ethics, and the health of the community.[41] Firms must have a license and at least one server in Vietnam for inspection at any time required, store detailed information about users and their activities, and remove illegal content within three hours.[42] Concerns about how Vietnam could use this to facilitate government access to data are real given Vietnam does not have a dedicated, independent data protection agency: the responsible agency is the Ministry of Public Security.[43]

Pakistan is also using data localization to support censorship and surveillance. Pakistan's "Removal and Blocking of Unlawful Online Content" law includes broad data localization requirements. It also allows the government to force companies to block content critical of the government and facilitate access to user data. It allows the Pakistan Telecommunication Authority to avoid existing data access and privacy safeguards, allowing it to intervene on behalf of law enforcement agencies to ask social media companies to provide user data.[44] It also makes it mandatory for firms to retain information, including traffic data linked to blocked content, and decrypted information about subscribers and their activity.

Data Localization for Law Enforcement and Regulatory Oversight

Countries use law enforcement and regulatory concerns about cross-border access to data to justify data localization (and as an excuse for digital protectionism). Some policymakers say data localization is the only way to get local and foreign firms to respond to requests for data from law enforcement and financial regulators. This reflects the mistaken belief that firms can avoid oversight and requests for data by simply transferring data out of a country. That firms can pursue some form of regulatory or legal arbitrage in terms

of picking and choosing which country's laws it follows and which it doesn't.[45] This is false. Data localization requirements do not change who is responsible for the data, regardless of where it is stored. The following sections analyze the issue of data localization for law enforcement and regulatory oversight concerns.

Data Localization for Law Enforcement

Some countries support data localization given the lack of effective cross-border law enforcement legal tools and treaties. If data is stored locally, the thinking goes, foreign governments will not be able to halt investigations by stopping providers from fulfilling government requests. This mistaken belief was central to proposed localization in India's draft data protection law.[46] However, policymakers in India fail to acknowledge all the contributing factors. For example, Indian law enforcement often files mutual legal assistance treaty (MLAT) requests that are incomplete, poorly drafted, or inappropriate (in that they aren't related to criminal activity).[47] For example, after the Department of Justice advised an Indian prosecutor to fill out an MLAT in 2012 to obtain U.S.-stored information, the court instead issued a summons for several U.S. tech firms for not cooperating.[48] Other policymakers use this law enforcement motivation to support localization as a disguise for different goals, like surveillance and protectionism.

Law enforcement-motivated data localization often stems from the fact that policymakers do not want to address the underlying issues with existing legal mechanisms to improve the process of making cross-border requests for data. The transnational nature of crime and digital services means that countries will inevitably need another country's help—even if they have localization. For example, a European Union report states that electronic evidence in some form is relevant in around 85 percent of total criminal investigations and that 55 percent of investigations require cross-border access to electronic evidence.[49] Current legal tools need an upgrade. For example, conflicting laws can put firms in a "catch 22" scenario where they face lawful requests for access to data from one country, the release of which may be legally prohibited in another.[50] Governments also have mismatched legal assistance treaties and laws.

Whether it is law enforcement or regulatory related, data localization is not the silver bullet policymakers think it is for improving access to data. The self-defeating nature of localization becomes clear given the scenario where every country requires localization, thus preventing the cooperation that will still inevitably be needed given the interconnected nature of the Internet, such as emails between two people and providers in different jurisdictions. But the potential for regulatory-motivated digital fragmentation is much broader. For example, medical labs must disclose confidential data about infectious diseases, firms must share clinical trial data with medical authorities, banks must disclose data on suspicious transactions, and accountants and their clients must share data for tax audits.

Instead, the globalization of criminal evidence should drive reforms regarding how law enforcement can access communications and other records in other countries as part of legitimate investigations while abiding by privacy and human rights protections. Criminals should not escape the law simply because police cannot access the data they need efficiently. Unfortunately, in the absence of updated legal mechanisms, there is the potential for a (legal) arms race calling for mandatory data localization requirements, which will ultimately hurt all law enforcement efforts to deal with what is a global problem.

Australia should pay attention and provide the necessary resources to improve existing legal processes and treaties as existing legal processes and treaties are out of date, needlessly complex, and often delayed due to poorly resourced local agencies.[51] At the moment, mutual legal assistance treaties (MLATs) remain the dominant international framework for enabling cross-border data access. The MLAT process is not working well. For example, the U.S. government can take up to 10 months to complete MLAT requests (leading to a massive backlog), while requests from the United States to Ireland take 15 to 18 months.[52] Meanwhile, some countries take years to respond to requests, while others, like Russia, often do not respond at all.[53]

Australia is doing the right thing in being a signatory to the Budapest Convention on Cybercrime—the world's first cybercrime treaty, negotiated 20 years ago—and supporting ongoing efforts to improve it via a new (second) protocol. This new protocol would help law enforcement agencies secure evidence from service providers in foreign jurisdictions.[54] The proposed language of the second protocol focuses on five major provisions: language of requests; videoconferencing; emergency mutual legal assistance; direct disclosure of subscriber information; and giving effect to foreign orders for the expedited production of data.[55]

Similarly, Australia is doing the right thing in negotiating a CLOUD ACT executive agreement with the United States, which will make the exchange of data for law enforcement purposes more efficient while still providing privacy and other safeguards. The U.S.-Australia and other CLOUD Act agreements incorporate commonly recognized global privacy principles while accounting for local interpretation and different legal structures. And overall, they work without impeding data flows.[56] These agreements provide a lawful mechanism for law enforcement in either Australia or the other signatory to request data directly from a service provider in the other country without going through the mutual legal assistance process.[57] CLOUD Act agreements do not give law enforcement agencies any new legal authority to acquire data. They simply help likeminded, rights-respecting countries improve the exchange of data for legitimate law enforcement investigations.[58]

Data Localization for Financial Regulatory Oversight

Financial regulatory oversight agencies use localization to target publicly listed companies, payment services, banks, and other financial firms as they think it's the only way to access data they need for their oversight responsibilities. In contrast, several enlightened financial regulators—usually reticent to give up any semblance of control—have worked with their trade officials and foreign counterparts on new legal frameworks and mechanisms for cooperation. The goal is to support cross-border data flows while ensuring they still have access to data for oversight purposes.[59]

Financial data is also among the most targeted categories for localization. Yet, in the logical end state where many countries enact localization policies, all will be hampered as today's global digital economy means there will inevitably be cross-jurisdictional data. U.S. financial regulators initially sought the option for data localization (before, thankfully, backtracking) for financial oversight.[60] The Reserve Bank of India cited the need for "unfettered" access to data for monitoring purposes in trying to justify its payments data localization requirement. Yet, policymakers in China, India, Turkey, and elsewhere that use this motivation for

localization routinely fail to provide evidence that they face genuine cross-border issues related to financial oversight.[61] The false promise of "unfettered" access is made clear by the fact that even with local storage, regulators will still have to request firms decrypt the data, in line with relevant legal checks and balances, before the data can be viewed.

Again, it's up to rule-of-law and rights-respecting countries to set up appropriate mechanisms to improve these processes. This is exactly what Australia has done via MOUs between the Australian Securities and Investment Commission and its counterparts, such as Singapore. In 2014, in a first-of-its-kind MOU, the Monetary Authority of Singapore (MAS) and the Australian Securities and Investments Commission (ASIC), agreed to allow licensed firms in one jurisdiction to provide relevant data to the authority in the other jurisdiction if it's required to fulfil its regulatory responsibilities.[62] It also set conditions on how the data can be used and how it must be protected. The MOU sets in places certain processes and standards to facilitate access in cooperation with partners.

It's also what Australia's key trading partners are doing. In 2018, MAS and the U.S. Commodity Futures Trading Commission (CFTC) signed a similar MOU.[63] This builds on a set of MOUs the two sides have in place, including one from 2013 on the exchange of information in the supervision and oversight of regulated entities that operate in the two countries.[64] Most recently, on June 13, 2019, MAS and the City of London signed a similar MOU that signifies both parties' intention to cooperate in facilitating data flows and other regulatory activities.[65] Singapore is pursuing these MOUs as it sees a future where these types of "data connectivity agreements" among countries will become as important as today's free trade agreements.[66]

MOU provisions dealing with data, data governance, and data flows restate shared principals and objectives and are on a good faith, best-effort basis—they're not legally binding. It's also important to note that they're not at the government-to-government level, but between respective regulatory agencies (not that both governments wouldn't be aware of what their regulators are doing). These MOUs and their data access provisions are not legally binding and are not overly prescriptive as they're seen as a first step toward better governance of a technology that continues to change. However, at the heart of these MOUs is the recognition that however fintech evolves, the free flow of data and regulatory access to it will remain critically important.

Singapore, Australia, and the United States are using these data connectivity agreements to provide confidence, clarity, and a connection between different regulations and regulators as many financial regulators are concerned about their ability to access data as part of ongoing oversight activities. As U.S. Under Secretary McIntosh stated: "Data connectivity facilitates financial regulators' access to the financial risk-related data needed to fulfil their mandates in ensuring safety and soundness….When data connectivity is impeded, firms, consumers, regulators, and the economy as a whole are all worse off, and we risk losing out on many benefits of today's digital economy."[67] The MOU sets in place processes and standards to facilitate access in cooperation with regulatory partners.

ENDNOTES

[1] "Australia's National Data Security Action Plan: A Call for Views," Australia's Department of Homeland Security, https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf.

[2] Daniel Castro, "Policymakers Should Distinguish Between Data Protection and Data Protectionism," Center for Data Innovation, May 31, 2022, https://datainnovation.org/2022/05/policymakers-should-distinguish-between-data-protection-and-data-protectionism/.

[3] "Declaration on the Establishment of a New International Economic Order.," United Nations General Assembly, 1974, https://digitallibrary.un.org/record/218450?ln=en.

[4] "Personally Controlled Electronic Health Records Bill 2011," https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4738#:~:text=Introduced%20with%20the%20Personally%20Controlled,will%20support%20the%20operation%20of.

[5] Tim Maurer, Isabel Skierka, Robert Morgus, and Mirko Hohmann, 'Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013,' Transatlantic Dialogues on Security and Freedom in the Digital Age Paper, November 2014), https://www.gppi.net/2014/11/24/technological-sovereignty-missing-the-point; Stephane Couture and Sophie Toupin, 'What Does the Notion of "Sovereignty" Mean When Referring to the Digital?' 2019, New Media & Society, https://journals.sagepub.com/doi/abs/10.1177/1461444819865984?journalCode=nmsa.

[6] For example, a July 2020 publication by the European Parliament's think tank states that, in the EU context, "digital sovereignty" refers to: "Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)," Tambiama Madiega, "Digital sovereignty for Europe" (European Parliamentary Research Service Ideas Paper, July 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

[7] European Commission president Ursula von der Leyen clearly stated regarding the EU's protectionist's objectives, "We must have mastery and ownership of key technologies in Europe," naming quantum computing, AI, blockchain, and critical chip technologies. Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme, November 27, 2019, https://ec.europa.eu/commission/presscorner/detail/es/speech_19_6408.

[8] Andrew Mitchell and Theodore Samlidis, "Cloud services and government digital sovereignty in Australia and beyond," International Journal of Law and Information Technology, Volume 29, Issue 4, Winter 2021, Pages 364–394, https://doi.org/10.1093/ijlit/eaac003.

[9] Tanwen Dawn-Hiscox, "Australian DoD will leave Global Switch due to fears of Chinese interference," Data Center Dynamics, June 21, 2017, https://www.datacenterdynamics.com/en/news/australian-dod-will-leave-global-switch-due-to-fears-of-chinese-interference/; John Tivey, Nirangjah, and Stephen Carlton, "Foreign direct investment reviews 2021: Australia," December 20, 2021, https://www.whitecase.com/publications/insight/foreign-direct-investment-reviews-2021-australia; "Use of patient data by foreign acquirers of healthcare companies," Baker McKenzie, April 5, 2019, https://insightplus.bakermckenzie.com/bm/healthcare-life-sciences/use-of-patient-data-by-foreign-acquirers-of-healthcare-companies/.

[10] "Assessing national digital strategies and their governance," Organization for Economic Cooperation and Development, May 20, 2022, https://www.oecd.org/digital/assessing-national-digital-strategies-and-their-governance-baffceca-en.htm.

[11] Ibid.

[12] Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

[13] The hack on the U.S. Office of Management and Budget occurred, at least in part, in an on-premise environment as a result of compromised user credentials. While the AWS report does not specify that it was referring to the OPM hack, it is more than likely the example it refers to. It's fairly clear from the agency OIG reports that OPM was running a number of their own data centers and they were behind on security. Min Hyun, "Addressing Data Residency with AWS," AWS Blog post, February, 2018,

https://aws.amazon.com/blogs/security/addressing-data-residency-with-aws/; The Majority Staff Report, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation" (Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress, September 7, 2016), https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/;

14 The Security and Exchange Board of India, "Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions," November 3, 2020, https://www.sebi.gov.in/legal/circulars/nov-2020/advisory-for-financial-sector-organizations-regarding-software-as-a-service-saas-based-solutions_48081.html.

15 Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (ITIF, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.

16 Daniel Castro and Travis Korte, "Data Innovation 101" (Center for Data Innovation, November 2013), https://www.datainnovation.org/2013/11/data-innovation-101/.

17 Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (Information Technology and Innovation Foundation, February, 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf; Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

18 For example, see Avanti Kumar, "Can Malaysia Really Become a Data Center Hub?" *MISAsia,* February 13, 2017, http://www.mis-asia.com/tech/data-centre/mdec-exclusive-can-malaysia-really-become-a-data-centre-hub/; "Indian Cloud Data Centres Will Make or Break Digital India," *FirstPost,* October 30, 2015, http://www.firstpost.com/business/sponsored-indian-cloud-data-centres-will-make-or-break-digital-india-2475598.html.

19 For more information on mercantilism, see Michelle A. Wein, Stephen J. Ezell, and Robert D. Atkinson, "The Global Mercantilist Index: A New Approach to Ranking Nations' Trade Policies" (Information Technology and Innovation Foundation, October 2014), http://www2.itif.org/2014-general-mercantilist-index.pdf.

20 https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where

21 "India Releases Revised Non-Personal Data Framework," Hunton Andrews Kurth blog post on the National Law Review, January 15, 2021, https://www.natlawreview.com/article/india-releases-revised-non-personal-data-framework; Ministry of Electronics and Information Technology, *Report by the Committee of Experts on Non-Personal Data Governance Framework* (Government of India, December 16, 2020), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.

22 Michael S. Rosenwald, "Cloud Centers Bring High-Tech Flash but Not Many Jobs to Beaten-Down Towns," *The Washington Post*, November 24, 2011, http://www.washingtonpost.com/business/economy/cloud-centersbring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html; Henry Blodget, "The Country's Problem in a Nutshell: Apple's Huge New Data Center in North Carolina Created Only 50 Jobs," *Business Insider*, November 28, 2011, http://www.businessinsider.com/apple-new-data-center-north-carolina-created-50-jobs-2011-11; Darrell Etherington, "Apple to Build a $2 Billion Data Command Center in Arizona," *TechCrunch*, February 2, 2015, https://techcrunch.com/2015/02/02/apple-to-build-a-2-billion-data-command-center-in-arizona/; Rich Miller, "The Economics of Data Center Staffing," *Data Center Knowledge*, January 18, 2008, http://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing/; Alison DeNisco Rayome, "Why data centers fail to bring new jobs to small towns," *TechRepublic,* September 19, 2016, https://www.techrepublic.com/article/why-data-centers-fail-to-bring-new-jobs-to-small-towns/.

23 Grant Gross, "This Wave of Data Center Consolidation is Different from the First One," *Data Center Knowledge,* February 8, 2018, https://www.datacenterknowledge.com/manage/wave-data-center-consolidation-different-first-one.

24 John Lenio, "The Mystery Impact of Data Centers on Local Economies Revealed," *Area Development,* 2015, http://www.areadevelopment.com/data-centers/Data-Centers-Q1-2015/impact-of-data-center-development-locally-2262766.shtml.

[25] Rich Miller, "The Economics of Data Center Staffing," *Data Center Knowledge,* January 18, 2008, https://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing.

[26] Dina Bass, "Microsoft Unveils Azure Sentinel Cloud Security Program," Data Center Knowledge, *February 28, 2019,* https://www.datacenterknowledge.com/microsoft/microsoft-unveils-azure-sentinel-cloud-security-program.

[27] Emily Holbrook, "Facebook's New Utah Data Center Engineered to Be 'Incredibly Water Efficient,'" *Environmental Leader,* June 1, 2018, https://www.environmentalleader.com/2018/06/facebooks-new-utah-data-center-engineered-to-be-incredibly-water-efficient/.

[28] Brendan O'Connor, "Quantifying the Cost of Forced Localization" (Leviathan Security Group, June 2015), http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization.

[29] As part of the proxy variable for data regulations, the study uses part of the OECD's Product Market Regulation in services to create a proxy that comes close to matching the types of regulations that are used regarding data. The real policy regulations for the select countries are then added to this index to estimate the real costs. Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization" (Centre for International Governance Innovation and Chatham House, May 2016), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.

[30] Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery" (European Centre for International Political Economy, March 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf; Matthais Bauer, Fredrik Erixon, Michal Krol, Hosuk Lee-Makiyama, and Bert Verschelde, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" (The European Centre for International Political Economy, March 2013), https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf; Matthias Bauer, Martina Ferracane, Hosuk Lee-Makiyama, Erik van der Marel, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States" (European Centre for International Political Economy, March 2016), http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf.

[31] Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

[32] German Chancellor Angela Merkel saying that the EU should claim digital sovereignty by developing its own platforms to manage data in order to reduce its reliance on U.S. provider is simply a call for protectionist-based import substitution in the digital era. Guy Chazan, "Angela Merkel urges EU to seize control of data from US tech titans," *Financial Times,* November 12, 2019, https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca; French President Emmanuel Macron is blunt: "The battle we're fighting is one of sovereignty." Charlene Barshefsky, "EU digital protectionism risks damaging ties with the US," *Financial Times,* August 2, 2020, https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103.

[33] Javier Espinoza and Guy Chazan, "Germany calls on EU to tighten grip on Big Tech," *Financial Times,* November 11, 2019, https://www.ft.com/content/2d538f22-048d-11ea-a984-fbbacad9e7dd.

[34] Eline Chivot, "EU Data Strategy Has Worthwhile Goal, But Misses the Mark," Center for Data Innovation blog post, August 13, 2020, https://datainnovation.org/2020/08/eu-data-strategy-has-worthwhile-goal-but-misses-the-mark/.

[35] Nigel Cory, "Response to the public consultation for the European Commission's white paper on a European approach to artificial intelligence" (ITIF, June 12, 2020), http://www2.itif.org/2020-eu-approach-ai.pdf?_ga=2.86726097.873378596.1596032106-254668983.1577993982.

[36] Erica Fraser, "Data Localisation and the Balkanisation of the Internet," *SCRIPTed*, 2016, Vol. 13, p. 359, https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/.

[37] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare blog post, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Samm Sacks, Qiheng Chen, and Graham Webster, "Five Important Takeaways From China's Draft Data Security

Law," DigiChina Project blog post, July 9, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law/.

38 Bill Bishop, "One country, one Internet?; TikTok; Gaokao; Floods in China; US FBI head on China," Sinocism newsletter, July 7, 2020, https://sinocism.com/p/one-country-one-internet-tiktok-gaokao.

39 For example, Russia stated that its personal data localization requirement (enacted in 2015) was to "provide extra protection for Russian citizens both from misuse of their personal data by foreign companies and surveillance of foreign governments." Alexander Savelyev, "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?" Computer Law & Security Review, 32 (2016) 128–145, https://doi.org/10.1016/j.clsr.2015.12.003; "Russia's security service tells internet firms to hand over user data: The Bell," *Reuters,* February 12, 2020, https://www.reuters.com/article/us-russia-internet/russias-security-service-tells-internet-firms-to-hand-over-user-data-the-bell-idUSKBN2060UV.

40 Daniel Castro, "India's Intermediary Liability Law Out of Step With Global Norms," Innovation Files blog post, May 11, 2021, https://itif.org/publications/2021/05/11/indias-intermediary-liability-law-out-step-global-norms.

41 Thomas Treutler and Giang Thi Huong Tran, "Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees," *Lexology,* December 18, 2019, https://www.lexology.com/library/detail.aspx?g=8833627c-e189-4d60-a472-6ee742cc38fd.

42 The Decree took effect on 15 April 2018. It updated Decree 72/2013/ND-CP (dated July 15, 2013). Yee Chung Seck and Thanh Son Dang, "Decree No. 27/2018/ND-CP amending and supplementing Decree No. 72/2013/ND-CP on Internet Services and Online Information," *Lexology,* April 23, 2018, https://www.lexology.com/library/detail.aspx?g=bec72ba6-167d-468e-938c-391199d8579c.

43 For example, the Director General of the Department of Cybersecurity and High-Tech Crime Prevention and Control under Vietnam's Ministry of Public Security is responsible for deciding on the required deletion, sending written requests for deletion to the relevant entities and auditing such entities' compliance with the LOC. "Updates to Draft Decree Detailing Certain Articles of Law on Cybersecurity," Baker McKenzie blog post, October 8, 2019, https://www.bakermckenzie.com/en/insight/publications/2019/10/updates-draft-decree-law-on-cybersecurity.

44 "PTA empowered to block online speech critical of government & public officers; gets power to block entire online systems," Digital Rights Monitor, November 18, 2020, https://www.digitalrightsmonitor.pk/pta-empowered-to-block-online-speech-critical-of-government-gets-power-to-block-entire-online-systems/; Sadaf Khan, Zoya Rehman, and Salwa Rana, "The Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2020: A legal analysis" (Media Matters for Democracy, 2020), https://www.digitalrightsmonitor.pk/wp-content/uploads/2021/01/Social-Media-Rules-2020-Legal-Analysis.pdf; "Media Matters for Democracy conducts an initial analysis of the new social media rules and their potential impact on digital rights and economy in Pakistan," Media Matters for Democracy blog post, November 23, 2020, https://mediamatters.pk/media-matters-for-democracy-conducts-an-initial-analysis-of-the-new-social-media-rules-and-their-potential-impact-on-digital-rights-and-economy-in-pakistan/.

45 Jane Kelsey, "DEPA lacks added value," East Asia Forum blog post, April 10, 2020, https://www.eastasiaforum.org/2020/04/10/depa-lacks-added-value/.

46 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians", 27 July 2018, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

47 Ibid; Amber Sinha, Elonnai Hickok, Udbhav Tiwari, and Arindrajit Basu, "Cross Border Data-Sharing and India: A Study in Processes, Content and Capacity," (Centre for Internet & Society, February 2016), https://cis-india.org/internet-governance/files/mlat-report.

48 "Centre not co-operating in complaint against websites: Court," *Zeenews,* December 5, 2012, zeenews.india.com/news/delhi/centre-not-co-operating-in-complaint-against-websites-court_814836.html.

49 "European Commission Impact assessment: electronic evidence in criminal matters," Commission Staff Working Document, April 17, 2018, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0118:FIN:EN:PDF.

50 As with the U.S. Electronic Communications Privacy Act, but this doesn't prohibit firms from voluntarily providing other non-content data.

[51] For a detailed analysis: Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders" (ITIF, July 24, 2017), https://itif.org/publications/2017/07/24/how-law-enforcement-should-access-data-across-borders; Microsoft Corporation v. United States, No. 14-2985 (2d Cir. 2017), "Government's Memorandum of Law in Opposition to Microsoft's Motion," (Preet Bharara, Attorney for the United States, April 20, 2014), *Just Security*, accessed June 29, 2017, https://www.justsecurity.org/wp-content/uploads/2014/05/Governments-Memorandum-of-Law-in-Opposition-to-Motion-to-Vacate-doc-97....pdf; "FY 2017 Budget Request – National Security" (U.S. Department of Justice, 2016), accessed June 29, 2017, https://www.justice.gov/jmd/file/822376/download.

[52] Richard Clarke et al., "Liberty and Security in a Changing World" (White House, December 18, 2013), accessed June 29, 2017, 227, https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world; *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights*, 115th Cong. (May 24, 2017) (testimony of Brad Wiegmann, Deputy Assistant Attorney General of the U.S. Department of Justice), accessed July 12, 2017, https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf.

[53] Brad Wiegmann, "Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights" (testimony to the Subcommittee on Crime and Terrorism Committee on the Judiciary United States Senate, May 24, 2017), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf.

[54] "Cybercrime: Towards a Protocol on evidence in the cloud," Council of Europe, June 8, 2017, https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud.

[55] Jennifer Daskal and Debrae Kennedy-Mayo, "Budapest Convention: What is it and How is it Being Updated?" Lawfare blog post, July 2, 2020, https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

[56] Caitlin Fennessy, "A Multilateral Surveillance Accord: Setting the Table," Lawfare blog post, April 23, 2021, https://www.lawfareblog.com/multilateral-surveillance-accord-setting-table.

[57] Peter Swire and Jennifer Daskal, "Frequently Asked Questions about the U.S. CLOUD Act," Cross Border Data Forum, April 16, 2019, https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/

[58] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World:The Purpose and Impact of the CLOUD Act* (Washington, D.C: white paper, April, 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

[59] The U.S.'s initial decision (later reversed) to exclude financial data from the Trans Pacific Partnership Agreement's anti-localization provisions is indicative.

[60] Nigel Cory and Robert D. Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements" (ITIF, April 25, 2016), https://itif.org/publications/2016/04/25/financial-data-does-not-need-or-deserve-special-treatment-trade-agreements; Nigel Cory, "The TPP's Financial Data Carve Out—USTR Closes a Loophole for Digital Protectionists," Innovation Files blog post, July 7, 2016, https://itif.org/publications/2016/07/07/tpp%E2%80%99s-financial-data-carve-out%E2%80%94ustr-closes-loophole-digital-protectionists.

[61] For details on cases in India and Turkey, see: Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018" (ITIF, January 28, 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

[62] "Memorandum of Understanding: Australian Securities and Investments Commission and the Monetary Authority of Singapore," https://download.asic.gov.au/media/2067384/monetary-authority-of-singapore-mou-2014.pdf.

[63] "Cooperation Arrangement: United States Commodity Futures Trading Commission and the Monetary Authority of Singapore," https://www.cftc.gov/sites/default/files/2018-09/cftc-mas-cooparrgt091318_16.pdf.

[64] "Memorandum of Understanding: United States Commodity Futures Trading Commission and the Monetary Authority of Singapore,"

https://www.cftc.gov/sites/default/files/idc/groups/public/@internationalaffairs/documents/file/masmou2013.pdf

65 "Singapore and UK to Enhance Cooperation in Data Connectivity, Talent Development, Green Finance and Cybersecurity," Monetary Authority of Singapore, June 13, 2019, https://www.mas.gov.sg/news/media-releases/2019/singapore-and-uk-to-enhance-cooperation.

66 ""Singapore FinTech: Innovation, Inclusion, Inspiration," Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, November 12, 2018, https://www.mas.gov.sg/news/speeches/2018/singapore-fintech.

67 "Address by Under Secretary McIntosh at the Sim Kee Boon Institute for Financial Economics at Singapore Management University," U.S. Department of Treasury, February 6, 2020, https://home.treasury.gov/news/press-releases/sm900.