Data Localization Laws And Their Impact on Privacy, Data Security And the Global Economy

BY BRET COHEN, BRITANIE HALL, AND CHARLIE WOOD

FROM MESSAGES SENT BY HORN across the Alps to printing press newspapers dispatched cross-continent by the Pony Express to viral cat videos shared across a 9000-mile-long transatlantic fiber optic cable, we have always sought to connect across vast distances via increasingly complex communications systems. But no such system has broken down geographical barriers quite like the modern Internet, with digital trade and cross-border data flows expected to continue to grow faster than the overall rate of global trade.[1] Despite both domestic and global industries' increased reliance on these data flows, more than two dozen countries have enacted or considered policies that require retention of data within their borders—so-called data localization policies—with the effect of restricting the free flow of information via the global Internet.

Countries enacting such measures have asserted that their goal is to protect their citizens' privacy and security, but such countries may also be seeking—whether they state so publicly or not—to protect their own national sovereignty by addressing difficulties in their traditional abilities to grant law enforcement access to data, protecting local business growth from global juggernauts, obtaining jurisdictional traction necessary to enforce local laws against multinational companies, and controlling the flow of ideas, speech, or culture within their borders. Whatever the motivation, the rise of these data localization measures threatens to balkanize the global Internet, restrict both domestic and global trade, and precipitate an overall decline in digital privacy rights and data security for people across the globe.

We examine below the stated and perceived motivations behind this trend, potential privacy and security effects, and a select snapshot of the most significant such policies around the world.

Bret Cohen is a partner in the Privacy and Cybersecurity group at Hogan Lovells US LLP where he particularly focuses on Internet and e-commerce and writes on global privacy laws as managing editor of the Chronicle of Data Protection blog, https://hldataprotection.com. Britanie Hall, a senior associate at Hogan Lovells, focuses on strategic counseling and public policy advising on privacy, cybersecurity, and emerging technologies. Charlie Wood is an associate at Hogan Lovells focusing on privacy and cybersecurity compliance and investigations. Hogan Lovells' Natalia Gulyaeva, Maria Sedykh, Mark Parsons, Jeff Olson, and Aston Goad also contributed to this article.

What Is "Data Localization"?

The term "data localization" generally refers to public policy efforts to require storage within a particular jurisdiction of data collected within that jurisdiction's boundaries. For example, Russia, China, Indonesia, and others have enacted explicit "forced" localization requirements applicable to broad swaths of industry that require data to be stored on servers within their respective borders, while other countries, such as Australia, Germany, South Korea, and Venezuela, have enacted industry-specific laws that require certain financial, health and medical information, online publishing, and telecommunications data collected from their citizens to be stored on local servers.[2] Many countries, including the United States, require data related to specified government transactions or important national security concerns to be stored locally.

In this article, we distinguish data localization from the broader and more widespread concept of personal data export restrictions found in some data protection laws. For example, the European Union and many other jurisdictions prohibit the international transfer of personal data unless the transferor takes steps to require that the recipient applies appropriate privacy protections before the information is transferred abroad. While these restrictions can make it more expensive and time-consuming to transfer data across borders, in some cases resulting in de facto data localization, they do not mandate data storage or processing within the country as do the data localization policies we address here. In addition, this article concentrates on localization efforts that apply broadly across industry sectors rather than more limited measures that focus on specific sectors or types of data.

Motivations Behind Localization

While the Internet is global, regulation is local. Governments may push for data localization to achieve diverse policy goals, with many citing privacy, security, or law enforcement concerns as primary drivers of regulation. Indeed, many countries tailor their localization efforts to specific purposes. Some require as a matter of national security the local storage or processing of data by government contractors or data related to critical infrastructure such as power plants. Others mandate in-country servers for telecommunications providers to enhance law enforcement efforts. Yet other countries seek to bolster privacy protections and corporate accountability by requiring sensitive data related to citizens' health or finances

to be stored locally. Some governments also point to increased surveillance of global data flows by foreign intelligence agencies as a reason to try to keep data within their borders.

Yet, some commentators speculate that data localization efforts may be less about data protection than trade protection, requiring local storage or processing as a way to boost their local economies by propping up or kickstarting their domestic technology industries or the local digital economy.[3] As global technology firms increasingly build servers around the world in an effort to decrease network latency and improve user experience, certain data localization policies may successfully influence local firms' investment by ensuring their access to local markets. Detractors of the data localization trend, however, question the ability of such policies to meet the stated goals.

Economic critiques of data localization measures have questioned the asserted pretense that these measures bolster local industry, instead pointing to stymied economic growth due to such factors as loss of access to foreign markets and uncertainty for investors with regard to regulatory burdens.[4] Economists have equated measures like data localization to import substitution as companies that seek local market access are forced to pay for in-country data storage or processing rather than "importing" such services to serve the local market.[5] In addition, directing companies to install additional servers in specific countries can potentially have negative impacts on local and global user experience. Past a certain threshold, extra servers do not necessarily decrease latency for users—and could actually spur an increase—as these servers may not be connectable to the same backbone network, might be hampered by government or other intermediary access, or could be supported by less effective technology and staffing.

Data localization requirements may lead to increased infrastructure costs that may then be passed on to consumers. Data localization can also undermine data security, for example by restricting the use of a broader market of data storage and processing solutions or by forcing a company to splinter its data processing operations rather than consolidating it. We discuss potential privacy and data security impacts in more detail below.

When strict rules requiring local retention or processing of data have been introduced by governments that are not otherwise known to be staunch guardians of privacy and other civil liberties, critics suspect more nefarious or anti-democratic motivations—i.e., that these measures are thinly veiled efforts to force companies to retain information about local citizens within easy access of government authorities so as to stifle free speech and political dissent under the guise of data protection or national security. Requirements to retain messaging records and decrypt individual account information have been criticized as unconstitutional state intrusions.[6] For example, in Kazakhstan the government has a history of shutting down social media and other forms of communication within the country in response to speech critical of the government, and some critics believe strict user identification requirements coupled with data localization measures are intended as a means to identify dissidents.[7]

Forced Data Localization May Impact Privacy and Data Security

Regardless of the motivations for the data localization trend, the possible costs of such policies are potentially significant for individuals, companies, the global economy, and the nations that aim to cabin data within their borders. In some circumstances, data protection is a legitimate reason for governments to limit the transfer of certain types of data to jurisdictions where the data may be subject to higher risks. However, limiting cross-border transfers to recipients that will guarantee an adequate level of data protection is fundamentally different than forced localization, which may have—in addition to anticompetitive and anti-trade effects—net-neutral or negative consequences on the relative privacy and data security of individuals' personal data. For example:

- ***Greater data decentralization that makes it harder for companies to exercise control over data privacy and security.*** A rising trend in forced data localization measures could result in companies either avoiding certain markets altogether or being forced to create and maintain numerous data centers. Such measures may hinder a firm's ability to exercise business judgment in managing its business risks and needs, reduce opportunities to take advantage of global economies of scale and expertise that may benefit privacy and security, and create additional points of security failure or privacy non-compliance. When companies must stretch their limited security resources in numerous directions, rather than to a strategic few or to an overall data governance program, their security and privacy compliance infrastructure may start to look more like multiple houses, each with a locked door and guard dog, than a fortress manned by experienced soldiers. In addition, enterprises forced to operate in multiple jurisdictions (or forgo market access altogether) may have difficulty applying appropriate physical, technical, and administrative security controls when storing data in locations that may have language barriers, decreased availability of trained personnel, a lack of legal remedies for criminal or negligent data loss, or limited access to hardware or parts.
- ***Greater risk of inaccurate information.*** In certain cases, data localization requirements permit the cross-border transfer of data, but only after storing a localized copy. Where this is the case, companies based outside jurisdictions that enact forced localization measures are likely to transfer at least some of the data to existing data centers as well, due to the benefits of centralized data sets. This practice increases the locations where the data is stored, which in turn increases the number of times the data set must be revised or deleted to remain up to date. More locations increase the likelihood of error. For example, where a request for deletion leads to deletion on only one server, a request for access produces a stale record, or a request to correct a record is not effectuated

A rising trend in forced data localization measures could result in companies either avoiding certain markets altogether or being forced to create and maintain numerous data centers.

across all data centers, there can be both a decrease in user experience and an increased chance that incorrect information leads to an adverse action against an individual.

■ ***Reduction in barriers to government and law enforcement access.*** Companies that collect consumer data have become a primary source of helpful information for governments, courts, and law enforcement. For example, data from a person's cell phone can reveal where the individual has recently been or what the individual has been doing, while few other sources can provide as complete a picture. However, legitimate needs of law enforcement or government to access data to prevent or investigate terrorism or other crimes should ideally be balanced with privacy protections to prevent government overreach that may target dissidents, stifle free speech and association, and repress certain ideologies or civil liberties.

Many businesses cooperate with government requests that are narrowly tailored to limit government overreach and protect due process rights of users but are reluctant to comply where there are fewer protections baked into the system for their users and the organization itself. Global Internet companies increasingly push back on government access requests, with many reports that show access requests are up but the percentage of requests being granted is down.[8] Companies subject to frequent law enforcement or government requests may be actively choosing to store their data in jurisdictions where they believe users' privacy and civil liberties will be protected and respected by the rule of law. Consumers in turn may choose to interact with companies which can commit to providing additional privacy protections. Strict forced data localization removes this choice from consumers and companies and thus reduces the barrier for governments to access information about their citizens, for good or for ill.

Key Data Localization Laws

From theoretical implications of data localization to practical application of these laws, both the largest country in the world—Russia—and the largest country by population in the world—China—have passed strict forced localization measures. As discussed below, the Chinese and Russian laws are thus likely to present the most risks and challenges to multinational companies. We also discuss below the laws now in place in Indonesia, Kazakhstan, Vietnam, and Nigeria.

China. After several years of discussions and revisions, the *Cyber Security Law of the People's Republic of China* came into force on June 1, 2017. The law gives the Cyberspace Administration of China (CAC) broad latitude to regulate data practices of both local Chinese companies and multinational enterprises that do business within China, including the authority to require certain data to be stored locally, to require the maintenance and sharing of web logs, and to require entities to obtain consent for cross-border transfers of personal data. The CAC has released draft implementation rules that provide some insight into the government's plan to implement these requirements.[9]

Significant uncertainty remains as of publication of this article as to the specific rules and procedures for assessing and reviewing data exports under the Cyber Security Law. It appears that the data localization requirements applicable to personal data and "other important data" will take effect on December 31, 2018, and it is clear from the law itself that the localization measures apply to operators of "critical information infrastructure" (CII). Draft export review measures published by the CAC, however, appear to extend the localization requirement to "network operators," which are far more broadly defined under the law to include network service providers and owners or operators of any systems that gather, store, transmit, exchange, or otherwise process information.[10] This definition, read most broadly, encompasses most if not all enterprises operating network infrastructure within China, as even non-technology-focused companies will operate information systems.

Based on comments made by representatives of the CAC at a public seminar concerning the implementation of the law, there is reason to believe that the localization measure will apply only to network operators' systems and networks that interface with external networks, rather than systems that are entirely internal to an organization such as HR systems, but this position is not confirmed. There has also been some suggestion that smaller or less sensitive data transfers by network operators, such as those involving less than 500,000 consenting data subjects, would be subject to a self-assessment and notification requirement, rather than a substantive security review by the CAC or industry regulator. International transfers by operators of CII and by network operators exceeding these thresholds are expected to be subject to a substantive security review.

The definition of CII has evolved somewhat over the course of the implementation of the law. The most recent draft measures released for comment in July 2017 continue to leave the scope of CII to the discretion of the CAC, in consultation with other government authorities.[11] Although the draft measures for the classification of CII have done little to clarify the precise scope, the scope is expected to include government agencies in sensitive fields such as energy, finance, and transportation, as well as public utilities, telecommunication and broadcasting networks, scientific research institutes, and manufacturers in sensitive fields. There is likely to be broad discretion for the CAC to add further categories, perhaps retrospectively.[12]

The effect of the localization measure is expected to be that, unless a security review has been successfully completed, operators of CII (and potentially network operators) will be required to locally store personal data and "other important data" collected within mainland China. The criteria for completing a security review have not yet been determined, but it seems reasonably clear at this stage that in order to be permissible, cross-border transfers must be necessary for business requirements, data subjects must have consented to exports of personal data, and the organization making the export must have assessed the security measures being applied to the transfer and the storage of the data at rest in the jurisdiction(s) of export, having regard to the sensitivity of the data involved, the risks involved in the transfer, and "other important matters" related to the transfer.[13]

While the definition of "personal data" under the Cyber Security Law is broadly consistent with definitions used under data protection laws internationally, the concept of "other important information" is undefined and does not have any readily apparent analogy. Observers of Chinese law will note that the country already has prohibitions against the international transfer of state secrets. State secrets have a nebulous definition but likely fall within the scope of "other important information." Clarifications from the CAC indicate that the relative importance of "other important information" is to be assessed from the perspective of the state, as opposed to individuals or companies.[14]

Given the significant degree of uncertainty as to the scope and effect of the Cyber Security Law, the impact of the law is difficult to assess at this stage. It is clear, however, that this uncertainty is in and of itself generating a significant impact on multinational businesses with operations in China, as many organizations that are likely to be network operators under the law now believe that there is a significant risk that they will be required to localize at least some of their data (and corresponding systems) in China. The economic impact alone will be significant. Researchers estimate that company decisions based on Chinese retention requirements applied broadly across industries may reduce China's GDP by up to 1.1 percent across all industries, with certain industries significantly higher (such as 2 percent in communications) and others significantly lower (.05 percent for metals and textiles), in addition to US$63 billion in consumer welfare losses.[15]

Russia. Russia has one of the world's first-implemented and most expansive data localization regimes, and has demonstrated a willingness to proactively enforce it. Its data localization law, Federal Law No. 242-FZ, went into effect on September 1, 2015.[16] In contrast to preceding data localization laws of other countries, which typically required localization only for data related to certain industries or subject matters, Russia's law applies to any personal data collected from Russian citizens within Russia. It also requires storage and processing of this personal data within the physical territory of Russia, as well as indication of the physical location of these databases in the notification form that most organizations subject to Russian data privacy law are required to file with the government. Russia's telecommunications regulator and data protection authority, Roskomnadzor, is responsible for enforcement.

Shortly before the law went into effect, Russian regulatory authorities issued a non-binding clarification stating that, with respect to personal data collected online, the localization requirement did not apply to every service on the Internet available to Russian citizens.[17] Rather, the product or service must be directed at Russia in some way. Relevant factors include whether a service has a Russian language option, uses a Russian top-level domain name, displays Russian-language advertisements, or accepts Russian currency as payment. The clarification also noted that users could not waive the statutory requirements by contract and that the law does not prohibit cross-border data transfers so long as the data is locally stored and updated in Russia, after which the personal data may be transferred outside of the country subject to the requirements of Russia's general data protection law (e.g., with the consent of the data subject).

Russia has demonstrated its commitment to these requirements. Most notably, in November 2016, a Russian court of appeal ruled that professional social network LinkedIn violated the data localization requirement in the course of providing its services to Russian citizens. A company may be penalized for violating the data localization requirement by having access to its websites and other online services blocked by Russian Internet service providers. So overnight, 6 million Russian LinkedIn users were no longer able to access the site. LinkedIn continues to be blocked via the Internet and in app stores in Russia.[18]

In addition, Roskomnadzor conducts scheduled and ad hoc compliance inspections of companies each year to assess compliance with data protection laws, including the data localization requirement. In September 2016, the agency released a report indicating that the vast majority of the over 1000 companies inspected in the first year the Russian law was in effect were in compliance with the data localization requirements. Roskomnadzor also reported that the information about the location of more than 63,000 databases containing personal data had been submitted.[19]

Roskomnadzor's enforcement activities appear to be encouraging compliance. A number of multinational companies now either publicly state that they comply with the data localization requirement or have reportedly purchased data center capacity in Russia in order to comply.[20]

Indonesia. Indonesia has passed several laws and regulations since 2012 focusing on data localization, including Government Regulation 82 (Reg 82/2012), the Minister of Communication and Informatics (MOCI) Regulation 20 of 2016 regarding Protection of Personal Data in Electronic Systems (Reg 20/2016), and the MOCI Circular Letter No. 3 (2016). Regulation 82 requires that Electronic System Providers (ESPs) operating systems that provide ambiguously defined "public services" and process data of Indonesian res-

idents place their data centers and disaster recovery centers for their systems within Indonesian territory.[21] "Public services," if read broadly, could potentially include both government organizations and certain public-facing private sector businesses in various industries that are serving an Indonesian customer base through some digital means or otherwise collecting personal data of Indonesian residents. The regulations seem intended to cover the protection of personal data. However, there are indications that the data localization requirement may not be limited to personal data alone and may in fact be applied to all data. A spokesperson for the MOCI was quoted not long after Regulation 82 was passed as stating that the scope of Regulation 82 "covers any institution that provides information technology-based services."[22]

Given the significant degree of uncertainty as to the scope and effect of the Cyber Security Law, the impact of the law is difficult to assess at this stage. It is clear, however, that this uncertainty is in and of itself generating a significant impact on multinational businesses with operations in China . . .

Regulation 20—an implementing regulation of Indonesia's Electronic Information and Transactions Law and Regulation 82 that was passed in December 2016 and will be effective in December 2018—sought to define "personal data" and provided more detailed provisions in an attempt to clarify Indonesia's data processing requirements at every stage of personal data's lifecycle.[23] But it remains murky as to whether Indonesian authorities will apply the localization requirements extraterritorially to foreign businesses collecting personal data from Indonesian residents. Data stored locally may also be mirrored abroad, so long as the business obtains data subject consent, coordinates with the MOCI, and submits certain plans and reports to the government. Regulation 20 further requires that the transfer must also comply with cross-border personal data exchange legislation, even though no such legislation exists to date.

The Indonesian government has been active in issuing regulations related to Internet services, including a mandatory registration of e-commerce service providers (Presidential Regulation 74/2017) and a registration requirement for providers of Over-the-Top services (MOCI Circular Letter No. 3/2016), but has not yet issued implementing regulations in either case. Regulators often use registration requirements as a means to identify and enforce localization measures.

Implementation of these regulations threatens significant disruption of regional operating platforms that have tended to host Indonesian data processing operations in jurisdictions like Singapore, where a more advanced data center and telecommunications sector can be found. In addition, companies have reported that it is expensive and difficult to build data centers in Indonesia, at least in part due to the country's lack of adequate infrastructure and uneven electricity distribution. Nonetheless, some companies operating within Indonesia (e.g., including foreign businesses like Microsoft Azure in its partnering with local data server providers) appear to be anticipating a broad interpretation of the law and are taking steps to comply before the localization requirements take effect in late 2017.[24]

Kazakhstan. Since 2005, Kazakhstan has required any website using the Kazakh top level domain ".kz" to host its information locally. The Kazakh government enforced this rule in a highly public way in 2010, forcing Google briefly to route all traffic from "google.kz" to "google.com" to avoid hosting a server in the country.[25] The Kazakh government retains the power to deny any application to register a ".kz" domain name if the applicant does locate servers within the country.[26]

Kazakhstan expanded its data localization requirements in 2016 to require that all personal data collected within Kazakhstan be stored locally, similar to Russia's data localization requirement.[27] Kazakh government officials have stated that they believe processing and storing data inside Kazakhstan is essential from a "safety point of view" and that they have the means to enforce compliance, as the government maintains control over the Internet infrastructure in the country through its majority ownership in KazakhTelecom, Kazakhstan's largest Internet service provider.[28] All other telecommunications companies are required to connect their services through the government-controlled backbone, which provides the government with a strong degree of control over content provision, allowing it to block traffic to services that are found to be in non-compliance.

Vietnam. Vietnam's Decree on Management, Provision, and Use of Internet Services and Information Content Online (Decree 72, signed into law in 2013), requires both foreign and domestic companies that operate Internet-based services to physically locate at least one server within Vietnam and to make those servers available for government inspection.[29] It remains unclear exactly how Decree 72 will apply to foreign cross-border service providers and what effect it will have on cross-border data flow, but the Vietnam authorities have indicated they will release guidance clarifying this point.

In 2014, Vietnam released draft implementation guidance that would require all over-the-top services (i.e., online services delivering audio, video, or other media over the Internet) to maintain a server within the country.[30] And in 2016, draft revisions to Decree 72 were released that would, inter alia, require Internet-based services to (1) store information content for at least 90 days after it is posted, (2) store information processing logs (including IP addresses) for at least two years after posting, (3) obtain detailed information

about registered users of services, including ID numbers and contact information that would be verified against a national database, and (4) store data locally in Vietnam.[31]

Vietnam also requires telecommunications and information technology services to comply with its laws on information storage and requires that businesses "trading in civil encryption products" obtain licenses to do so.[32] Vietnam asserts that the data localization measures in place are necessary to protect the security and privacy of Vietnamese Internet users and to allow law enforcement to manage websites committing copyright abuse or exploiting other content without permission.[33]

While not requiring localization, Circular 38/2016/TT-BTTTT (December 2016) of the Ministry of Information and Communications (MIC) requires foreign websites, social networks, online applications, and search engines, any of which are accessible in Vietnam, and that (1) receive one million or more visits from Vietnamese residents per month, or (2) lease a data center to store digital information in Vietnam, to register and cooperate with the MIC with respect to content that infringes the laws of Vietnam. This includes taking down and identifying individuals who post content that threatens national security, incites violence, propagates pornography, or contradicts national traditions.[34]

Nigeria. While no Nigerian statute specifically addresses data localization, the National Information Technology Development Agency (NITDA), the policy-implementing arm of Nigeria's Federal Ministry of Communication and de facto data protection authority, has articulated "local content" requirements. In 2013, the NITDA issued Guidelines for Nigerian Content Development in Information Communication Technology. The Guidelines, which explicitly state their intent to drive indigenous innovation and promote the local Information Communication Technology (ICT) industry, include a mandate that all "subscriber and consumer data" be hosted locally.[35] These Guidelines have not been revised since they were first issued; however, NITDA issued a "final notice" in October of 2015 stating that all affected entities must comply. Some commentators have argued that the legal basis for these particular Guidelines is uncertain.[36]

Absent enforcement action or further clarification, it is unclear how the data localization requirements will translate into actual obligations on companies, especially multinational companies. Indeed, it is not clear which companies are subject to the requirements. And the guidelines require compliance by "ICT Companies" and "all companies operating within the industry," but they do not define what types of companies fit within this scope.[37] The Office of the U.S. Trade Representative stated that the Guidelines appear to "require all foreign and domestic businesses to store all data concerning Nigerian citizens in Nigeria."[38] The U.S. Department of State, on the other hand, noted that NITDA was under new leadership as of September 2016, and that the Nigerian government had a history of "mixed signals on enforcement of local content requirements and their implications," leading to "uncertainty over local content enforcement."[39]

Conclusion

The common thread in the enactment of data localization laws around the world has been the desire of governments to exert local control over the Internet, at least as it is accessible to their citizens. Multinational companies, in particular those that rely heavily on the Internet, are caught in the crossfire. As these data localization laws proliferate, the cost of doing business globally increases because complying enterprises must either open new data centers, change their network architecture, or use a local cloud vendor. Meanwhile, privacy and security suffer as companies are forced to store data in a way that is not the most efficient or effective.

The reality is that data localization laws are here to stay. As companies invest in compliance and governments without these laws see the short-term benefits that accrue to the localizing government in the form of increased access to data and a boost to the local economy, more nations may want to get in the localization game. Without coalitions or policies to combat data localization efforts, the struggle between global business and nationalistic interests will most likely amplify over the years ahead. ■

---

[1] *See generally* Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, Info. Tech. & Innovation Found. (May 2017) [hereinafter *Cross-Border Data Flows*], http://www2.itif.org/2017-cross-border-data-flows.pdf.

[2] *See id.* Australia's My Health Records Act of 2012 prevents various private and public operators and service providers of Australia's Health Record System from storing, holding, processing, or handling health records outside of Australia, although health data may still be transferred outside of Australia if it is scrubbed of personal information. *See* Act No. 63 of 2012, My Health Records Act 2012, pt. 5, § 77(1) (Austl.), https://www.legislation.gov.au/Details/C2016C01104 (last visited Sept. 18, 2017). In July 2017, an update to the German Telecommunications Act began requiring companies storing metadata as required by that act to keep that data within Germany's borders. *See* Telekommunikationsgesetz § 113b, para. 1 (Pflichten zur Speicherung von Verkehrsdaten), https://www.gesetze-im-internet.de/tkg_2004/__113b.html (in German only) (last visited Sept. 18, 2017).

[3] *See, e.g.*, Neha Mishra, *Data Localization Laws in a Digital World: Data Protection or Data Protectionism?* (2016), http://publicspherejournal.com/wp-content/uploads/2016/02/06.data_protection.pdf.

[4] *See* Erik van der Marel et al., *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, European Ctr. for Int'l Political Econ. (May 2014), http://ecipe.org/publications/dataloc/; H. Akın Ünver, *Cross-Border Data Transfers and Data Localization* (June 2016), EDAM Cyber Policy Paper Series 2016/3, http://edam.org.tr/en/File?id=3192.

[5] *See* Office of the U.S. Trade Representative, *2017 National Trade Estimate Report on Foreign Trade Barriers* 375 (Mar. 2017), https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf ("Russian government officials, including President Putin, have signaled that import substitution is now a central tenet of Russian economic policy.").

[6] *See* U.S. Dep't of State, Bureau of Democracy, Human Rights & Labor, *Russia 2016 Country Reports on Human Rights Practices* 30, 51 (Mar. 2017), https://www.state.gov/documents/organization/265678.pdf; Anna

Borshchevskaya, *'Brave New World': Russia's New Anti-Terrorism Legislation*, Forbes (July 8, 2016), https://www.forbes.com/sites/annaborshchevskaya/2016/07/08/brave-new-world-russias-new-anti-terrorism-legislation/.

[7] *See, e.g.*, Jillian C. York, *What's Going on in Central Asia?*, Elec. Frontier Found. (Nov. 29, 2012), https://www.eff.org/deeplinks/2012/11/whats-going-on-in-central-asia; Kaveh Waddell, *Kazakhstan's New Encryption Law Could Be a Preview of US Policy*, Atlantic (Dec. 8, 2015), https://www.theatlantic.com/technology/archive/2015/12/kazakhstans-new-encryption-law-could-be-a-preview-of-us-policy/419250/.

[8] *See, e.g.*, Google, *Transparency Report: Government Requests to Remove Content*, https://www.google.com/transparencyreport/removals/government/?utm_source=privacy+bookmarks (last visited Sept. 18, 2017); Facebook, Government Requests Report, https://govtrequests.facebook.com/ (last visited Sept. 18, 2017).

[9] *See* China Copyright & Media, *Circular of the State Internet Information Office on the Public Consultation on the Measures for the Assessment of Personal Information and Important Data Exit Security* (Draft for Soliciting Opinions) (Apr. 26, 2017), https://chinacopyrightandmedia.wordpress.com/2017/04/11/circular-of-the-state-internet-information-office-on-the-public-consultation-on-the-measures-for-the-assessment-of-personal-information-and-important-data-exit-security-draft-for-soliciting-opinions/ (in Chinese); Chinese Copyright & Media, *Critical Information Infrastructure Security Protection Regulations* (July 12, 2017), https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/ (unofficial English translation); Mark Parsons, *China Passes Controversial Cyber Security Law*, Hogan Lovells Chronicle of Data Prot. (Nov. 15, 2016), http://www.hldataprotection.com/2016/11/articles/international-eu-privacy/china-passes-controversial-cyber-security-law/; Mark Parsons, *"Cybersecurity Review" Takes Shape in China*, Hogan Lovells Chronicle of Data Prot. (Feb. 10, 2017), http://www.hldataprotection.com/2017/02/articles/international-eu-privacy/cybersecurity-review-takes-shape-in-china/; Mark Parsons, *China's Data Localization Measures Open for Comment*, Hogan Lovells Chronicle of Data Prot. (Apr. 20, 2017), http://www.hldataprotection.com/2017/04/articles/international-eu-privacy/chinas-data-localization-measures-open-for-comment/; Mark Parsons et al., *China's Revised Draft Data Localisation Measures*, Hogan Lovells Chronicle of Data Prot. (May 25, 2017), http://www.hldataprotection.com/2017/05/articles/international-eu-privacy/chinas-revised-draft-data-localisation-measures/.

[10] Network Security Law of the Nat'l People's Congress of the People's Republic of China, art. 76(1) and (3) [hereinafter Cyber Security Law], http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (in Chinese), and http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en (unofficial English translation) (last visited Sept. 18, 2017).

[11] Hogan Lovells, *A Brief Analysis of the Draft Key Information Infrastructure Protection Measures* (Aug. 2017), https://f.datasrvr.com/fr1/417/53987/A_brief_analysis_of_the_draft_key_information_infrastructure_protection_measuresV2.pdf.

[12] *See* Chinese Copyright & Media, *Critical Information Infrastructure Security Protection Regulations*, *supra* note 9; Timothy P. Stratford, *China Seeks Public Comments on Draft Regulation on the Protection of Critical Information Infrastructure*, Nat'l Law Rev. (July 13, 2017), https://www.natlawreview.com/article/china-seeks-public-comments-draft-regulation-protection-critical-information.

[13] Cyber Security Law, *supra* note 10, arts. 31 and 37.

[14] *See* Alexander Chipman Koty, *China's New Cybersecurity Law: Clarifications, Implementation Delay Announced*, China Briefing (June 15, 2017), http://www.china-briefing.com/news/2017/06/15/chinas-new-cybersecurity-law-clarifications-implementation-delays.html.

[15] *See* Matthias Bauer, Martina F. Farracane & Erik van der Marel, Global Commission on Internet Governance, *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization* (May 2016), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf (last accessed July 5, 2016).

[16] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks [hereinafter Data Localization Law], https://pd.rkn.gov.ru/authority/p146/p191/ (official translation in English) (last visited Sept. 18, 2017).

[17] Ministry of Telecom & Mass Commc'ns of the Russian Fed'n, *Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года* (Feb. 12, 2016), http://minsvyaz.ru/ru/personaldata. *See also* Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, Bloomberg BNA (Aug. 5, 2015), https://www.bna.com/russia-clarifies-looming-n17179934521/.

[18] Cecilia Kang & Katie Benner, *Russia Requires Apple and Google to Remove LinkedIn from Local App Stores*, N.Y. Times (Jan. 6, 2017), https://nyti.ms/2i242YQ; Ingrid Lunden, *Russia Says 'Nyet,' Continues Linkedin Block After It Refuses to Store Data in Russia*, TechCrunch (Mar. 7, 2017), https://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/.

[19] Natalia Gulyaeva et al., *Russian Data Localization Update: A Year In*, Hogan Lovells Chronicle of Data Prot. (Sep. 15, 2016), http://www.hldataprotection.com/2016/09/articles/international-eu-privacy/russian-data-localization-update-a-year-in/.

[20] *Владислав Новый & Анна Балашова, Apple стала соседом Booking.com* (Sept. 10, 2015), https://www.kommersant.ru/doc/2806495 (in Russian); *Twitter Reportedly Caves to Russian Censors, Will Possibly Move Data to Russian Servers*, Moscow Times (Apr. 19, 2017), https://themoscowtimes.com/news/twitter-plans-to-transfer-personal-data-of-russian-users-to-russia-by-2018-57759; Andrew Roth, *Russia Says Extremists Planned Deadly Bombing Using Encrypted Chat App Telegram*, Wash. Post (June 26, 2017), http://wapo.st/2rUqtlb; Max Seddon, *Telegram Founder Agrees to Register App with Russian Censors*, Fin. Times (June 28, 2017), https://www.ft.com/content/8bfc8e20-5c15-11e7-9bc8-8055f264aa8b.

[21] *See* Regulation of the Gov't of the Rep. of Indonesia No. 82 of 2012 Concerning Electronic and Transaction Operation, http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html (translation in English) (last visited Sept. 18, 2017); Office of the U.S. Trade Representative, *Fact Sheet: Key Barriers to Digital Trade* (Mar. 2016), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade.

[22] *Indonesia May Force Web Giants to Build Local Data Centers*, Asia Sentinel (Jan. 17, 2014), http://www.asiasentinel.com/econ-business/indonesia-web-giants-local-data-centers/.

[23] *See* Gilang Ardana, *KOMINFO Releases Personal Data Protection Regulation*, Am. Chamber of Commerce in Indonesia (Jan. 17, 2017), https://www.amcham.or.id/fe/5487-kominfo-releases-personal-data-protection-regulation; Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tanggal 1 Desember 2016 (2016), (in Indonesian), https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016 (last visited Sept. 18, 2017).

[24] *See Telkomtelstra, Microsoft Launch Hybrid Cloud Solution*, Jakarta Post (Aug. 11, 2017), http://www.thejakartapost.com/adv/2017/08/11/telkomtelstra-microsoft-launch-hybrid-cloud-solution.html ("This is a joint effort to tap into Indonesia's growing cloud services market, helping companies to *comply with the local data residency policy*, lower latency and better access performance, and trusted local support to implement cloud strategy into their business.") (emphasis added). *See Indonesia Heading for Sensible Cloud Policy?*, ConnectedAsia (Jan. 25, 2016), http://www.connectedasia.com/indonesia-heading-for-sensible-cloud-policy/.

[25] Bill Coughran, *Changes to the Open Internet in Kazakhstan*, Google Blog (June 7, 2011), https://googleblog.blogspot.com/2011/06/changes-to-open-internet-in-kazakhstan.html.

[26] Kazakhstan Network Info. Ctr., Press Release (June 8, 2011), http://nic.kz/docs/announc_14_06_2011.jsp (in Russian); Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 706 (2015); Glob. Campaign for Free Expression, *Article 19: Note on Kazakhstan's Regulations for the Allocation of Domain Space* 2–3 (Oct. 2005), http://www.osce.org/fom/16759?download=true.

[27] *Cross-Border Data Flows*, *supra* note 1, at 26; *Kazakhstan: Data Protection 2017*, ICLG (May 15, 2017), https://iclg.com/practice-areas/data-protection/data-protection-2017/kazakhstan#chaptercontent1 ("storage of Per-

sonal Data is only allowed through databases located in Kazakhstan"); Law of the Republic of Kazakhstan No. 370-11 of January 7, 2003, on Electronic Documents and Electronic Digital Signatures (as amended up to Law No. 419-V of November 24, 2015), WIPO, http://www.wipo.int/wipolex/en/details.jsp?id=16138 (in Russian and Kazakh only) (last visited Sept. 18, 2017).

[28] *Cross-Border Data Flows*, *supra* note 1; Daniyar Sabitov, *Information Security in Kazakhstan: Protection of Data and Ideas* (Inst. of World Econ. & Politics Working Paper, Mar. 2016), http://iwep.kz/files/attachments/article/2016-05-31/daniyar_sabitov_information_security.pdf.

[29] Decree No. 72/2013/ND-CP of July 15, 2013 On the Management, Provision and Use of Internet Services and Online Information, https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF (last visited Sept. 18, 2017). The law defines these services as: "social networks," art. 25(9); "aggregated information websites," art. 24(1) (information that is collected from multiple sources about "politics, economics, culture and/or society," art. 3(19)); "mobile telecommunications networks," art. 28(2); and "online game service providers," art. 34.

[30] *See* Letter from Marc P. Mealy, Vice President-Policy, US-ASEAN Bus. Council, & Jimmy Goodrich, Dir., Glob. Policy, Info. Tech. Indus. Council, to Dr. Nguyen Bac Son, Minister of Info. & Commc'ns, Vietnam (Jan. 6, 2015), http://cloud.chambermaster.com/userfiles/UserFiles/chambers/9078/File/ICT/2015/VietnamOTTCircular-USABC-ITILetterFINAL.pdf.

[31] Letter from Hans W. Vriens, Secretariat, Asia Internet Coal., to Legal Dep't, Vietnam Chamber of Commerce & Indus. 2 (Oct. 17, 2016) (Formal Comments on the Draft Decree Amending Decree 72, Asia Internet Coalition), https://www.aicasia.org/wp-content/uploads/2016/11/AIC-Comments-on-Decree-Amending-Decree-72-2016_10_17.pdf.

[32] Law No.: 86/2015/QH13, Law on Network Information Security, arts. 10(3) and 31(1), http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf (last visited Sept. 18, 2017).

[33] Chander & Lê, *supra* note 26.

[34] Decree No. 72, *supra* note 29, art. 5.

[35] Office for Nigerian Content Dev. in Info. & Commc'n Tech., Guidelines for Nigerian Content Development in Information Communication Technology 12.1(4) and 14.1(2), at 19, 23 (effective Dec. 3, 2013) [hereinafter Guidelines], http://onc.org.ng/onc-guidelines-download.

[36] *Tax Alert: NITDA Has Issued a Final Notice of Local Content Compliance for ICT Companies*, PricewaterhouseCoopers Nigeria (Oct. 2015), http://pwcnigeria.typepad.com/files/tax-alert—final-notice-on-local-content-guidelines-for-ict-companies.pdf; Tola Akinmutimi, *NITDA Issues Local Content Compliance Final Notice to ICT Firms*, Nat'l Mirror 41 (Oct. 30, 2015), https://issuu.com/73092/docs/binder1_6921e5e246416d/41.

[37] For instance, the Guidelines also require that ICT companies migrate network peering provisions to locally available services. *See* Guidelines, *supra* note 35, at 16, 19 (11.3(2) and 12.1(6)). The presence of such requirements might indicate a presumption of physical in-country footprint even though the Guidelines make no such distinction. The Guidelines state only that an ICT is "a combination of equipment and services that enables remote gathering, processing, storage, conveyance and delivery of various forms of information." Guidelines, *supra* note 35, at n.4.

[38] *2017 National Trade Estimate Report on Foreign Trade Barriers*, *supra* note 5, at 327.

[39] U.S. Dep't of State, Bureau of Econ. & Bus. Affairs, Nigeria Investment Climate Statements for 2017, http://www.state.gov/e/eb/rls/othr/ics/investmentclimatestatements/index.htm?year=2017&dlid=269767 (last visited Sept. 18, 2017).